ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ

εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

**ΥΠΟΕΡΓΟ: ΥΠΟΕΡΓΟ 3 «ΔΡΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΠΟΙΟΤΗΤΑΣ ΕΠΙΜΟΡΦΩΤΙΚΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ»**

**της Πράξης «ΔΡΑΣΕΙΣ ΣΥΝΕΧΙΖΟΜΕΝΗΣ ΚΑΤΑΡΤΙΣΗΣ 2014-2018»**
**κωδ. ΟΠΣ 5000245**

# ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ:

# Γενικός Κανονισμός Προστασίας Δεδομένων: Οι υποχρεώσεις της Δημόσιας Διοίκησης

## ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΛΙΚΟ

**Κωδικός εκπαιδευτικού υλικού:**

**Κωδικός Πιστοποίησης προγράμματος: 636**

Ευρωπαϊκή Ένωση
Ευρωπαϊκά Διαρθρωτικά και Επενδυτικά Ταμεία
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**ΥΠΟΕΡΓΟ: ΥΠΟΕΡΓΟ 3 «ΔΡΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΠΟΙΟΤΗΤΑΣ ΕΠΙΜΟΡΦΩΤΙΚΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ»**

# ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ:

# Γενικός Κανονισμός Προστασίας Δεδομένων: Οι υποχρεώσεις της Δημόσιας Διοίκησης

## ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ


**Μέλη Ομάδας**

**Συντονιστής: Δρ. Γεώργιος Παπαμιχαήλ**

**Συγγραφείς: Δρ. Κωνσταντίνος Λιμνιώτης, Δρ. Γεώργιος Ρουσόπουλος**

**Αξιολογητές/τριες: Δρ. Ευφροσύνη Σιουγλέ, Ιωάννης Ματζαβάκης**




Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# Περιεχόμενα





Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 1. Εισαγωγή

Το Ινστιτούτο Επιμόρφωσης του Εθνικού Κέντρου Δημόσιας Διοίκησης και Αυτοδιοίκησης διοργανώνει με επιτυχία, από τις αρχές του 2018 το σεμινάριο με τίτλο «Γενικός Κανονισμός Προστασίας Δεδομένων: Οι υποχρεώσεις της Δημόσιας Διοίκησης». Στο σεμινάριο αυτό έχουν συμμετάσχει εκατοντάδες υπαλλήλων των Δημοσίου και ιδίως στελέχη που υπηρετούν ή πρόκειται να υπηρετήσουν στη νευραλγική θέση του Υπευθύνου Προστασίας Δεδομένων ή υπηρετούν σε θέσεις ευθύνης οργανικών μονάδων που σχετίζονται με επεξεργασίες δεδομένων προσωπικού χαρακτήρα.

Στόχος του σεμιναρίου είναι να εισάγει τους εκπαιδευόμενους στη λογική του Γενικού Κανονισμού αλλά και γενικότερα των νομικών προβλέψεων αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, εστιάζοντας στις διατάξεις που αφορούν κυρίως το δημόσιο τομέα και με προσανατολισμό σε πρακτικά ζητήματα που συχνά καλούνται να αντιμετωπίσουν οι δημόσιοι φορείς..

Αναπόφευκτα, το σύνολο των διατάξεων αυτής της νομοθεσίας, δεν μπορεί να καλυφθεί πλήρως σε ένα σεμινάριο λίγων ημερών. Άλλωστε, το εν λόγω εκπαιδευτικό πρόγραμμα αποσκοπεί στο να παρέχει τις βάσεις για όποιον θέλει να εμβαθύνει στο εν λόγω πεδίο ή και ενδεχομένως να ασχοληθεί ενεργά με την προστασία δεδομένων. Για το σκοπό αυτό, οι σημειώσεις που ακολουθούν δεν παρουσιάζουν όλα τα ζητήματα, ούτε όσα παρουσιάζονται αναλύονται σε κάθε λεπτομέρειά τους. Στόχος των συγγραφέων είναι να δώσουν ένα εγχειρίδιο αναφοράς, το οποίο θα βοηθήσει όποιον επιθυμεί να ξεκινήσει την ενασχόληση με την προστασία προσωπικών δεδομένων. Για όποιον όμως θελήσει να ασχοληθεί περαιτέρω, θα βρει στις σημειώσεις πολλές αναφορές και κείμενα προς εμβάθυνση, τα οποία θα τον βοηθήσουν για το επόμενο βήμα.

Το παρόν υλικό βασίζεται σε μεγάλο βαθμό και στην εμπειρία που έχουν αποκομίσει οι συγγραφείς από την πλέον των τριών ετών διδασκαλία τους στο εν λόγω σεμινάριο, ενώ επίσης έχουν αξιοποιηθεί τόσο η νομολογία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα όσο επίσης και σχετικά κείμενα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 2. Εισαγωγή στο θεσμικό πλαίσιο προστασίας προσωπικών δεδομένων: Ιστορική αναδρομή, το ευρωπαϊκό πλαίσιο

Η 27η Απριλίου του 2016 σηματοδοτεί μια μεγάλη αλλαγή στο θεσμικό πλαίσιο της Ε.Ε.. Τη μέρα αυτή ολοκληρώθηκε η διαδικασία έγκρισης του Γενικού Κανονισμού Προστασίας Δεδομένων (εφεξής, ΓΚΠΔ [1]), ο οποίος επικαιροποίησε και ομογενοποίησε το πλαίσιο προστασίας των προσωπικών δεδομένων που η Ε.Ε. είχε εισάγει από το 1995. Ο κανονισμός τέθηκε σε ισχύ στις 24 Μαΐου 2016, ενώ δόθηκε μια μεταβατική διετία για την προετοιμασία της εφαρμογής τους και την προσαρμογή στις ρυθμίσεις του. Ξεκίνησε να εφαρμόζεται από τις 25 Μαΐου 2018.

Ο κανονισμός βασίστηκε στην προϋπάρχουσα Οδηγία 95/46/ΕΚ [2] τη νομολογία των αρχών προστασίας δεδομένων αλλά και του ΔΕΕ, ενισχύοντας σημαντικά το βασικό καθεστώς προστασίας δεδομένων, παρέχοντας ισχυρότερα δικαιώματα στους πολίτες και πολλές αλλαγές όσον αφορά την εναρμόνιση και τη διασυνοριακή συνεργασία για την επιβολή της νομοθεσίας μεταξύ των εποπτικών αρχών προστασίας δεδομένων.

## 2.1 Ιστορική αναδρομή

Ο ΓΚΠΔ ήταν η «απάντηση» της ΕΕ σε μια εικοσαετία ραγδαίων εξελίξεων, εισαγωγής επεμβατικών τεχνολογιών σε μια ολοένα και πιο παγκοσμιοποιημένη οικονομία, καθώς και μαζικής επέκτασης εφαρμογών που χρησιμοποιούν προσωπικά δεδομένα χαρακτήρα σχεδόν σε κάθε πτυχή της καθημερινότητας με αποδοχή τους από τους πολίτες ως τμήμα της καθημερινότητάς τους. Η έγκριση της συνθήκης της Λισαβόνας [3] και η αναγωγή της προστασίας των προσωπικών δεδομένων σε θεμελιώδες δικαίωμα στην ΕΕ έδωσε τη δυνατότητα για αλλαγές στο σχετικό θεσμικό πλαίσιο και η Ευρωπαϊκή Επιτροπή παρουσίασε το σχέδιο του ΓΚΠΔ στις αρχές του 2012. Μετά από μακροχρόνιες διαπραγματεύσεις, πιθανότατα και υπό το βάρος των αποκαλύψεων του Edward Snowden, η ΕΕ κατέληξε να εγκρίνει ένα φιλόδοξο



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κείμενο. Κρίσιμο όμως για την κατανόηση των διατάξεων του ΓΚΠΔ είναι να αντιληφθούμε το πλαίσιο μέσα στο οποίο λειτουργεί.

### 2.1.1 Ατομικά δικαιώματα και ελευθερίες

Η ελευθερία και η ισότητα είναι συστατικά στοιχεία του δημοκρατικού πολιτεύματος. Βασικό χαρακτηριστικό της έννοιας της ελευθερίας είναι να μην υπόκειται κανείς στη βούληση ενός άλλου. Στη σύγχρονη δημοκρατία, ελευθερία σημαίνει δυνατότητα ανεμπόδιστης ανάπτυξης της προσωπικότητας, ανεμπόδιστα από εξωτερικές παρεμβάσεις. Το κράτος οφείλει να εξασφαλίζει ότι όλοι οι πολίτες απολαμβάνουν εξίσου αυτή την δυνατότητα. Συνεπώς, τίθεται αυτομάτως ένα όριο στην ελευθερία του καθενός και της καθεμιάς από εμάς: Η ελευθερία των άλλων. Επομένως, η ελευθερία είναι δικαίωμα, αλλά ταυτόχρονα, ευθύνη και υποχρέωση σεβασμού της ελευθερίας των άλλων.

Με ποιόν όμως τρόπο εκφράζεται η έννοια της ελευθερίας στην πράξη στις σημερινές δημοκρατικές κοινωνίες; Η απάντηση είναι: με την αναγνώριση δικαιωμάτων. Το βασικό κείμενο στο οποίο κατοχυρώνονται τα δικαιώματα ενός ανθρώπου, τόσο ως άτομο όσο και ως μέρος του κοινωνικού συνόλου είναι το Σύνταγμα ενός κράτους.

Τα συνταγματικά κατοχυρωμένα δικαιώματα διακρίνονται, με βάση το περιεχόμενό τους, σε τρεις γενικές κατηγορίες:

**Ατομικά δικαιώματα**: Αυτά δίνουν στο άτομο τη δυνατότητα να «*αμύνεται*» απέναντι σε ενδεχόμενη αυθαιρεσία των οργάνων της κρατικής εξουσίας. Το κράτος πρέπει να απέχει, να μην παρεμβαίνει στη σφαίρα της ιδιωτικής αυτονομίας. Τέτοια δικαιώματα είναι για παράδειγμα τα εξής: προσωπική ασφάλεια, αρχή του νόμιμου δικαστή, άσυλο της κατοικίας και προστασία του ιδιωτικού βίου, δικαίωμα αναφοράς στις αρχές, θρησκευτική ελευθερία, ελευθερία τύπου και έκφρασης κ.α.

**Πολιτικά δικαιώματα**: Αυτά εγγυώνται τη συμμετοχή του ατόμου στις πολιτικές διαδικασίες, την άσκηση της εξουσίας. Τέτοια δικαιώματα είναι για παράδειγμα τα εξής: Το δικαίωμα του εκλέγειν και εκλέγεσθαι, η ίδρυση ή συμμετοχή σε πολιτικό κόμμα, ο διορισμός ως δημοσίου υπαλλήλου σε δημόσιες θέσεις, ο διορισμός ως ενόρκου κ.α.

**Κοινωνικά δικαιώματα**: Αυτά συνιστούν εγγυήσεις για την παρέμβαση της



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

πολιτείας στην κοινωνική ζωή και την εξασφάλιση παροχών για τη δικαιότερη κατανομή του κοινωνικού πλούτου. Τέτοια δικαιώματα είναι για παράδειγμα τα εξής: η προστασία της οικογένειας, του γάμου, της μητρότητας και της παιδικής ηλικίας, η υγεία, η εργασία, η ελευθερία της τέχνης, της επιστήμης και της παιδείας, η προστασία του φυσικού και πολιτιστικού περιβάλλοντος κ.α.

Φυσικά, το Σύνταγμα, εκτός από δικαιώματα, καθιερώνει και υποχρεώσεις των πολιτών. Τέτοιες υποχρεώσεις είναι για παράδειγμα οι εξής: σεβασμός του Συντάγματος και τήρηση των νόμων, κοινωνική ευθύνη και εθνική αλληλεγγύη, φορολογική, στρατολογική και υποχρεωτική εκπαίδευση, κ.α.

Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί, όπως είναι εύκολο να καταλάβει κανείς, ατομικό δικαίωμα. Είναι όμως ένα «νέο» σχετικά δικαίωμα, η κατοχύρωση του οποίου σχετίζεται με τους κινδύνους που επιφέρει η δυνατότητα μαζικής επεξεργασίας πληροφοριών που εισήγαγε στο δεύτερο μισό του 20ου αιώνα η ραγδαία ανάπτυξη της πληροφορικής.

### 2.1.2 Ευρωπαϊκή χάρτα δικαιωμάτων του ανθρώπου και πρώτοι εθνικοί νόμοι

Η εποχή μετά το Β' Παγκόσμιο Πόλεμο σηματοδοτεί την σύναψη ισχυρών διεθνών συνθηκών στις οποίες κατοχυρώνονται τα ανθρώπινα δικαιώματα. Το 1948, στην Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου [4] κατοχυρώνεται στο άρθρο 12[1] το δικαίωμα στην προστασία της ιδιωτικής σφαίρας του ατόμου έναντι αυθαίρετων επεμβάσεων τρίτων (και κυρίως του κράτους) για πρώτη φορά σε διεθνές νομικό κείμενο. Η Ελλάδα κυρώνει τη διακήρυξη με το ν. 2329/1953.

Το 1950 υπογράφεται η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ [5]) με την οποία δημιουργείται το Συμβούλιο της Ευρώπης. Σε αυτή προβλέπεται στο άρθρο 8 το Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής.

**Άρθρο 8 ΕΣΔΑ**

1. Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής

[1] Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ζωής του, της κατοικίας του και της αλληλογραφίας του.

2. Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.

Το δικαίωμα αυτό, αν και δεν κάνει αναφορά σε προσωπικά δεδομένα, δίνει για πρώτη φορά προστασία στον πολίτη από αδικαιολόγητες παρεμβάσεις του κράτους στην ιδιωτική του ζωή, όπως με την παρακολούθηση των επικοινωνιών του ή την ποινικοποίηση της σεξουαλικής του ζωής. Σε κάποιες περιπτώσεις, το δικαίωμα αυτό επεκτάθηκε ώστε να προστατεύει και από την επέμβαση ιδιωτών (π.χ. από παρακολούθηση επικοινωνιών από εργοδότη) αλλά χωρίς να μπορεί να θεωρηθεί ότι προστατεύει ένα πολίτη από τις πράξεις άλλων ατόμων.

Η αλλαγή που επέβαλε την ανάγκη για επέκταση της προστασίας με ένα νέο δικαίωμα ήρθε με τη ολοένα και ταχύτερη διείσδυση των ηλεκτρονικών υπολογιστών στις δραστηριότητες κρατών και επιχειρήσεων. Ήδη από τη δεκαετία του 1960 οι Η/Υ χρησιμοποιούνται σε διάφορες εργασίες δημοσίων και ιδιωτικών φορέων, όπως για μισθοδοσίες, δημόσια μητρώα και αρχεία, μεγάλα νοσοκομεία κ.α.. Ο αρχικά μεγάλος όγκος τους και το τεράστιο κόστος τους σταδιακά μειώνεται, ενώ ταυτόχρονα οι δυνατότητές τους ολοένα και αυξάνονται. Τη δεκαετία του 1970 η συζήτηση επικεντρώνεται στους κινδύνους για την ιδιωτική ζωή όχι μόνο από λάθη σε αυτοματοποιημένες επεξεργασίες αλλά και για το φόβο της χρήσης κεντρικών βάσεων δεδομένων από απολυταρχικά καθεστώτα. Το λεγόμενο «φακέλωμα» ήταν άλλωστε πρακτική γνωστή τόσο στο Δυτικό όσο και στον Ανατολικό κόσμο.

Για πρώτη φορά ο όρος «Προστασία Δεδομένων» (στα γερμανικά Datenschutz) εμφανίζεται σε νόμο του κρατιδίου της Έσσης. Μάλιστα, πρωτεργάτης του θεωρείται ένας Έλληνας, ο Σπύρος Σημίτης. Τα επόμενα χρόνια της δεκαετίας του 1970 ακολουθούν και άλλα κράτη (Σουηδία, Ομοσπονδιακή Δημοκρατία της Γερμανίας, Γαλλία, Αυστρία, Δανία, Νορβηγία και Λουξεμβούργο).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Η νομοθεσία για τα προσωπικά δεδομένα προσπαθεί να αντιμετωπίσει τον κίνδυνο που επέρχεται με τη χρήση Η/Υ· οι Η/Υ από τη φύση τους διευκολύνουν τη μαζική επεξεργασία πληροφοριών και νέες χρήσεις αυτών, χωρίς κανένα όριο. Χωρίς τους Η/Υ είναι πολύ πιθανό ότι όλα τα ζητήματα θα μπορούσαν να αντιμετωπιστούν με άλλα νομοθετικά εργαλεία

☞ Η νομοθεσία για τα προσωπικά δεδομένα προσπαθεί να περιορίσει την κατάχρηση των ατομικών πληροφοριών μέσω πληροφοριακών συστημάτων.

### 2.1.3 Η Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία δεδομένων

Το 1981 είναι ένα σημείο καμπής για την νομοθεσία των προσωπικών δεδομένων. Το έτος αυτό ψηφίζεται από το Συμβούλιο της Ευρώπης η Σύμβαση 108 (για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία των προσωπικών πληροφοριών) [6]. **Η πράξη αυτή ήταν και παραμένει η μόνη νομικά δεσμευτική διεθνής πράξη στον τομέα της προστασίας των προσωπικών δεδομένων** (εκτός ΕΕ). Κι αυτό γιατί ως συνθήκη του Συμβουλίου της Ευρώπης είναι ανοιχτή σε υπογραφή και από κράτη εκτός της ευρωπαϊκής ηπείρου. Τουλάχιστον οκτώ (8) κράτη, εκτός από τα μέλη του Συμβουλίου της Ευρώπης, την έχουν επικυρώσει έως σήμερα (συνολικά 55 έως τα τέλη του 2021). Η Σύμβαση 108 κυρώθηκε από την Ελλάδα με το Ν.2068/1992, ενώ άρχισε να ισχύει από την 1/1/1995. Πρόσφατα, το 2018, η σύμβαση τροποποιήθηκε με πρόσθετο πρωτόκολλο (10/10/2018) με στόχο να βελτιωθεί και να επικαιροποιηθεί [7]. Η Ελλάδα υπέγραψε το Πρωτόκολλο στις αρχές του Σεπτεμβρίου 2019 και πρέπει να εισάγει νόμο για την εφαρμογή του.

Σύμφωνα με τη συνθήκη, τα κράτη που τη συνυπογράφουν απαιτείται να λάβουν απαραίτητα μέτρα στην εθνική τους νομοθεσία ώστε να εφαρμόζουν τις αρχές που καθορίζει η συνθήκη με στόχο να εξασφαλίζεται ότι στην επικράτειά τους θα είναι σεβαστό το θεμελιώδες δικαίωμα όλων των ανθρώπων για την προστασία των δεδομένων προσωπικού χαρακτήρα. Βασικά χαρακτηριστικά της συνθήκης είναι ότι αναγνωρίζεται ότι για κάποιες προσωπικές πληροφορίες που θεωρούνται πιο κοντά



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

στο πυρήνα της προσωπικότητας ενός ατόμου απαιτούνται περισσότερες διασφαλίσεις προκειμένου να είναι δυνατό για κάποιον να τις επεξεργαστεί αυτοματοποιημένα. Είναι η πρώτη φορά που, διεθνώς, κάποιες κατηγορίες προσωπικών δεδομένων αναγνωρίζονται ως «ειδικές κατηγορίες δεδομένων» τα λεγόμενα ευαίσθητα προσωπικά δεδομένα.

(…) Οι πληροφορίες προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή άλλες πεποιθήσεις, όπως και οι πληροφορίες προσωπικού χαρακτήρα που σχετίζονται με την υγεία ή την σεξουαλική ζωή, δεν δύνανται να αποτελέσουν αντικείμενο αυτοματοποιημένης επεξεργασίας, εάν το εσωτερικό δίκαιο δεν προβλέπει κατάλληλες εγγυήσεις. Το αυτό ισχύει για τις πληροφορίες προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες (…)

Στο άρθρο 13 της συνθήκης προβλέπεται η λειτουργία εθνικών αρχών για την προστασία των προσωπικών δεδομένων.

## 2.2 Το Ευρωπαϊκό πλαίσιο προστασίας δεδομένων προ του ΓΚΠΔ

Πριν εξετάσουμε την εξέλιξη της νομοθεσίας για τα προσωπικά δεδομένα στην Ευρωπαϊκή Ένωση, είναι χρήσιμο να δούμε συνοπτικά με ποιο τρόπο είναι διαρθρωμένο το σύστημα δικαίου της Ένωσης. Το σύστημα αυτό δεν διαφέρει ουσιωδώς από το σύστημα των περισσοτέρων Κ-Μ, αλλά έχει τις δικές του ιδιαιτερότητες.

Το δίκαιο της ΕΕ περιλαμβάνει το πρωτογενές και το παράγωγο δίκαιο της ΕΕ.

Πρωτογενές Δίκαιο: Οι Συνθήκες, και συγκεκριμένα η Συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ [8]) και η Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ [9]), έχουν κυρωθεί από όλα τα κράτη μέλη της και αποτελούν το «πρωτογενές δίκαιο της ΕΕ». Στις αρχές της δεκαετίας του 2000 τα Κ-Μ προσπάθησαν, αλλά απέτυχαν, να εισάγουν και συνθήκη για τη θέσπιση Συντάγματος της Ευρώπης.

Παράγωγο Δίκαιο: Οι κανονισμοί, οι οδηγίες και οι αποφάσεις της ΕΕ που εκδίδονται από τα θεσμικά της όργανα κατόπιν σχετικής εξουσιοδότησης βάσει των Συνθηκών. Συνοπτικά διακρίνεται σε:



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Κανονισμοί: Έχουν *γενική, ενιαία και απόλυτη ισχύ*, είναι δεσμευτικοί προς όλα τα κράτη μέλη και ισχύουν άμεσα σε κάθε κράτος μέλος. Έτσι, δεν απαιτείται έκδοση οποιασδήποτε διοικητικής πράξης ή συμπληρωματικού μέτρου για να εφαρμοστεί στο κάθε κράτος. Δεσμεύουν όχι μόνο τα Κ-Μ ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου, αλλά επεκτείνονται και στους ιδιώτες. Μπορεί βέβαια να απαιτείται αντίστοιχη εναρμόνιση του εσωτερικού δικαίου των Κ-Μ προς αποφυγή συγκρούσεων.
- Οδηγίες: Είναι *δεσμευτικές μόνο ως προς το αποτέλεσμα* που επιδιώκεται στο κράτος μέλος προς το οποίο απευθύνονται, αλλά αφήνουν την επιλογή του τρόπου και των μέσων στην αρμοδιότητα των εθνικών κρατών, τάσσοντας μια καθορισμένη προθεσμία μέσα στην οποία θα πρέπει να υλοποιηθούν οι στόχοι που θέτει. Απευθύνονται μόνο στο κράτος μέλος, το οποίο οφείλει να εισάγει νόμο για την εφαρμογή της και όχι άμεσα στους ιδιώτες.
- Αποφάσεις: Είναι δεσμευτικές άμεσα και στο σύνολό τους, αλλά μόνο για αυτούς στους οποίους προορίζονται.
- Γνώμες – Συστάσεις: Δεν έχουν δεσμευτική ισχύ, αλλά βοηθούν στην ασφαλή ερμηνεία του δικαίου.

Σε πολλές περιπτώσεις βέβαια, ένας κανονισμός περιέχει συγκεκριμένες επιμέρους ρυθμίσεις που αφήνουν την ευχέρεια στα Κ-Μ να επιλέξουν τον τρόπο εφαρμογής συγκεκριμένων ρυθμίσεων στο εσωτερικό μιας χώρας, έχουν δηλαδή και χαρακτηριστικά οδηγίας.

### 2.2.1 Η προστασία των προσωπικών δεδομένων στο δίκαιο της ΕΕ

Οι αρχικές Συνθήκες των Ευρωπαϊκών Κοινοτήτων δεν περιείχαν καμία αναφορά σε ανθρώπινα δικαιώματα, καθώς η τότε Ευρωπαϊκή Οικονομική Κοινότητα είχε σχεδιαστεί με σκοπό την οικονομική συνεργασία και την εγκαθίδρυση κοινής αγοράς. Θεμελιώδης αρχή η οποία εξακολουθεί να ισχύει σήμερα είναι η αρχή της δοτής αρμοδιότητας, σύμφωνα με την οποία, η ΕΕ ενεργεί μόνο εντός των ορίων των αρμοδιοτήτων που της αναθέτουν τα κράτη μέλη, όπως προβλέπεται στις Συνθήκες της. Σε αντίθεση με ό,τι συμβαίνει με το Συμβούλιο της Ευρώπης, οι Συνθήκες της ΕΕ δεν προβλέπουν καμία ρητή αρμοδιότητα σε θέματα θεμελιωδών δικαιωμάτων. Ωστόσο, καθώς το ΔΕΕ σταδιακά εξέδιδε αποφάσεις με τις οποίες ενέτασσε τα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

θεμελιώδη δικαιώματα στις λεγόμενες γενικές αρχές του ευρωπαϊκού δικαίου, και καθώς οι πολιτικές της ΕΕ έχουν αντίκτυπο στα ανθρώπινα δικαιώματα, η ΕΕ προέβη το 2000 στη διακήρυξη του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (εφεξής Χάρτης [10]).

Ο Χάρτης ενσωματώνει το πλήρες φάσμα των ατομικών, πολιτικών, οικονομικών και κοινωνικών δικαιωμάτων των ευρωπαίων πολιτών, σε μία σύνθεση των κοινών συνταγματικών παραδόσεων και των κοινών διεθνών υποχρεώσεων των Κ-Μ. Περιλαμβάνει 6 κεφάλαια: αξιοπρέπεια, ελευθερίες, ισότητα, αλληλεγγύη, δικαιώματα των πολιτών και δικαιοσύνη. Αν και αρχικά είχε τη μορφή διακήρυξης, κατέστη νομικά δεσμευτικός *ως πρωτογενές ενωσιακό δίκαιο* (κατά παραπομπή του άρθρου 6 ΣΕΕ) με την έναρξη ισχύος της συνθήκης της Λισαβόνας, την 1/12/2009.

Ο Χάρτης εγγυάται τόσο το σεβασμό της ιδιωτικής και οικογενειακής ζωής (άρθρο 7) όσο και την προστασία των δεδομένων προσωπικού χαρακτήρα (άρθρο 8). **Συνεπώς, από το 2009, η προστασία των δεδομένων προσωπικού χαρακτήρα έχει αναχθεί μέσω των συνθηκών σε θεμελιώδες δικαίωμα για τους πολίτες της ΕΕ**, ακόμα και για τα Κ-Μ που δεν έχουν σχετική συνταγματική πρόβλεψη. Πλέον –λαμβάνοντας υπόψη και τις τροποποιήσεις στη νομοθετική διαδικασία που εισήγαγε η Συνθήκη της Λισαβόνας- η ΕΕ έχει τη δυνατότητα να νομοθετήσει σε επίπεδο Ένωσης με τρόπο που να εξασφαλίζει άμεση εφαρμογή ρυθμίσεων σε όλα τα Κ-Μ.

**Άρθρο 8 – Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης**

Προστασία των δεδομένων προσωπικού χαρακτήρα

1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.
2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεχθέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.
3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.

Η αλλαγή αυτή είναι μια σημαντική εξέλιξη. Οι παλιότεροι κανόνες της ΕΕ περί προστασίας δεδομένων βασίζονταν στην ανάγκη για ορθή λειτουργία της εσωτερικής αγοράς και την αναγκαιότητα προσέγγισης των εθνικών νομοθεσιών, ώστε να μην



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εμποδίζεται η ελεύθερη κυκλοφορία των δεδομένων εντός της ΕΕ. Πλέον η προσέγγιση του δικαιώματος δεν αφορά μόνο τη λειτουργία της αγοράς αλλά ξεκάθαρα και την προστασία το πυρήνα του ατομικού δικαιώματος, ενώ καλύπτει όλα τα θέματα αρμοδιότητας της ΕΕ, ακόμα και την αστυνομική και δικαστική συνεργασία.

### 2.2.2 Η εξέλιξη του δικαίου της ΕΕ σε σχέση με τα προσωπικά δεδομένα

Ήδη τη δεκαετία του 1990 αρκετά Κ-Μ διέθεταν εθνική νομοθεσία για την προστασία των δεδομένων ενώ τα περισσότερα είχαν υπογράψει και τη Σύμβαση 108 του Συμβουλίου της Ευρώπης. Οι διαφορετικές ρυθμίσεις ανά Κ-Μ έθεταν εμπόδια στην ανταλλαγή δεδομένων μεταξύ των κρατών και την λειτουργία των επιχειρήσεων. Έτσι προέκυψε η ανάγκη για εναρμόνιση των νομοθεσιών αυτών, ώστε αφενός να διασφαλίζεται υψηλό επίπεδο προστασίας και αφετέρου ελεύθερη ροή των δεδομένων προσωπικού χαρακτήρα μεταξύ των διαφόρων κρατών μελών. Η ελεύθερη κυκλοφορία εμπορευμάτων, κεφαλαίων, υπηρεσιών και προσώπων στην εσωτερική αγορά απαιτούσε ελεύθερη ροή των δεδομένων και αυτό έπρεπε να συμβαίνει σε ένα ασφαλές περιβάλλον.

Το 1995 εγκρίνεται η πρώτη νομική πράξη της ΕΕ σχετικά με την προστασία των δεδομένων, **η οδηγία 95/46/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η οδηγία είχε ως βάση τη σύμβαση 108 και τις υφιστάμενες εθνικές νομοθεσίες και εισήγαγε την υποχρέωση στα Κ-Μ να νομοθετήσουν με βάση τα εξής βασικά χαρακτηριστικά:

- ελεύθερη ροή δεδομένων εντός της εσωτερικής αγοράς
- ενιαίο (ισοδύναμο) και υψηλό επίπεδο προστασίας των δεδομένων.
- καθιέρωση των ανεξάρτητων εποπτικών αρχών
- εδαφικό πεδίο εφαρμογής που περιλαμβάνει και κράτη ΕΟΧ

Στα Κ-Μ δόθηκαν περιορισμένα περιθώρια ελιγμού κατά την μεταφορά της οδηγίας, ώστε να επιτευχθεί μεγάλο επίπεδο ομοιογένειας της νομοθεσίας, ενώ προβλέφθηκε και ομάδα εργασίας για το συντονισμό του έργου των εποπτικών αρχών των Κ-Μ και



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

με γνωμοδοτικό ρόλο. Δεδομένου ότι η εν λόγω ομάδα εργασίας προβλεπόταν στο άρθρο 29 της Οδηγίας, καθιερώθηκε για αυτήν ο όρος «Ομάδα Εργασίας του άρθρου 29» (Article 29 Working Party) – εφεξής, Ο.Ε του άρθρου 29. Η οδηγία δεν μπορούσε να ρυθμίσει θέματα αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις, τα οποία δεν είχαν σχέση με τη ρύθμιση της εσωτερικής αγοράς, αντικείμενο που ήταν ο στόχος της ΕΕ σε εκείνο το στάδιο.

Λίγα χρόνια μετά, το 2001 εκδόθηκε ο Κανονισμός (ΕΕ) 2001/45, ο οποίος αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα από όργανα και οργανισμούς της Ε.Ε. Ο κανονισμός αυτός ακολουθούσε τις ίδιες βασικές αρχές.

Εξειδίκευση της νομοθεσίας για τα προσωπικά δεδομένα αποτέλεσε η οδηγία 97/66/ΕΚ η οποία πολύ γρήγορα, εντός πέντε ετών, αντικαταστάθηκε από την οδηγία 2002/58/ΕΚ [11] σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, τη λεγόμενη οδηγία «e-Privacy». Η οδηγία αυτή, η οποία ισχύει και σήμερα (μετά από τροποποίησή της με την Οδηγία 2009/136/ΕΚ [12]), αποτελεί lex-specialis νομοθετικό κείμενο, εισάγοντας ειδικούς κανόνες για την προστασία των προσωπικών δεδομένων και του απορρήτου των επικοινωνιών, οι οποίοι εφαρμόζονται από παρόχους υπηρεσιών ηλεκτρονικής επικοινωνίας.

### 2.2.3 Η ανάγκη για τροποποίηση της οδηγίας 95/46/ΕΚ

Αν και η οδηγία του 1995 είχε σκοπό την εναρμόνιση του θεσμικού πλαισίου των Κ-Μ και ένα αυξημένο επίπεδο προστασίας δικαιωμάτων, στην πράξη μεταφέρθηκε με διαφορετικό τρόπο σε κάθε Κ-Μ. Οι βασικοί κανόνες ήταν μεν κοινοί, αλλά σε κάθε κράτος υπήρχαν ορισμοί που διέφεραν και κανόνες που ερμηνεύτηκαν διαφορετικά στις εθνικές νομοθεσίες. Η υποχρέωση της οδηγίας να εξασφαλιστεί ένα ελάχιστον μεν αλλά υψηλό επίπεδο προστασίας οδήγησε κάποια Κ-Μ σε εισαγωγή μεγαλύτερων περιορισμών, ενώ άλλα Κ-Μ προτιμούσαν περισσότερο ανοιχτούς για την αγορά κανόνες. Επίσης, τα επίπεδα επιβολής της νομοθεσίας και η βαρύτητα των κυρώσεων διέφεραν αρκετά. Το πιο σημαντικό είναι ότι από το χρόνο κατάρτισης της οδηγίας, στα μέσα της δεκαετίας του 1990, είχαν συντελεστεί σημαντικές αλλαγές στην τεχνολογία των πληροφοριών. Στα τέλη της δεκαετίας του 2010 η αγορά όδευε ολοένα και σε περισσότερο παγκοσμιοποιημένη οικονομία. Οι μικρές ή μεγάλες



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

διαφοροποιήσεις στα Κ-Μ δυσχέραιναν πολύ τη διασυνοριακή λειτουργία των επιχειρήσεων και έκαναν την ενιαία αγορά πρακτικά πολύ δύσκολη. Όλοι αυτοί οι λόγοι κατέστησαν αναγκαία τη μεταρρύθμιση της νομοθεσίας της ΕΕ για την προστασία των προσωπικών δεδομένων. Η συνθήκη της Λισαβόνας, με την οποία μάλιστα δόθηκε η δυνατότητα στην ΕΕ να νομοθετήσει και για τα ζητήματα αστυνομικής και δικαστικής συνεργασία, έδωσε την ευκαιρία για μια ευρεία αναθεώρηση του θεσμικού πλαισίου.

## 2.3 Το Ελληνικό θεσμικό πλαίσιο έως το ΓΚΠΔ

### 2.3.1 Ο ν. 2472/1997 – πρώτος νόμος για τα προσωπικά δεδομένα στην Ελλάδα

Η Ελλάδα, μέχρι και το 1997 είχε ένα ατελές πλαίσιο προστασίας προσωπικών δεδομένων. Η χώρα μας είχε κυρώσει από το 1992 τη σύμβαση 108 του Συμβουλίου της Ευρώπης, η οποία άρχισε να ισχύει από το 1995, αλλά χωρίς να εφαρμόζεται στην πράξη. Η βασική αλλαγή έγινε με την εισαγωγή του ν. 2472/1997 [13] «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (ΦΕΚ Α 50/10.04.1997). Με το νόμο αυτό ενσωματώθηκε στην ελληνική έννομη τάξη η οδηγία 95/46/ΕΚ. Ο νόμος δεν είχε άμεση συνταγματική αναφορά, αλλά υποστηρίζεται ότι μπορούσε να στηριχθεί στα άρθρα 2§1, 5§1, 9§1 και 19 του Συντάγματος του 1975 με τις τροποποιήσεις του 1986. Από το 1997 και μετά ξεκίνησε και η λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) ως ανεξάρτητης αρχής (αλλά ακόμα χωρίς άμεση συνταγματική θεμελίωση της ανεξαρτησίας της).

Όπως ήταν αναμενόμενο, ο νόμος ακολουθούσε σε μεγάλο βαθμό την οδηγία 95/46/ΕΚ, εισάγοντας όμως νέες ειδικότερες έννοιες που εμφανίστηκαν μόνο στην Ελλάδα, όπως η «διασύνδεση» αρχείων αλλά χωρίς να αξιοποιήσει όλες τις ευελιξίες που άφηνε η οδηγία. Χαρακτηριστικό είναι ότι στο αρχικό πλαίσιο προστασίας δεδομένων της ΕΕ προβλεπόταν, ως μέτρο πρόληψης των δραστηριοτήτων επεξεργασίας δεδομένων, η γνωστοποίηση στις εποπτικές αρχές των δραστηριοτήτων αυτών και η αδειοδότηση όσων ενείχαν επεξεργασία ευαίσθητων δεδομένων. Καθώς η αρχική έκδοση του ν. 2472/1997 είχε ελάχιστες εξαιρέσεις από τις υποχρεώσεις



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

γνωστοποίησης και άδειας, όλες οι επιχειρήσεις, ακόμα και οι πιο μικρές, είχαν τη γραφειοκρατική υποχρέωση να γνωστοποιήσουν στην Αρχή Προστασίας Δεδομένων ακόμα και τις πιο τυπικές τους δραστηριότητες (π.χ. αρχεία προσωπικού και πελατών). Αυτό οδήγησε στην υποβολή εκατοντάδων χιλιάδων γνωστοποιήσεων αρχείου έως το 1999. Φυσικά ο νόμος τροποποιήθηκε ώστε να εξαιρούνται από την υποχρέωση γνωστοποίησης οι τυπικές δραστηριότητες.

### 2.3.2 Το άρθρο 9Α του Συντάγματος

Η λειτουργία της νομοθεσίας για τα προσωπικά δεδομένα, ακόμα και μετά την ψήφιση του ν. 2472/1997 είχε δεχθεί αμφισβήτηση, λόγω της μη ρητής συνταγματικής κατοχύρωσης. Παράλληλα, ακόμα μεγαλύτερη αμφισβήτηση είχε δεχθεί η θεσμική κατοχύρωση της Αρχής Προστασίας Δεδομένων ως Ανεξάρτητης Αρχής. Για πολλούς, η έννοια της Ανεξάρτητης Αρχής, δηλαδή μιας δημόσιας αρχής μη ελεγχόμενης από την κλασική εκτελεστική εξουσία (κυβέρνηση), η οποία ήταν μάλιστα σε θέση να ελέγχει ως ένα βαθμό, δομές της εκτελεστικής εξουσίας, ήταν ξένη προς το Ελληνικό Σύνταγμα.

Η συζήτηση αυτή τελείωσε το 2001 με την αναθεώρηση του Συντάγματος, όταν και προστέθηκε το άρθρο $9^{Α}$ για την προστασία των προσωπικών δεδομένων. Μάλιστα, με τον τρόπο αυτό, η προστασία των προσωπικών δεδομένων έγινε ευρύτερη των υποχρεώσεων της οδηγίας, καθώς η εφαρμογή του εθνικού νόμου δεν περιοριζόταν σε όσα θέματα μπορεί να ρυθμίσει το δίκαιο της ΕΕ, αλλά ακόμα και σε αυτά που είναι εκτός του πεδίου του εφαρμογής, όπως η εθνική ασφάλεια. Ήδη στο ν. 2472/1997 προβλεπόταν η δυνατότητα της ΑΠΔΠΧ, υπό αυστηρές προϋποθέσεις (π.χ. παρουσία του προέδρου της), να ελέγχει ακόμα και την Εθνική Υπηρεσία Πληροφοριών.

**Άρθρο 9Α Συντάγματος**: Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει

Παράλληλα, με το άρθρο $101^{Α}$ του Συντάγματος κατοχυρώνεται και συνταγματικά η ανεξαρτησία της ΑΠΔΠΧ (μια από τις πέντε αρχές) ενώ καθορίζεται και ο τρόπος επιλογής τους, με αυξημένη πλειοψηφία της διάσκεψης των Προέδρων της Βουλής.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

### 2.3.3 Λοιπή σχετική νομοθεσία

Ο ν. 2472/1997 δέχθηκε, κατά καιρούς, μικρές αλλαγές, χωρίς να διαφοροποιηθούν ουσιαστικά οι βασικές του αρχές· αυτό άλλωστε θα ήταν σε αντίθεση με την οδηγία 95/46/ΕΚ. Με την πάροδο των ετών, το εθνικό δίκαιο εμπλουτίστηκε με άλλες σχετικές διατάξεις, ενώ ακολούθησε τις αλλαγές της νομοθεσίας της ΕΕ. Ειδικότερα αναφέρουμε τα εξής:

- Ν. 3471/2006 [14] «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών» Ο νόμος αυτός εναρμόνισε το εθνικό δίκαιο με την οδηγία «ePrivacy» 2002/58/ΕΚ. Αντικατέστησε το ν. 2774/1999. Ο νόμος αυτός ισχύει έως σήμερα με διάφορες τροποποιήσεις, οι βασικότερες των οποίων έχουν επέλθει με το ν. 4070/2012 βάσει της οδηγίας 2009/136/ΕΚ. Διατάξεις του νόμου αυτού αναλύονται στην Ενότητα 13.
- Ν. 3917/2011 «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών (εναρμόνιση με 2006/24/ΕΚ), χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις». Ο νόμος αυτός, στο πρώτο του μέρος, μεταφέρει στο εθνικό δίκαιο την οδηγία 2006/24/ΕΚ, η οποία εν τω μεταξύ έχει ακυρωθεί από το ΔΕΕ, χωρίς όμως να έχουν ακυρωθεί και οι σχετικοί εθνικοί νόμοι. Στο άρθρο 14 του νόμου, εισήχθη ειδικό άρθρο, κατόπιν γνωμοδότησης της ΑΠΔΠΧ, για την ορθή λειτουργία συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους, με το οποίο οριοθετήθηκε η χρήση καμερών από δημόσιες αρχές. Σχετική συζήτηση γίνεται και στην Ενότητα 14.

## 2.4 Το αναθεωρημένο πλαίσιο προστασίας δεδομένων στην Ελλάδα

Το Μάιο του 2016 εγκρίθηκε στην ΕΕ μια δέσμη νομοθετικών μέτρων για την προστασία δεδομένων που φιλοδοξούν να προετοιμάσουν την Ευρώπη για την ψηφιακή εποχή. Η δέσμη αυτή περιλαμβάνει δύο βασικά εργαλεία, τον Κανονισμό (ΕΕ) 2016/679 και την Οδηγία (ΕΕ) 2016/680.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

### 2.4.1 Γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ)

Ο «Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)» έγινε πολύ γρήγορα γνωστός σε όλο τον κόσμο ως GDPR (General Data Protection Regulation). Αποτελεί ένα ουσιαστικό βήμα για την ενίσχυση των θεμελιωδών δικαιωμάτων των προσώπων και για τη διευκόλυνση της επιχειρηματικής δραστηριότητας με τη διευκρίνιση των κανόνων για τις επιχειρήσεις και τους δημόσιους φορείς στην ενιαία ψηφιακή αγορά. Προσπαθεί να αντιμετωπίσει τον κατακερματισμό στα διάφορα εθνικά νομοθετικά συστήματα με τις διαδικασίες συνεκτικότητας αλλά και τον περιττό διοικητικό φόρτο, με κατάργηση διαδικασιών όπως οι γνωστοποιήσεις. Η εισαγωγή της αρχής της λογοδοσίας, μεταφέρει πλέον μεγάλο βάρος απόδειξης της νομιμότητας, προληπτικά, στις εταιρείες και τους δημόσιους φορείς. Παράλληλα, είναι σχεδιασμένος με τρόπο που εκτιμάται ότι θα αντέξει περισσότερο στις μελλοντικές τεχνολογικές αλλαγές. Ο κανονισμός ενσωματώθηκε και στη συμφωνία με τον ΕΟΧ ώστε να εφαρμόζεται και από τις τρεις χώρες της που δεν είναι μέλη της ΕΕ (Νορβηγία, Ισλανδία, Λιχτενστάιν).

Ως κανονισμός, ξεκίνησε να ισχύει άμεσα σε όλα τα ΚΜ από τις 25/5/2016, αλλά δόθηκε σε όλους τους φορείς ένα διάστημα προσαρμογής. Ο ΓΚΠΔ χαρακτηρίστηκε μερικές φορές ως κανονισμοδηγία. Τα ΚΜ έπρεπε, το αργότερο έως την ημερομηνία εφαρμογής του, να εισάγουν στο εσωτερικό τους δίκαιο ορισμένα μέτρα για την εφαρμογή του (π.χ. να ορίσουν την αρμόδια εθνική αρχή) ενώ σε λίγα συγκεκριμένα άρθρα του έχει δοθεί ευελιξία στα ΚΜ να διαφοροποιηθούν ως ένα βαθμό ή να προσδιορίσουν ειδικότερους κανόνες για συγκεκριμένες επεξεργασίες. Στις 25/5/2018 ο ΓΚΠΔ τέθηκε σε εφαρμογή, ακόμα κι αν ένα ΚΜ (όπως η Ελλάδα) δεν είχε ολοκληρώσει την εφαρμογή του με εθνικό νόμο.

### 2.4.2 Οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου

Το «αδελφάκι» του ΓΚΠΔ είναι η Οδηγία (ΕΕ) 2016/680 [15]. Η οδηγία αυτή, προστατεύει το θεμελιώδες δικαίωμα των πολιτών για την προστασία των δεδομένων,



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

όταν αυτά χρησιμοποιούνται από αρχές επιβολής του ποινικού δικαίου για σκοπούς επιβολής του νόμου (πολλές φορές αναφέρεται καταχρηστικά ως «αστυνομική» οδηγία), όπως η Αστυνομία, το Λιμενικό ή και η Πυροσβεστική, όταν το αντικείμενό τους είναι η δίωξη εγκλημάτων. Διασφαλίζει την προστασία των προσωπικών δεδομένων θυμάτων, μαρτύρων και υπόπτων εγκληματικών πράξεων και διευκολύνει τη διασυνοριακή συνεργασία για την καταπολέμηση του εγκλήματος και της τρομοκρατίας. Οι διατάξεις της οδηγίας ακολουθούν σε πολύ μεγάλο βαθμό τη λογική του ΓΚΠΔ. Σε μεγάλο βαθμό οι υποχρεώσεις των υπευθύνων επεξεργασίας και τα δικαιώματα των υποκειμένων των δεδομένων είναι παρόμοια, με εξαιρέσεις που είναι κατάλληλα σχεδιασμένες για την ορθή λειτουργία των αρχών αυτών. Μάλιστα, οι περισσότερες από τις «αστυνομικές» αρχές οφείλουν να εφαρμόζουν την οδηγία 2016/680 για κάποιες από τις δραστηριότητές τους (αυτές που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας) ενώ για άλλες δραστηριότητες (αυτές που είναι διοικητικής φύσης, συμπεριλαμβανομένων των διοικητικών κυρώσεων) εφαρμόζουν το ΓΚΠΔ.

Η οδηγία τέθηκε σε ισχύ στις 5 Μαΐου 2016 και τα ΚΜ όφειλαν να τη μεταφέρουν στο εθνικό τους δίκαιο έως τις 6 Μαΐου 2018. Η Ελλάδα καθυστέρησε πάνω από ένα έτος στη μεταφορά της οδηγίας.

### 2.4.3 Η εφαρμογή του αναθεωρημένου πλαισίου στην Ελλάδα – ν. 4624/2019

Με τον ν. 4624/2019 (ΦΕΚ Α'137/29.8.2019 [16]) «*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις*» ελήφθησαν τα απαραίτητα μέτρα εφαρμογής του ΓΚΠΔ και παράλληλα ενσωματώθηκε στην εθνική νομοθεσία η Οδηγία 2016/680.

Για τη ενσωμάτωση των δύο ευρωπαϊκών κειμένων δημιουργήθηκε νομοπαρασκευαστική επιτροπή, οι εργασίες της οποίας διήρκεσαν μεγάλο χρονικό διάστημα. Τελικά, και υπό την απειλή προστίμου από την ΕΕ λόγω μη ενσωμάτωσης της οδηγίας 2016/680, ο νόμος 4624/2019 ψηφίστηκε τον Αύγουστο του 2019 με τη



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

διαδικασία του επείγοντος. Μετά την έκδοσή του, η ΑΠΔΠΧ (η οποία δεν είχε προλάβει να γνωμοδοτήσει για το τελικό σχέδιο του νόμου, παρά μόνο άτυπα και σε ενδιάμεσες εκδόσεις του που διέφεραν από την τελική [17]) εξέδωσε αναλυτική γνωμοδότηση [18] με την οποία άσκησε κριτική σε αρκετές διατάξεις του νόμου. Η Αρχή επεσήμανε ότι κατά την εφαρμογή του νόμου από αυτή δεν θα τύχουν εφαρμογής κατά την άσκηση των αρμοδιοτήτων της διατάξεις του ν. 4624/2019, οι οποίες θα κριθούν ότι έρχονται σε αντίθεση με τον ΓΚΠΔ ή δεν βρίσκουν έρεισμα σε «ρήτρες ανοίγματος – εξειδίκευσης» ενώ έκανε πλείστες παρατηρήσεις για μη ορθή ενσωμάτωση σε διάφορα άρθρα του νόμου. Κάποια από τα βασικά σημεία κριτικής είναι η μη δυνατότητα δημιουργίας «εθνικής νομικής βάσης» για επεξεργασίες δεδομένων προσωπικού χαρακτήρα, η μη ορθή εξειδίκευση κανόνων για την προστασία των εργαζομένων, οι εκτεταμένοι περιορισμοί των δικαιωμάτων των υποκειμένων χωρίς να ορίζονται συγκεκριμένες ρυθμίσεις διασφάλισης (όπως απαιτεί ο ΓΚΠΔ), η απουσία ρύθμισης για τα δικαστήρια, η εξαίρεση της εθνικής ασφάλειας (ζήτημα που δεν μπορεί να ρυθμίσει το δίκαιο της ΕΕ, αλλά απορρέει από το Σύνταγμα), οι ευρύτατες εξαιρέσεις σε σχέση με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς, η εισαγωγή της συγκατάθεσης ως νομικής βάσης για τους σκοπούς της οδηγίας 2016/680 κ.α.

Πρακτικά, αυτό σημαίνει ότι **ένας δημόσιος φορέας που δρα ως υπεύθυνος επεξεργασίας, οφείλει, κατ' αρχήν, να ανατρέχει στις ρυθμίσεις του ΓΚΠΔ και να χρησιμοποιεί τις διατάξεις του ν. 4624/2019 μόνο όταν είναι ξεκάθαρο ότι ο εθνικός αυτός νόμος δε βρίσκεται σε σύγκρουση με το ΓΚΠΔ.**

Επομένως, το σημερινό (αρχές 2022) θεσμικό πλαίσιο για την προστασία των προσωπικών δεδομένων στην Ελλάδα περιλαμβάνει:

- Το ΓΚΠΔ (Κανονισμός (ΕΕ) 2016/679) [1]
- Το ν. 4624/2019 [16] ο οποίος εφαρμόζεται:
    i. Για τους σκοπούς της «αστυνομικής» οδηγίας 2016/680 [15] (κεφάλαιο Δ του νόμου) και
    ii. Σε όσες περιπτώσεις ο ΓΚΠΔ προβλέπει ρήτρες ανοίγματος ή εξειδίκευσης (δηλαδή δίνει τη δυνατότητα στα Κ-Μ να νομοθετήσουν)
- Το ν. 3471/2006 (με τις τροποποιήσεις του) [14] που εφαρμόζεται στην



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επεξεργασία δεδομένων προσωπικού χαρακτήρα από παρόχους υπηρεσιών ηλεκτρονικής επικοινωνίας (και του οποίου οι διατάξεις επηρεάζουν τους φορείς του δημοσίου σε λίγες, καθορισμένες περιπτώσεις).

Τα ανωτέρω ισχύουν τόσο για δημόσιο όσο και για ιδιωτικό τομέα. Στη συνέχεια αναλύουμε τις βασικές διατάξεις του ανωτέρω θεσμικού πλαισίου, με κύριο προσανατολισμό στο δημόσιο τομέα (αν και πολλά ζητήματα ισχύουν αυτούσια και για τον ιδιωτικό τομέα). Μάλιστα, το άρθρο 4 στοιχ. α' του ν. 4624/2019 ορίζει τους δημόσιους φορείς ως «*οι δημόσιες αρχές, οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, τα νομικά πρόσωπα δημοσίου δικαίου, οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δεύτερου βαθμού και τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό*».

## 2.5 Βιβλιογραφία για περισσότερη μελέτη

- Πολιτική και Δίκαιο, Β΄ Γενικού Λυκείου, Καλλιόπη Παπακωνσταντίνου, Λεωνίδας Κατσίρας [19]
- T4DATA Project - The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation - Douwe Korff and Marie Georges [20]
- Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης (FRA - CoE) – Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων (έκδοση 2018) [21]
- Βασίλης Σωτηρόπουλος - Το άρθρο 9Α του Συντάγματος 1975/1986/2001 [22]



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 3. Ο ΓΚΠΔ: Στόχος και πεδίο εφαρμογής

Ο ΓΚΠΔ είναι ένα νομοθετικό κείμενο με ιδιαίτερη ορολογία. Κατά τη διάρκεια των ετών μετά την έναρξη εφαρμογής της Οδηγίας 95/46/ΕΚ έχουν παγιωθεί οι βασικές έννοιες και οι βασικοί ορισμοί της νομοθεσίας για τα προσωπικά δεδομένα. Οι ορισμοί αυτοί μπορεί να διαφέρουν από τη νομοθεσία άλλων φορέων. Πριν λοιπόν αρχίσουμε να αναλύουμε τη νομοθεσία, ας προσπαθήσουμε να κατανοήσουμε τις βασικές της έννοιες. Με τον τρόπο αυτό θα είμαστε σε θέση να ερμηνεύσουμε το ρόλο ενός φορέα του δημοσίου (αλλά και ιδιωτικού) τομέα στο «οικοσύστημα» μιας επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Οι ορισμοί που θα αναλύσουμε περιέχονται, κυρίως, στο άρθρο 4 του ΓΚΠΔ.

## 3.1 Τι είναι Δεδομένα Προσωπικού Χαρακτήρα;

Ο ορισμός του ΓΚΠΔ για τα δεδομένα προσωπικού χαρακτήρα (τα οποία συχνά, στην καθομιλουμένη, αποκαλούνται απλά «προσωπικά δεδομένα») είναι: «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*»

Ο ορισμός είναι πάρα πολύ ευρύς αλλά πάρα πολύ εύκολο να γίνει κατανοητός. Για να αποτελεί μία πληροφορία προσωπικό δεδομένο, θα πρέπει να ισχύουν τα εξής:

- Να είναι πληροφορία, ανεξαρτήτως είδους, που…
- αναφέρεται (μπορεί να αποδοθεί), έμμεσα ή άμεσα,
- σε ένα φυσικό πρόσωπο[2].

Πρακτικά αυτό σημαίνει ότι στην ευρωπαϊκή νομοθεσία, κάθε πληροφορία που σχετίζεται με έναν άνθρωπο εν ζωή, καλύπτεται κατ' αρχήν από το θεσμικό πλαίσιο προστασίας προσωπικών δεδομένων. Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, αν δηλαδή μια πληροφορία μπορεί άμεσα ή έμμεσα να αποδοθεί

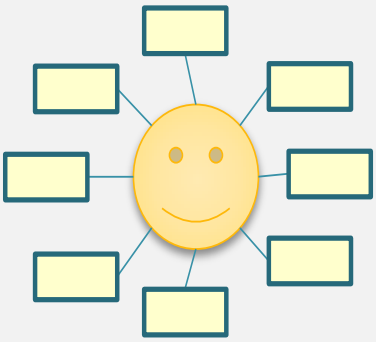
[2] Φυσικό πρόσωπο: άνθρωπος εν ζωή. Ο ορισμός δεν καλύπτει θανόντες.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σε ένα άνθρωπο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Μάλιστα, δεν έχει σημασία αν τα μέσα αυτά είναι στη διάθεση του κατόχου των πληροφοριών. Έμμεση ταυτοποίηση μπορεί να γίνει και με διασταύρωση με άλλες γνωστές πηγές.

**Παράδειγμα:** Σε μια βάση δεδομένων ενός Υπουργείου, κάθε τιμή (όρισμα) μιας οντότητας που αντιστοιχεί σε έναν άνθρωπο (π.χ. σε ένα πολίτη) είναι προσωπικό δεδομένο (π.χ. ονοματεπώνυμο, ΑΦΜ, ΑΜΚΑ, ημερομηνία γέννησης κ.α.). Προσωπικό δεδομένο όμως αποτελεί και κάθε άλλη τιμή, η οποία αντιστοιχεί σε άλλη οντότητα, αν μέσω ερωτημάτων ή μέσω διασύνδεσης –ακόμα και με άλλες βάσεις δεδομένων-, αυτή η τιμή μπορεί να συσχετισθεί με ένα άνθρωπο (π.χ. αν υπάρχει πίνακας σε έναν οργανισμό με τους ακριβείς μισθούς ανά κατηγορία υπαλλήλου και χρόνια προϋπηρεσίας, ενώ ταυτόχρονα σε άλλον πίνακα με στοιχεία του προσωπικού καταγράφεται, για κάθε υπάλληλο ονομαστικά, τόσο η κατηγορία του όσο και η προϋπηρεσία του: συνδυασμός των δύο πινάκων επιτρέπει τον προσδιορισμό του μισθού για τον κάθε υπάλληλο).



Ο Κανονισμός δίνει ενδεικτικά παραδείγματα για μερικές κατηγορίες προσωπικών δεδομένων, θέλοντας να δώσει έμφαση σε ορισμένες πληροφορίες. Τέτοια π.χ. είναι τα αναγνωριστικά στοιχεία ταυτότητας, τα δεδομένα της θέσης ενός προσώπου (π.χ. από το GPS του κινητού μας), τα επιγραμμικά (online) αναγνωριστικά ταυτότητας (π.χ. email, ονόματα χρήστη υπηρεσιών, IP διευθύνσεις) και παράγοντες που αφορούν κάθε μα κάθε πτυχή της δραστηριότητας ενός ανθρώπου. Σήμερα, με την αύξηση της χρήσης «έξυπνων» ηλεκτρονικών συσκευών, κάθε μια τέτοια συσκευή παράγει πληροφορίες, οι οποίες είναι πολύ πιθανό να μπορούν να συνδεθούν με τον



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ιδιοκτήτη ή το χρήστη τους. Παραδείγματα προσωπικών δεδομένων είναι οι καταγραφές συνομιλιών για απόδειξη συναλλαγών, οι εικόνες από κάμερες για την εξακρίβωση των προσώπων που έχουν διαπράξει μια πράξη ή παράβαση, γραπτά ή σχέδια ενός παιδιού, οι πληροφορίες συντήρησης ενός ιδιωτικού αυτοκινήτου, οι αξιολογήσεις ενός δημοσίου υπαλλήλου, το προσωπικό του μητρώο κ.ά. Όλες αυτές οι πληροφορίες, είναι προσωπικά δεδομένα.

Εξαιρούνται από την έννοια των προσωπικών δεδομένων τα ανώνυμα δεδομένα, αυτά δηλαδή τα οποία δεν μπορεί (πλέον) να συνδεθούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Περαιτέρω ανάλυση της έννοιας των ανώνυμων δεδομένων αλλά και των ψευδώνυμων δεδομένων (τα οποία όμως αποτελούν προσωπικά) θα βρείτε στην Ενότητα 15.

Προφανώς, ο παραπάνω ορισμός, δεν περιλαμβάνει νομικά πρόσωπα. Συνεπώς, οι πληροφορίες που αφορούν ένα νομικό πρόσωπο δεν εμπίπτουν στο προστατευτικό πλαίσιο του ΓΚΠΔ. Βέβαια, αυτό δεν σημαίνει ότι δεν μπορεί να προστατεύονται από άλλες διατάξεις απορρήτου (π.χ. τραπεζικό ή φορολογικό) ή ότι δεν μπορεί να υπάρχουν ειδικές ρυθμίσεις ως προς αυτές (π.χ. όταν ένα νομικό πρόσωπο συμβάλλεται με πάροχο υπηρεσίας ηλεκτρονικής επικοινωνίας). Προσοχή: οι πληροφορίες σχετικά με την επαγγελματική δραστηριότητα ενός φυσικού προσώπου, αν και φορολογικά μπορεί να έχουν την ίδια μεταχείριση με αυτές ενός νομικού προσώπου, αποτελούν (και) προσωπικά δεδομένα του εν λόγω φυσικού προσώπου.

☞ **Ως κατακλείδα**: Σχεδόν κάθε πληροφορία μπορεί να είναι προσωπικό δεδομένο. Είναι όμως μεγάλο λάθος να θεωρούμε ότι δεν επιτρέπεται να τη χρησιμοποιήσουμε. Αν εξασφαλίσουμε ότι την επεξεργαζόμαστε νόμιμα, δεν υπάρχει εμπόδιο.

**Ερώτηση δραστηριότητας**: Σε υπόθεσή του[3] το ΔΕΕ εξέτασε αν οι δυναμικές διευθύνσεις IP, οι οποίες αλλάζουν κάθε φορά που πραγματοποιείται νέα σύνδεση στο διαδίκτυο, αποτελούν προσωπικά δεδομένα. Μια ιστοσελίδα κατέγραφε και

[3] ΔΕΕ, C-582/14, Patrick Breyer κατά Bundesrepublik Deutschland
**https://curia.europa.eu/juris/liste.jsf?language=el&jur=C,T,F&num=C-582/14&td=ALL**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αποθήκευε δυναμικές διευθύνσεις IP για την πρόληψη κυβερνοεπιθέσεων. Όμως, μόνο ο πάροχος υπηρεσιών διαδικτύου διέθετε τις συμπληρωματικές πληροφορίες που ήταν αναγκαίες για την εξακρίβωση της ταυτότητάς του. Με παρόμοιο τρόπο λειτουργούν πολλές ιστοσελίδες σήμερα. Ο διαχειριστής της ιστοσελίδας, δεν μπορεί να γνωρίζει σε ποιο πρόσωπο αντιστοιχεί μια IP διεύθυνση. Το ΔΕΕ όμως έκρινε ότι αποτελεί προσωπικό δεδομένο. Γιατί; Αιτιολογήστε.

Δείτε το σύνδεσμο ή ανατρέψτε στο εγχειρίδιο του FRA [21] (σελ 117-118) για να δείτε το σκεπτικό του δικαστηρίου.

### 3.1.1 Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

Στο πλαίσιο του Ευρωπαϊκού δικαίου υπάρχουν κάποιες (ειδικές) κατηγορίες δεδομένων προσωπικού χαρακτήρα οι οποίες, εκ φύσεως, ενδέχεται να ενέχουν μεγαλύτερο κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όταν υποβάλλονται σε επεξεργασία. Τα δεδομένα αυτά **σχετίζονται ιδίως με τον πυρήνα της προσωπικότητας ενός ατόμου** και είναι αυτά που παλαιότερα ήταν γνωστά ως «ευαίσθητα προσωπικά δεδομένα» (εξ αυτού, ο παλαιότερος αυτός όρος ενίοτε χρησιμοποιείται και σήμερα). Αυτά τα δεδομένα είναι:

- Αυτά που αποκαλύπτουν τη **φυλετική ή εθνοτική καταγωγή**. Προσοχή, δεν πρέπει να συγχέονται με την υπηκοότητα (ιθαγένεια) ενός προσώπου, η οποία αποτελεί (απλό) δεδομένο ταυτότητα. Τέτοια π.χ. μπορεί να είναι η ένταξη σε μειονότητες ή συγκεκριμένη εθνική καταγωγή Έλληνα υπηκόου.
- Αυτά που αποκαλύπτουν **πολιτικά φρονήματα, θρησκευτικές ή άλλες πεποιθήσεις**, συμπεριλαμβανομένων των **φιλοσοφικών πεποιθήσεων**. Τέτοια μπορεί να είναι η ένταξη σε πολιτικό κόμμα, οι πολιτικές απόψεις ενός ανθρώπου, η θρησκεία του και η συμμετοχή του σε θρησκευτικές ή πολιτικές δραστηριότητες,
- Αυτά που αποκαλύπτουν τη συμμετοχή ενός ατόμου σε **συνδικαλιστική οργάνωση**. Από την άλλη πλευρά, η υποχρεωτική συμμετοχή σε ΝΠΔΔ που έχει και συνδικαλιστικό χαρακτήρα (Π.χ. Τεχνικό ή Οικονομικό Επιμελητήριο, Δικηγορικός ή Ιατρικός Σύλλογος) δεν αποτελεί ειδικές κατηγορίες δεδομένων.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

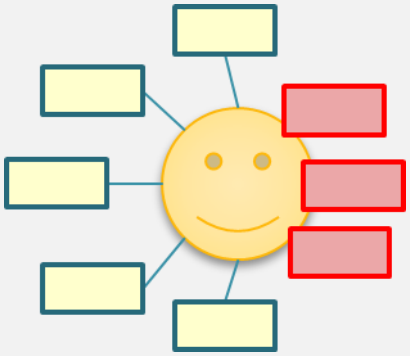
- Αυτά που αφορούν την **υγεία, τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό**. Σε αυτά περιλαμβάνονται τα δεδομένα ασθενειών, αναπηριών, σωματικής και ψυχικής υγείας.
- Τα **γενετικά δεδομένα**, δηλαδή οι πληροφορίες του DNA ενός ατόμου. Αυτές προκύπτουν, συνήθως, από ανάλυση βιολογικού δείγματος και παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού ατόμου.
- Τα **βιομετρικά δεδομένα** τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση.

Τα παραπάνω δεδομένα αυτά υπόκεινται σε ειδικό χειρισμό και οι προϋποθέσεις υπό τις οποίες η επεξεργασία τους είναι νόμιμη είναι περιορισμένες.

Μια ξεχωριστή κατηγορία ειδικών δεδομένων είναι αυτά που αφορούν ποινικές καταδίκες και αδικήματα. Τέτοια π.χ. είναι οι πληροφορίες του ποινικού μητρώου. Η δυνατότητα επεξεργασίας αυτών των κατηγοριών δεδομένων είναι ακόμα πιο περιορισμένη.

Μερικές φορές, για να περιγράψουμε δεδομένα προσωπικού χαρακτήρα που δεν ανήκουν στις παραπάνω ειδικές κατηγορίες, χρησιμοποιούμε καταχρηστικά τον όρο «απλά» προσωπικά δεδομένα, ως αντίθεση.

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα είναι αυτές που σχετίζονται με τον πυρήνα της προσωπικότητας ενός ατόμου.



☞ Πολλοί συνηθίζουν να χρησιμοποιούν τον όρο «ευαίσθητα δεδομένα» για



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

οποιαδήποτε πληροφορία θεωρούν, με το δικό τους υποκειμενικό κριτήριο, ότι είναι ιδιαίτερα σημαντική – π.χ. τα στοιχεία φορολογικής δήλωσης ή ακόμα και ο ίδιος ο ΑΦΜ. Αυτό δεν είναι ακριβές, σύμφωνα με τα ανωτέρω: τούτο βέβαια δεν σημαίνει ότι τα «απλά» (μη ευαίσθητα) δεδομένα δεν χρήζουν προστασίας.

## 3.2 Η έννοια της επεξεργασίας

Κάθε πράξη που διενεργείται σε δεδομένα προσωπικού χαρακτήρα θεωρείται «επεξεργασία» προσωπικών δεδομένων. Στην ουσία, η νομοθεσία ελέγχει ακριβώς αυτό, την επεξεργασία των προσωπικών δεδομένων, καθώς από αυτή μπορεί να προκύψουν κίνδυνοι για τα δικαιώματα και τις ελευθερίες των ατόμων. Επεξεργασία μπορεί να έχουμε είτε σε αυτοματοποιημένη μορφή (π.χ. με Η/Υ) είτε και χειροκίνητα σε διαρθρωμένα συστήματα αρχειοθέτησης. Ο ΓΚΠΔ αναφέρει ενδεικτικά περιπτώσεις που πρέπει να θεωρούμε ότι υφίσταται επεξεργασία. Τέτοιες είναι:

- Η **συλλογή**. Τέτοια είναι π.χ. όταν κάποιος καταγράφει ονόματα και διευθύνσεις κατοίκων από τα κουδούνια τους ή όταν κάποιος συλλέγει δημόσια διαθέσιμες πληροφορίες από αναζητήσεις στο διαδίκτυο.
- Η **καταχώριση**. Τέτοια είναι π.χ. όταν ένας φορέας καταχωρίζει σε βάση δεδομένων πληροφορίες τις οποίες έχει πρώτα συλλέξει.
- Η **οργάνωση**. Τέτοια είναι π.χ. όταν ένας φορέας ταξινομεί πληροφορίες που ήδη διαθέτει, ώστε να είναι ευκολότερα αναζητήσιμες.
- Η **διάρθρωση.** Τέτοια είναι π.χ. όταν κάποιος μορφοποιεί τις πληροφορίες που διαθέτει με διαφορετικό τρόπο, ώστε να συνδέονται μεταξύ τους αρμονικότερα.
- Η **αποθήκευση.** Τέτοια είναι π.χ. όταν κάποιος αποθηκεύει σε ηλεκτρονικό αρχείο πληροφορίες ή ακόμα και σε έγχαρτη μορφή.
- Η **προσαρμογή** ή η **μεταβολή.** Τέτοια είναι π.χ. όταν κάποιος τροποποιεί αποθηκευμένες πληροφορίες.
- Η **ανάκτηση.** Τέτοια είναι π.χ. όταν κάποιος ανακτά πληροφορίες οι οποίες είχαν προηγουμένως διαγραφεί.
- Η **αναζήτηση** πληροφοριών**.** Τέτοια είναι π.χ. όταν κάποιος αναζητά



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προσωπικά δεδομένα στο διαδίκτυο ή προσπαθεί να αναγνωρίσει ένα πρόσωπο σε μια καταγραφή βίντεο.

- Η **χρήση.** Τέτοια είναι π.χ. όταν ένας φορέας χρησιμοποιεί προσωπικά δεδομένα για την έκδοση μιας διοικητικής πράξης.
- Η **κοινολόγηση με διαβίβαση.** Τέτοια είναι π.χ. όταν ένας φορέας αποστέλλει ένα έγγραφο που περιέχει προσωπικά δεδομένα σε περιορισμένο αριθμό (γνωστών) αποδεκτών.
- Η **διάδοση** ή **κάθε άλλη μορφή διάθεσης.** Τέτοια είναι π.χ. όταν ένας φορέας αναρτά ένα έγγραφο που περιέχει προσωπικά δεδομένα στο διαδίκτυο.
- Η **συσχέτιση** ή ο **συνδυασμός.** Τέτοια είναι π.χ. όταν ένας φορέας συνδυάζει πληροφορίες που διαθέτει σε διαφορετικά μητρώα ή αρχεία, για την έκδοση μιας διοικητικής πράξης.
- Ο **περιορισμός**. Τέτοια είναι π.χ. όταν ένας φορέας επισημαίνει κάποιες πληροφορίες ως εμπίπτουσες σε ειδικό απόρρητο, ώστε να περιοριστεί η χρήση τους ή όταν ενώ θα έπρεπε να διαγράψει τις πληροφορίες, τις τηρεί σε ειδικό αρχείο για νομικούς λόγους.
- Η **διαγραφή** ή η **καταστροφή** δεδομένων**.**

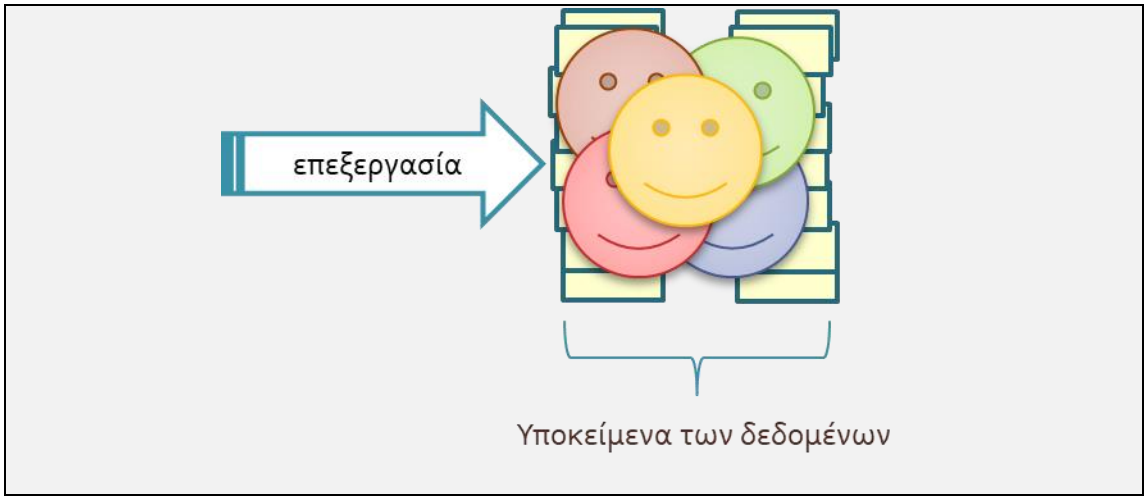
☞ **Υποκείμενο των δεδομένων (data subject)**: Τα φυσικά πρόσωπα των οποίων τα δεδομένα υφίστανται επεξεργασία ονομάζονται «υποκείμενα των δεδομένων»

Ο ορισμός αυτός, αν και μπορεί να μην είναι τόσο εύηχος, είναι απόλυτα ακριβής γραμματικά. Το υποκείμενο των δεδομένων είναι ο φορέας των δικαιωμάτων του ΓΚΠΔ.

Η νομοθεσία για τα προσωπικά δεδομένα *επεμβαίνει* στο στάδιο της «επεξεργασίας» και επιβάλλει να ελέγχεται η νομιμότητα κάθε πράξης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης




### 3.3 Οι Ρόλοι: Υπεύθυνος Επεξεργασίας - Εκτελών την Επεξεργασία

Για την κατανόηση των ρυθμίσεων για την προστασία προσωπικών δεδομένων, είναι κρίσιμο να κατανοήσουμε ποιοι είναι αυτοί που έχουν την ευθύνη, έναντι της νομοθεσίας αυτής αλλά και έναντι των δικαιωμάτων των υποκειμένων των δεδομένων. Μόνο έτσι είναι δυνατό να αποδοθούν ευθύνες για πράξεις ή παραλείψεις σε σχέση με μια επεξεργασία προσωπικών δεδομένων. Επίσης, ένα υποκείμενο των δεδομένων διαθέτει δικαιώματα τα οποία πρέπει να είναι σε θέση να ασκεί προς τον εκάστοτε αρμόδιο. Οι ρόλοι του «Υπεύθυνου Επεξεργασίας» (data controller) και του «Εκτελούντος την Επεξεργασία» (data processor) καθορίζονται ρητά στο άρθρο 4 του ΓΚΠΔ και λειτουργούν με τον ίδιο τρόπο σε όλο το φάσμα της νομοθεσίας για τα προσωπικά δεδομένα στην Ε.Ε. και το Συμβούλιο της Ευρώπης.

Με βάση αυτούς τους ρόλους καθορίζεται ποιος είναι υπεύθυνος:

- για τη **συμμόρφωση** με διαφορετικούς κανόνες προστασίας δεδομένων
- για τον τρόπο με τον οποίο τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα **δικαιώματά** τους

Πέραν από τους δύο αυτούς ρόλους, ο ΓΚΠΔ αναφέρει επίσης ως (διαφορετικού τύπου) ρόλους τον «Αποδέκτη» και τον «Τρίτο» ανάλογα με τη συμμετοχή τους ή όχι σε μια επεξεργασία.

Οι έννοιες αυτές είναι λειτουργικές έννοιες. Δηλαδή δεν αρκεί να ορίζονται τυπικά σε κείμενο(π.χ. σε ένα νόμο ή σε μια πολιτική προστασίας δεδομένων) αλλά να αντιστοιχούν και με την πρακτική που ακολουθείται κατά την επεξεργασία δεδομένων.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

### 3.3.1 Ο Υπεύθυνος της επεξεργασίας

Ο Υπεύθυνος Επεξεργασίας είναι ίσως ο βασικότερος ρόλος για την προστασία προσωπικών δεδομένων και είναι αυτός που **καθορίζει** τα ουσιώδη χαρακτηριστικά της και ευθύνεται, στο μεγαλύτερο βαθμό, για τη συμμόρφωση με τη νομοθεσία.

Ο ορισμός του ΓΚΠΔ για τον Υπεύθυνο Επεξεργασίας αναφέρει: «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους*». Η έννοια του υπευθύνου της επεξεργασίας είναι αυτόνομη, υπό την έννοια ότι πρέπει να ερμηνεύεται κυρίως σύμφωνα με το κοινοτικό δίκαιο για την προστασία των δεδομένων, και λειτουργική, υπό την έννοια ότι προορίζεται να κατανείμει αρμοδιότητες εκεί όπου βρίσκεται η πραγματολογική επιρροή και, επομένως, βασίζεται μάλλον σε πραγματολογική παρά σε τυπική ανάλυση.

Από τον ορισμό αυτό κατανοούμε ότι ο ορισμός έχει πέντε συστατικά στοιχεία, τα οποία θα δούμε συνοπτικά.

#### 3.3.1.1 Φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας

Επί της ουσίας, δεν υπάρχει περιορισμός στο ποιος μπορεί να θεωρηθεί ως υπεύθυνος επεξεργασίας. Μπορεί να είναι μια μεγάλη πολυεθνική εταιρεία, ένας δημόσιος φορέας αλλά και ένας ιδιώτης. Στο δημόσιο τομέα[4] όμως, αναζητούμε, συνήθως, τον υπεύθυνο επεξεργασίας σε υψηλό επίπεδο, στη νομική οντότητα ενός δημόσιου φορέα, και όχι σε μεμονωμένους υπαλλήλους, διευθυντές, γενικούς γραμματείς ή υπουργούς, ούτε σε μεμονωμένα τμήματα ή διευθύνσεις. Ακόμα κι αν ένας υπάλληλος ή μια οργανική μονάδα (π.χ. τμήμα ή διεύθυνση) έχει αναλάβει τη διεκπεραίωση της δραστηριότητας επεξεργασίας, ο υπάλληλος ή η μονάδα δεν θεωρούνται υπεύθυνοι επεξεργασίας, καθώς δεν έχουν την αυτονομία να δρούν και να αποφασίζουν μόνοι τους, αλλά ενεργούν υπό τον έλεγχο και τις εντολές του φορέα

[4] Αντίστοιχα και στον ιδιωτικό τομέα υπεύθυνος επεξεργασίας δεν θεωρείται ο Διευθυντής ή ο Πρόεδρος του ΔΣ μιας επιχείρησης, αλλά το νομικό πρόσωπο της επιχείρησης.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τους.

☞ Κάθε δραστηριότητα επεξεργασίας προσωπικών δεδομένων από υπαλλήλους, η οποία διενεργείται στο πλαίσιο των δραστηριοτήτων του φορέα των υπαλλήλων, πρέπει να θεωρείται ότι λαμβάνει χώρα υπό τον έλεγχο του φορέα.

#### 3.3.1.2 Καθορίζει

Με βάση τις κατευθυντήριες γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων[5] (εφεξής, ΕΣΠΔ) [23], η έννοια του **ποιος καθορίζει** σκοπούς και μέσα επεξεργασίας συνδέεται με μια από δύο βασικές περιπτώσεις:

α) Καθορισμός λόγω εκ του νόμου υποχρέωσης: Όπως προκύπτει και από τη διάταξη για τον ορισμό του υπεύθυνου επεξεργασίας, αυτός μπορεί να ορίζεται σε νόμο (εθνικό ή ευρωπαϊκό) που αφορά μια δραστηριότητα επεξεργασίας προσωπικών δεδομένων. Υπάρχουν διατάξεις με τις οποίες ο νομοθέτης ρητά προσδιορίζει ένα υπεύθυνο επεξεργασίας. Αυτό προϋποθέτει ότι ο νομοθέτης έχει κάνει σωστή ανάλυση ώστε ο φορέας που ορίζεται ως υπεύθυνος επεξεργασίας να έχει πραγματική δυνατότητα ελέγχου της επεξεργασίας. Πιο συχνό είναι όμως να μην καθορίζεται ρητά ο υπεύθυνος επεξεργασίας στο νόμο, αλλά να θεσμοθετούνται καθήκοντα για ένα φορέα, από τα οποία προκύπτει η υποχρέωσή του να επεξεργαστεί προσωπικά δεδομένα.

☞ Ένας φορέας θεωρείται υπεύθυνος επεξεργασίας όταν προκύπτει ότι για να εκτελέσει μια εκ του νόμου αρμοδιότητά του είναι απαραίτητο να επιτελέσει επεξεργασία προσωπικών δεδομένων.

β) Καθορισμός εκ των πραγμάτων

Απουσία νόμου, απαιτείται να εξεταστούν οι πραγματικές συνθήκες ώστε να καθοριστεί ποιος είναι ο υπεύθυνος επεξεργασίας. Στην περίπτωση δημοσίων φορέων, οι οποίοι οφείλουν να λειτουργούν με βάση την αρχή της νομιμότητας της δημόσιας διοίκησης, είναι ασφαλέστερο ο καθορισμός να γίνεται με βάση τις θεσμοθετημένες αρμοδιότητες του φορέα.

[5] Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων περιγράφεται στην Ενότητα 12



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

### 3.3.1.3 Μόνος ή από κοινού με άλλους

Ο ορισμός του υπεύθυνου επεξεργασίας στο ΓΚΠΔ προβλέπει ότι σκοπός και τρόπος επεξεργασίας μπορεί να καθορίζεται από παραπάνω από έναν φορέα. Αυτή είναι η περίπτωση των «από κοινού υπεύθυνων επεξεργασίας» (joint controllers). Δηλαδή, ένας φορέας μπορεί να μην αποφασίζει για όλα τα ουσιώδη χαρακτηριστικά της επεξεργασίας, αλλά να μοιράζεται την ευθύνη με άλλους φορείς. Τα κριτήρια και οι προϋποθέσεις για την περίπτωση από κοινού υπευθύνων επεξεργασίας θα εξεταστούν στον άρθρο 26 του ΓΚΠΔ.

### 3.3.1.4 Σκοποί και τρόπος

Για να βρούμε το ποιος καθορίζει το σκοπό και τα μέσα για μια επεξεργασία προσωπικών δεδομένων πρέπει να αναζητήσουμε την απάντηση στα εξής δύο ερωτήματα:

1. **Γιατί** γίνεται μια επεξεργασία;
2. **Πώς** (με ποιο τρόπο) γίνεται μια επεξεργασία;

Στο δημόσιο τομέα το «γιατί» γίνεται μια επεξεργασία συνδέεται (θεωρητικά πάντα) με μια αρμοδιότητα ενός φορέα, η οποία –προφανώς με βάση την αρχή της νομιμότητας- του έχει αποδοθεί με διάταξη νόμου. Βέβαια, ο υπεύθυνος επεξεργασίας δεν αρκεί να διαθέτει την αρμοδιότητα (το «γιατί») αλλά πρέπει και στην πράξη, με κάποιο τρόπο, να την ασκεί (το «πώς»). Ο καθορισμός του σκοπού δεν αρκεί από μόνος του, αλλά πρέπει να συνοδεύεται και από ένα καθορισμό των «**ουσιωδών**» μέσων της επεξεργασίας. Αν όμως ένας φορέας συνεργάζεται με έναν άλλο φορέα, ως υπεργολάβο, για την εκτέλεση μιας επεξεργασίας, και καθορίζει το πλαίσιο των ενεργειών του υπεργολάβου, δεν υπάρχει αμφιβολία ότι ο πρώτος φορέας είναι ο υπεύθυνος επεξεργασίας.

Δυστυχώς οι περιστάσεις δεν είναι πάντα τόσο ξεκάθαρες. Συνήθως, ο σκοπός της επεξεργασίας εύκολα ή δύσκολα μπορεί να αποδοθεί σε ένα φορέα, ειδικά στο δημόσιο που αυτό συνδέεται με τις αρμοδιότητες του φορέα. Με ποια κριτήρια μπορούμε να αναγνωρίζουμε αν ένας φορέας καθορίζει τα «ουσιώδη» μέσα της επεξεργασίας; Με βάση το ΕΣΠΔ, ουσιώδη μέσα είναι αυτά που συνδέονται με το



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σκοπό της επεξεργασίας, όπως:

- Ποια προσωπικά δεδομένα θα τύχουν επεξεργασίας;
- Για πόσο χρόνο πρέπει αυτά να τηρούνται;
- Ποια πρόσωπα μπορεί να έχουν πρόσβαση σε αυτά;
- Ποιες είναι οι κατηγορίες των υποκειμένων των δεδομένων;

Τα «μη ουσιώδη» μέσα αφορούν πιο πρακτικές πτυχές της υλοποίησης της επεξεργασίας, όπως την επιλογή λογισμικού ή υλισμικού (softaware/hardware) και το λεπτομερή καθορισμό των μέτρων ασφάλειας.

☞ Ο υπεύθυνος επεξεργασίας μπορεί να καθορίζει τα βασικά χαρακτηριστικά μιας επεξεργασίας και να αφήνει στους εκτελούντες την επεξεργασία (όπως αυτοί περιγράφονται στη συνέχεια) την ευχέρεια του λεπτομερούς προσδιορισμού τους.

#### 3.3.1.5 Επεξεργασία

Είναι σύνηθες μια δραστηριότητα να απαρτίζεται από πολλές επιμέρους επεξεργασίες προσωπικών δεδομένων. Για παράδειγμα, η πληρωμή της μισθοδοσίας στο δημόσιο απαιτεί υπολογισμό του μισθού με βάση τα κριτήρια του νόμου (από το φορέα), αποστολή των πληροφοριών στην Ενιαία Αρχή Πληρωμών και διεκπεραίωση των πληρωμών μέσω του διατραπεζικού συστήματος ΔΙΑΣ. Είναι σαφές ότι για να ολοκληρωθεί η πληρωμή απαιτείται η συνέργεια τριών τουλάχιστον φορέων, αλλά ο κάθε ένας από αυτούς ελέγχει πλήρως τον επιμέρους σκοπό ή και τα μέσα της επεξεργασίας. Ένας υπεύθυνος επεξεργασίας μπορεί λοιπόν, να συνδέεται με το σύνολο των πράξεων επεξεργασίας μιας δραστηριότητας ή και μόνο με κάποιες από τις δραστηριότητες. Στην πράξη, όταν για μια δραστηριότητα εμπλέκονται αρκετοί φορείς, αυτή θα πρέπει να αναλύεται σε επιμέρους δραστηριότητες ώστε να καθορίζεται ο υπεύθυνος επεξεργασίας (ή οι ρόλοι) για κάθε μία από αυτές.

☞ Στη Δημόσια Διοίκηση το λειτουργικό κριτήριο για τον καθορισμό του υπευθύνου επεξεργασίας συνάπτεται κατ' αρχήν με τις **αρμοδιότητες που απονέμει ο νόμος** σε συγκεκριμένη αρχή, υπηρεσία ή νομικό πρόσωπο δημοσίου δικαίου, οι οποίες, επιπλέον, **πρέπει στην πράξη να ασκούνται** από τους φορείς τους.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Παράδειγμα:** Η Διεύθυνση Προσωπικού ενός Υπουργείου τηρεί τους φακέλους των υπαλλήλων του Υπουργείου. Για τη δραστηριότητα αυτή υπεύθυνος επεξεργασίας θα πρέπει να θεωρείται το Υπουργείο και όχι η συγκεκριμένη Διεύθυνση, ούτε ο Διευθυντής της. Αν και η Διεύθυνση και ο προϊστάμενός της μπορεί να έχουν την εξουσία να αποφασίζουν για λεπτομέρειες σχετικά με τον τρόπο της επεξεργασίας (π.χ. με ποιο τρόπο θα ταξινομούνται και θα φυλάσσονται οι φάκελοι των υπαλλήλων) συνεχίζουν να ενεργούν υπό τον έλεγχο του Υπουργείου (π.χ. πειθαρχικός έλεγχος).

**Παράδειγμα**: Ο νόμος προσδιορίζει ότι ένας Δήμος παρέχει επίδομα σε άπορους δημότες. Για την εκτέλεση της εκ του νόμου αρμοδιότητάς του, τον τρόπο της οποίας καθορίζει ο ίδιος, ο Δήμος είναι απαραίτητο να επεξεργαστεί προσωπικά δεδομένα, άρα είναι υπεύθυνος επεξεργασίας, χωρίς να πρέπει να αναφέρεται ρητά στη διάταξη.

### 3.3.2 Ο Εκτελών την Επεξεργασία

Ο ορισμός του ΓΚΠΔ για τον εκτελούντα την επεξεργασία είναι: «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας*». Από τον ορισμό καταλαβαίνουμε ότι ο ΓΚΠΔ δεν περιορίζει το ρόλο του εκτελούντα την επεξεργασία. Μπορεί να είναι δημόσια υπηρεσία, μπορεί να είναι μια εταιρεία, μπορεί να είναι και ένας ιδιώτης. Οι δύο βασικές προϋποθέσεις για τον εκτελούντα την επεξεργασία είναι:

1. Είναι διακριτή οντότητα από τον υπεύθυνο επεξεργασίας και
2. Επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας.

Διακριτή οντότητα σημαίνει ότι ένα τμήμα της ίδιας δημόσιας υπηρεσίας, ή ένας υπάλληλος της (με οποιαδήποτε μορφή εξάρτησης από την δημόσια υπηρεσία π.χ. δημοσίου δικαίου, ΙΔΑΧ, συμβασιούχος) δεν μπορεί να θεωρείται ως εκτελών την επεξεργασία. Ο ΓΚΠΔ αντιμετωπίζει τον υπεύθυνο επεξεργασίας ως ένα (ζωντανό)



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

οργανισμό τα όργανα του οποίου (τμήματα και υπάλληλοι) δεν ενεργούν ανεξάρτητα από τον οργανισμό. Το πάσης φύσης εξαρτώμενο προσωπικό του υπευθύνου επεξεργασίας οφείλει να ενεργεί υπό τις οδηγίες του (βλ. άρθρο 29 ΓΚΠΔ) αλλά χωρίς να διαθέτει την αυτοτέλεια του εκτελούντα την επεξεργασία.

Ο εκτελών την επεξεργασία επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας, αλλά όχι υπό την άμεση εποπτεία του. Ο εκτελών την επεξεργασία οφείλει βέβαια να εξυπηρετεί τους σκοπούς της επεξεργασίας του υπευθύνου και να ακολουθεί τις οδηγίες του, αλλά έχει την ευχέρεια να κρίνει με ποιο τρόπο θα εξυπηρετήσει τα συμφέροντα του υπευθύνου.

Οι συνηθέστερες περιπτώσεις στη δημόσια διοίκηση είναι ο εκτελών την επεξεργασία ενός δημόσιου υπευθύνου επεξεργασίας να είναι:

- Ένας ιδιώτης ανάδοχος έργου (π.χ. υπεργολάβος)
- Ένας άλλος δημόσιος φορέας, ο οποίος αναλαμβάνει με διάταξη νόμου, την υποστήριξη της εκτέλεσης της αρμοδιότητας άλλων δημοσίων φορέων.

Τυπικοί δημόσιοι φορείς που αναλαμβάνουν το ρόλο του εκτελούντα την επεξεργασία σε διάφορες περιπτώσεις είναι για παράδειγμα η ΓΓΠΣΔΔ για εφαρμογές του Taxisnet, η ΚτΠ Α.Ε. για διάφορα έργα, η ΗΔΙΚΑ για υποστήριξη φορέων κοινωνικής ασφάλισης, η ΕΔΥΤΕ Α.Ε. (χωρίς αυτό να σημαίνει ότι οι φορείς αυτοί, για άλλες επεξεργασίες, δεν μπορεί να είναι οι ίδιοι υπεύθυνοι επεξεργασίας).

Στη σημερινή παγκοσμιοποιημένη οικονομία υπάρχουν «μεγάλοι» εκτελούντες την επεξεργασία για δραστηριότητες όμως η παροχή υπηρεσιών που σχετίζονται με πληροφοριακά συστήματα, όπως π.χ. υπολογιστικού νέφους (cloud computing). Επίσης, είναι συνηθισμένο ένας εκτελών την επεξεργασία να μπορεί να «προσλάβει» και άλλον επιμέρους εκτελούντα την επεξεργασία. Ο ΓΚΠΔ έχει κατάλληλες προβλέψεις για τις αναθέσεις σε εκτελούντες την επεξεργασία στο άρθρο 28.

**Παράδειγμα:** Ο Δήμος Α, αναθέτει σε μία εταιρεία πληροφορικής Β την ανάπτυξη ιστοσελίδας για την είσπραξη νέων δημοτικών τελών. Οι δημότες του Δήμου Α μπορούν να κάνουν εγγραφή (registration) στην ιστοσελίδα, να ενημερώνονται και να προβαίνουν σε πληρωμή μέσω Διαδικτύου. Η πλήρης τεχνική υποστήριξη/συντήρηση της ιστοσελίδας γίνεται από την εταιρεία Β. Για την περαίωση των ηλεκτρονικών πληρωμών, ο Δήμος Α συνεργάζεται με την εταιρεία Γ η οποία είναι πιστοποιημένος

πάροχος υπηρεσιών ηλεκτρονικών πληρωμών και επεξεργάζεται δεδομένα πιστωτικών καρτών δημοτών του Α προκειμένου να ολοκληρωθεί μία πληρωμή.
Στην περίπτωση αυτή, υπεύθυνος επεξεργασίας είναι ο Δήμος Α, ενώ οι εταιρείες Β και Γ είναι εκτελούσες την επεξεργασία. Η Γ εταιρεία μπορεί να είναι και αυτοτελώς υπεύθυνος επεξεργασίας, καθώς εκ του νόμου, ως ίδρυμα πληρωμών, οφείλει να τηρεί στοιχεία των συναλλαγών με πιστωτικές κάρτες.
Οι δημότες (χρήστες) είναι υποκείμενα των δεδομένων.

### 3.3.3 Αποδέκτες και τρίτοι

Ο ΓΚΠΔ καθορίζει δύο ακόμα ρόλους οι οποίοι αφορούν, κυρίως, την εξουσιοδοτημένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα οποία κατέχει ο υπεύθυνος επεξεργασίας.
«Τρίτος» είναι πρόσωπο άλλο, εκτός από:

- Το υποκείμενο των δεδομένων
- Τον υπεύθυνο επεξεργασίας
- Τον εκτελούντα την επεξεργασία.
- τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα

Αυτό σημαίνει ότι πρόσωπα που εργάζονται σε φορέα διαφορετικό από τον υπεύθυνο επεξεργασίας θα είναι «τρίτοι» (ή θα ανήκουν σε «τρίτο»). Από την άλλη πλευρά, τα τμήματα ενός δημόσιου φορέα που, με βάση οργανόγραμμα, επεξεργάζονται δεδομένων πολιτών, για την εξυπηρέτηση της αρμοδιότητας του φορέα, δεν είναι «τρίτοι». Οι τρίτοι δε μετέχουν, με κανένα τρόπο, στην δραστηριότητα επεξεργασίας.
**Ο όρος «αποδέκτης» είναι ευρύτερος από τον όρο «τρίτος».** Αποδέκτης είναι «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία* ***κοινολογούνται*** *τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι*». Ο αποδέκτης μπορεί να είναι είτε πρόσωπο άλλο, πέραν του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία –οπότε θα είναι τρίτος– ή πρόσωπο εντός του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, όπως


Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

υπάλληλος ή άλλο τμήμα εντός της ίδιας υπηρεσίας[6].

Η διάκριση μεταξύ αποδεκτών και τρίτων έχει σημασία μόνο σε σχέση με τη νόμιμη κοινοποίηση δεδομένων. Οι υπάλληλοι υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία μπορούν να είναι αποδέκτες δεδομένων προσωπικού χαρακτήρα χωρίς καμία περαιτέρω νομική απαίτηση, εάν συμμετέχουν στις πράξεις επεξεργασίας του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Αποτελούν απλά, κατά μία έννοια, «κύτταρα» του οργανισμού στον οποίο υπηρετούν. Οι υπάλληλοι έχουν την υποχρέωση να παρέχουν την εργασία τους προς τον εργοδότη τους, αλλά δεν αντιμετωπίζονται ως έχοντες πρόσθετη ειδική ευθύνη από τη νομοθεσία για τα προσωπικά δεδομένα, στο βαθμό που δεν χρησιμοποιούν τα δεδομένα για δικό τους σκοπό. κάτι που θα παρέβαινε τις οδηγίες της υπηρεσίας τους. Οι ευθύνες βαρύνουν πάντα τον εργοδότη τους (υπεύθυνο ή εκτελούντα την επεξεργασία). Αντιθέτως, τρίτος, ο οποίος αποτελεί αυτοτελή οντότητα σε σχέση με τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, δεν εξουσιοδοτείται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα τα οποία επεξεργάζεται υπεύθυνος επεξεργασίας παρά μόνο για συγκεκριμένους νόμιμους λόγους σε συγκεκριμένη περίπτωση.

- ☞ Υπάλληλοι (με οποιαδήποτε σχέση εργασίας) του υπευθύνου και του εκτελούντος δεν έχουν ευθύνη όσο επεξεργάζονται τα προσωπικά δεδομένα στη βάση των εντολών των εργοδοτών τους.
- ☞ Καθίστανται όμως τρίτοι αν παραβούν τις εντολές για δικό τους σκοπό.

Ο ορισμός των αποδεκτών έχει μια εξαίρεση. Δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με νόμο δεν θεωρούνται ως αποδέκτες. Με τον τρόπο αυτό, οι υπεύθυνοι επεξεργασίας εξαιρούνται από την υποχρέωση ενημέρωσης του υποκειμένου των δεδομένων, όταν διενεργείται συγκεκριμένη έρευνα από φορολογικές ή τελωνειακές αρχές, μονάδες οικονομικής έρευνας, ανεξάρτητες διοικητικές αρχές ή αρχές χρηματοπιστωτικών αγορών. Τα αιτήματα λήψης στοιχείων που αποστέλλονται από τις δημόσιες αυτές αρχές θα πρέπει να είναι πάντα γραπτά, αιτιολογημένα και

[6] Για τον ορισμό του αποδέκτη ακολουθούμε τη λογική του εγχειριδίου FRA-CoE [21]. Καθώς το θέμα βρίσκεται σε συζήτηση στο ΕΣΠΔ, ενδέχεται να πρέπει να τροποποιηθεί κατάλληλα.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σύμφωνα με την περίσταση και δεν θα πρέπει να αφορούν το σύνολο των υποκειμένων των δεδομένων ή να οδηγούν στη διασύνδεση πληροφοριακών συστημάτων. Προφανώς βέβαια, μετά τη χορήγηση των στοιχείων, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις εν λόγω δημόσιες αρχές θα πρέπει να συμμορφώνεται προς τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας.

## 3.4 Σύστημα αρχειοθέτησης

Στον ΓΚΠΔ ορίζεται ως «σύστημα αρχειοθέτησης»:

- κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα
- τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια,
- είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

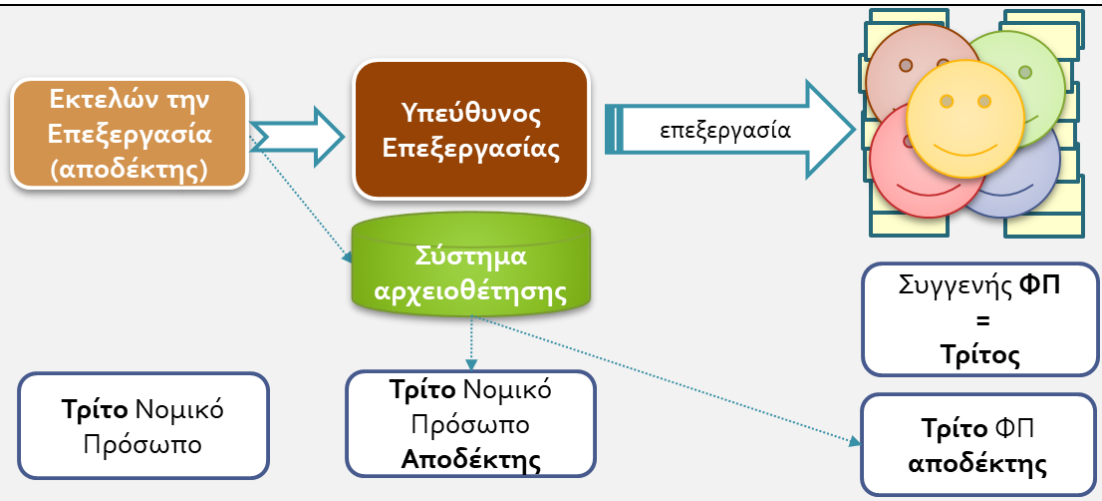
Ο ορισμός αυτός (που αντικατέστησε αυτόν του «αρχείου» στην παλαιότερη νομοθεσία) χρησιμοποιείται για να διαπιστωθεί εάν μια μη αυτοματοποιημένη (χειροκίνητη) επεξεργασία εμπίπτει στο πεδίο εφαρμογής του ΓΚΠΔ. Διαρθρωμένο σύστημα αρχειοθέτησης είναι αυτό το οποίο κατηγοριοποιεί ένα σύνολο δεδομένων προσωπικού χαρακτήρα, καθιστώντας τα προσβάσιμα βάσει ορισμένων κριτηρίων. Για παράδειγμα, εάν ένα γραφείο προσωπικού μικρής υπηρεσίας τηρεί έντυπο αρχείο αδειών, το οποίο περιέχει όλα τα στοιχεία των αδειών που έχουν εκδοθεί με αλφαβητική ταξινόμηση ανά υπάλληλο, το αρχείο αυτό θα συνιστά χειροκίνητο σύστημα αρχειοθέτησης.

Η έννοια του «συστήματος αρχειοθέτησης» χρησιμοποιείται επίσης και για τις ποινικές κυρώσεις του άρθρου 38 του ν. 4624/2019, αλλά αυτό είναι κάτι που αφορά αποκλειστικά τις διωκτικές αρχές. Κατά κανόνα όμως γίνεται δεκτό ότι κάθε αποθήκευση πληροφοριών σε ηλεκτρονική μορφή, οδηγεί σε ένα σύστημα αρχειοθέτησης, καθώς είναι πάντα εύκολη η ηλεκτρονική αναζήτηση με κάποια κριτήρια. Οι Βάσεις Δεδομένων είναι κλασικά παραδείγματα συστημάτων αρχειοθέτησης.

| **Παράδειγμα:** Το «οικοσύστημα» επεξεργασίας προσωπικών δεδομένων |
|---|



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης




Το οικοσύστημα αυτό συμπληρώνεται από την Εποπτική Αρχή, η οποία επιβλέπει την εφαρμογή της νομοθεσίας

**Ερώτηση δραστηριότητας**: Ανεξάρτητη δημόσια Αρχή (Α) εισπράττει εκ του νόμου παράβολα από αιτήσεις φυσικών προσώπων. Για την διαδικασία αίτησης ανέθεσε στην ιδιωτική εταιρεία (Β) να υλοποιήσει ειδική ιστοσελίδα, η οποία φιλοξενείται στην υποδομή G-Cloud του Υπουργείου (Γ). Η εταιρεία Β έχει αναλάβει την υποστήριξη των χρηστών σε περίπτωση τεχνικών προβλημάτων, ενώ το Υπουργείο Γ την αδιάλειπτη λειτουργία της υποδομής και κάποια από τα μέτρα ασφάλειας αυτής, όσα συνδέονται με τη λειτουργία της υποδομής. Για την πληρωμή των παραβόλων, η Αρχή Α δίνει τη δυνατότητα ηλεκτρονικής πληρωμής, μέσω της Τράπεζας Δ.
Αναλύστε τις δραστηριότητες επεξεργασίας και προσδιορίστε ποιος είναι υπεύθυνος επεξεργασίας και ποιος εκτελών την επεξεργασία.

## 3.5 Ο στόχος του ΓΚΠΔ

Ο Κανονισμός παίρνει τη σκυτάλη από την Οδηγία 95/46/ΕΚ. Ο βασικός του στόχος παραμένει ο ίδιος. Να θεσπίσει κανόνες που αφορούν:

- την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και
- την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα.

Πρακτικά, ο ΓΚΠΔ, όπως και η οδηγία, προσπαθεί να ισορροπήσει τις ανάγκες της αγοράς για απρόσκοπτη ανταλλαγή δεδομένων, ώστε να είναι δυνατό να λειτουργεί η



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σύγχρονη ηλεκτρονική και παγκοσμιοποιημένη οικονομία με τρόπο αποδοτικό, ενώ παράλληλα να εξασφαλίζονται τα θεμελιώδη δικαιώματα και οι ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ε.Ε. σημαίνει ότι, εφόσον τηρείται ο κανονισμός, δεν μπορεί να περιορίζεται ή να απαγορεύεται η ροή των προσωπικών δεδομένων εντός της Ε.Ε.. Για να πετύχει αυτό το στόχο, η Ε.Ε. εισήγαγε κανονισμό, ώστε οι κανόνες να είναι κοινοί για όλα τα Κ-Μ.

☞ Σε μια γρήγορα εξελισσόμενη αγορά, στην οποία τα προσωπικά δεδομένα αποτελούν «αξία», πρέπει να επιτυγχάνεται ομαλή λειτουργία της αγοράς και ταυτόχρονα προστασία των δικαιωμάτων και ελευθεριών των φυσικών προσώπων.

Βέβαια, με τις ρήτρες εξειδίκευσης και ευελιξίας, την εποπτεία του ΓΚΠΔ μέσω των διαφορετικών διοικητικών διαδικασιών των εποπτικών αρχών κάθε Κ-Μ και τις διαδικασίες συνεκτικότητας και συνεργασίας, είναι αμφίβολο αν μπορεί να επιτευχθεί η επιθυμητή συνεκτικότητα. Αυτό όμως είναι ένα ζήτημα που δεν αφορά τον εκάστοτε δημόσιο τομέα, στον οποίο έχει αποκλειστική αρμοδιότητα η εκάστοτε εθνική εποπτική αρχή (προστασίας προσωπικών δεδομένων).

## 3.6 Το πεδίο εφαρμογής του ΓΚΠΔ

Ο ΓΚΠΔ, αν και ενιαίας εφαρμογής σε όλη την ΕΕ (καλύτερα τον ΕΟΧ), δεν εφαρμόζεται σε κάθε δραστηριότητα επεξεργασίας προσωπικών δεδομένων. Αν και το πεδίο εφαρμογής του είναι αρκετά ευρύ, υπάρχουν εξαιρέσεις στις οποίες δεν εφαρμόζεται. Το πεδίο εφαρμογής του διακρίνεται σε «ουσιαστικό», δηλαδή σε σχέση με τις δραστηριότητες που μπορεί να εμπίπτουν σε αυτόν, και εδαφικό, δηλαδή σε σχέση με τις περιοχές στις οποίες εφαρμόζεται ο κανονισμός.

### 3.6.1 Ουσιαστικό πεδίο εφαρμογής

Στο άρθρο 2 του ΓΚΠΔ ορίζεται σε ποιες περιπτώσεις αυτός εφαρμόζεται. Ο κανόνας είναι ότι ο ΓΚΠΔ «*εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*σε σύστημα αρχειοθέτησης.*» Δηλαδή ο κανονισμός κατ' αρχήν εφαρμόζεται όταν υπάρχει:

- εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα ή
- μη αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης

Η πρώτη περίπτωση σημαίνει ότι οποτεδήποτε υπάρχει αυτοματοποιημένη επεξεργασία, έστω και σε ένα τμήμα αυτής, ο ΓΚΠΔ εφαρμόζεται άμεσα. Η εφαρμογή του κανονισμού δεν συνδέεται με την ύπαρξη συστήματος αρχειοθέτησης (αρχείου). Άρα, μια ηλεκτρονική εφαρμογή η οποία χρησιμοποιεί προσωπικά δεδομένα, ακόμα και χωρίς να τα αποθηκεύει, εμπίπτει στο πεδίο εφαρμογής του Κανονισμού. Τυπικό παράδειγμα είναι ένα σύστημα βιντεοεπιτήρησης χωρίς καταγραφή· η απλή επόπτευση θεωρείται επεξεργασία για την οποία εφαρμόζεται η ΓΚΠΔ.

Η δεύτερη περίπτωση καλύπτει τα διαρθρωμένα συστήματα μη ηλεκτρονικής αρχειοθέτησης. Τυπικό παράδειγμα είναι ένα σύστημα φακέλων το οποίο εφόσον είναι διαρθρωμένο με κάποια κριτήρια (π.χ. ονοματεπώνυμο, αριθμούς και βιβλίο πρωτοκόλλου) εμπίπτει στις διατάξεις του ΓΚΠΔ.

Ο Κανονισμός δεν εφαρμόζεται σε τέσσερις διακριτές περιπτώσεις, όπως πιο κάτω:

#### 3.6.1.1 Δραστηριότητα η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης

Χαρακτηριστικό παράδειγμα είναι οι δραστηριότητες που σχετίζονται με την εθνική ασφάλεια ενός Κ-Μ. Προσοχή όμως: οι δραστηριότητες αυτές καλύπτονται από την ΕΣΔΑ, με αποτέλεσμα το κράτος που έχει προσχωρήσει στη σύμβαση 108 να οφείλει να διαθέτει εθνικό νόμο ο οποίος να εφαρμόζεται και ως προς αυτές. Επίσης, καθώς το Ελληνικό Σύνταγμα δεν περιορίζει το πεδίο εφαρμογής, υποστηρίζεται ότι το δικαίωμα στην προστασία των προσωπικών δεδομένων υφίσταται και ως προς τις δραστηριότητες αυτές [18]. Στην Ελλάδα με το ν. 4624/2019, κάποιες δραστηριότητες των αρχών εθνικής ασφάλειας εξαιρούνται από τον έλεγχο της αρμόδιας αρχής.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

#### 3.6.1.2 Από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ

Οι δραστηριότητες αυτές περιλαμβάνουν την κοινή εξωτερική πολιτική και πολιτική ασφαλείας της ΕΕ και καλύπτουν όλους τους τομείς της εξωτερικής πολιτικής και το σύνολο των ζητημάτων που αφορούν την ασφάλεια της Ένωσης, συμπεριλαμβανομένου του προοδευτικού καθορισμού κοινής αμυντικής πολιτικής, η οποία μπορεί να οδηγήσει σε κοινή άμυνα.

#### 3.6.1.3 Από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας

Είναι η λεγόμενη «οικιακή» εξαίρεση, σύμφωνα με την οποία εξαιρούνται από το ΓΚΠΔ δραστηριότητες που είναι *αποκλειστικά* προσωπικές ή οικιακές. Όπως προκύπτει από την αιτιολογική σκέψη υπ' αριθμ. 18 του ΓΚΠΔ, αν μια δραστηριότητα συνδέεται με κάποια επαγγελματική ή εμπορική δραστηριότητα δεν μπορεί να θεωρείται προσωπική. Παραδείγματα είναι η προσωπική ή οικιακή αλληλογραφία και η τήρηση αρχείου διευθύνσεων, η κοινωνική δικτύωση χωρίς δημόσια ανάρτηση και οι σχετικές επιγραμμικές (online) δραστηριότητες που ασκούνται στο πλαίσιο τέτοιων δραστηριοτήτων, η χρήση καμερών εντός οικιακού χώρου για την προστασία της οικογένειας. Σε περίπτωση όπως που μια οικιακή δραστηριότητα δεν περιορίζεται *αποκλειστικά* σε οικιακό χώρο, τότε εφαρμόζεται ο ΓΚΠΔ (π.χ. κάμερα για την προστασία οικίας που εποπτεύει τμήμα δημόσιου χώρου [24]).

#### 3.6.1.4 Από αρχές που είναι αρμόδιες για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

Στις περιπτώσεις βέβαια αυτές, αντί του ΓΚΠΔ, εφαρμόζεται η «αστυνομική» Οδηγία (ΕΕ) 2016/680, η οποία προβλέπει παρόμοιες διασφαλίσεις.

### 3.6.2 Εδαφικό πεδίο εφαρμογής

Το εδαφικό πεδίο εφαρμογής της νομοθεσίας για τα προσωπικά δεδομένα



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τροποποιήθηκε σημαντικά με το ΓΚΠΔ. Ενώ με την οδηγία 95/46/ΕΚ καθοριζόταν το Κ-Μ που είχε αρμοδιότητα για την εφαρμογή της, πλέον, στο άρθρο 3, καθορίζεται ρητά πότε ένας φορέας εμπίπτει στο πεδίο εφαρμογής του ΓΚΠΔ. Χρησιμοποιούνται δύο κριτήρια:

1) το κριτήριο της «εγκατάστασης», σύμφωνα με το άρθρο 3 παράγραφος 1, και
2) το κριτήριο της «στόχευσης» σύμφωνα με το άρθρο 3 παράγραφος.

Εάν πληρούται ένα από αυτά τα δύο κριτήρια, οι διατάξεις του ΓΚΠΔ εφαρμόζονται στη σχετική επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον οικείο υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία.

Το πρώτο κριτήριο προβλέπει ότι ο ΓΚΠΔ εφαρμόζεται στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης. Άρα, μια επιχείρηση με εγκατάσταση εκτός Ε.Ε. και για δραστηριότητες στο «πλαίσιο» των οποίων εντάσσεται αυτή η εγκατάσταση, υποχρεούται να εφαρμόζει το ΓΚΠΔ.

Το δεύτερο κριτήριο προβλέπει ότι αν ένας υπεύθυνος επεξεργασίας δεν έχει εγκατάσταση στην ΕΕ, αλλά εφόσον οι δραστηριότητες επεξεργασίας του σχετίζονται με:

- προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από αυτά, ή
- παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης

τότε εφαρμόζεται ο ΓΚΠΔ. Τέτοιες περιπτώσεις είναι π.χ. όταν ένα ηλεκτρονικό κατάστημα πουλάει προϊόντα σε πολίτες που βρίσκονται στην ΕΕ, ανεξάρτητα της χώρας που βρίσκεται το κατάστημα, ή όταν μια εφαρμογή από εταιρεία εκτός ΕΕ χρησιμοποιεί συμπεριφορική διαφήμιση.

Περισσότερες λεπτομέρειες, μπορείτε να βρείτε στις σχετικές Κατευθυντήριες Γραμμές του ΕΣΠΔ [25].

Η περίπτωση των δημοσίων αρχών είναι όμως πάρα πολύ απλή, σε σχέση με το άρθρο 3.

☞ Μια δημόσια αρχή Κ-Μ της Ε.Ε. εμπίπτει πάντα στο πεδίο εφαρμογής του ΓΚΠΔ, εκτός κι αν κάποιες από τις δραστηριότητές της εξαιρούνται, με βάση τις



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εξαιρέσεις του άρθρου 2 του Κανονισμού

Τέλος, ο ΓΚΠΔ εφαρμόζεται και από υπεύθυνο επεξεργασίας εγκατεστημένο σε τόπο όπου εφαρμόζεται το δίκαιο ΚΜ δυνάμει του δημόσιου διεθνούς δικαίου (με το οποίο ρυθμίζονται οι έννομες σχέσεις μεταξύ κρατών).

## 3.7 Ρήτρες ανοίγματος και ρήτρες ευελιξίας

Όπως αναφέρθηκε νωρίτερα, ο κανονισμός, με τις λεγόμενες ρήτρες ευελιξίας και ρήτρες ανοίγματος, αφήνει τη δυνατότητα στα Κ-Μ να τον τροποποιήσουν ή να τον συμπληρώσουν στην πράξη, χωρίς βέβαια να μεταβάλλεται η ουσία του. Συγκεκριμένα, τα Κ-Μ έχουν τη δυνατότητα να διατηρήσουν ή να θεσπίσουν περαιτέρω όρους (και περιορισμούς) σε συγκεκριμένες διατάξεις, όπως π.χ.:

- Για την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία (άρ 9 παρ. 4)
- Θέσπιση περιορισμών στα δικαιώματα (άρ. 23)
- Όριο συγκατάθεσης ανηλίκων (άρ. 8)

Επίσης, τα Κ-Μ έχουν τη δυνατότητα να εξειδικεύσουν κανόνες (μεταξύ των οποίων και νομικές βάσεις) για τις πιο κάτω περιπτώσεις:

- Ελευθερία έκφρασης και πληροφόρησης
- Απασχόληση (με σκοπό την προστασία του εργαζόμενου)
- Αρχειοθέτηση προς το δημόσιο συμφέρον - επιστημονική ή ιστορική έρευνα ή στατιστικούς σκοπούς,
- Πρόσβαση του κοινού στα δημόσια έγγραφα
- Επεξεργασία εθνικού αριθμού ταυτότητας
- Ελεγκτικές αρχές
- Εκκλησίες και θρησκευτικές ενώσεις

Κατά την νομοθέτηση κανόνων για τα παραπάνω τα Κ-Μ πρέπει να είναι προσεχτικά ώστε να σέβονται τις αρχές του Κανονισμού και να μην υπερβαίνουν την εξουσιοδότηση που τους δίδεται να νομοθετήσουν. Ως προς τι ισχύει στο ελληνικό δίκαιο επί των ανωτέρω, περισσότερες πληροφορίες δίνονται στις αντίστοιχες επόμενες ενότητες.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 3.8 Βιβλιογραφία για περισσότερη μελέτη

- Ο.Ε. άρθρου 29 - Γνώμη 4/2007 σχετικά με την έννοια του όρου ‘δεδομένα προσωπικού χαρακτήρα’ [26]
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR [23]
- Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία» [27]
- Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3) [25]



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 4. Οι αρχές που διέπουν την επεξεργασία δεδομένων

Στο άρθρο 5 του ΓΚΠΔ προσδιορίζονται οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι αρχές αυτές αποτελούν τη βάση για τις λεπτομερέστερες διατάξεις που περιέχονται στα επόμενα άρθρα του κανονισμού. Επομένως, η κατανόηση των επτά αυτών αρχών είναι πρωταρχικής σημασίας ώστε να μπορούμε να εφαρμόσουμε σωστά τις ρυθμίσεις του Κανονισμού. Κι αυτό γιατί μέσα τους κρύβεται η λογική της νομοθεσίας.

## 4.1 Νομιμότητα, αντικειμενικότητα και διαφάνεια

Ο ΓΚΠΔ ορίζει ότι τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η πρώτη αρχή του Κανονισμού έχει τρεις πτυχές.

α) Νομιμότητα (Lawfulness): Η σύννομη επεξεργασία απαιτεί ένα νόμιμο λόγο (μία νομική βάση) ο οποίος προβλέπεται στη νομοθεσία για την προστασία δεδομένων. Πρακτική η εν λόγω αρχή «δείχνει» στο άρθρο 6 του Κανονισμού, το οποίο αναλύεται στη συνέχεια.

β) Αντικειμενικότητα (Fairness): Το θεμιτό της επεξεργασίας συνδέεται κυρίως με την υποχρέωση του υπευθύνου επεξεργασίας να ενημερώνει τα υποκείμενα των δεδομένων και το ευρύ κοινό ότι επεξεργάζεται δεδομένα με σύννομο τρόπο.

γ) Διαφάνεια (Transparency): Η αρχή αυτή αφορά την υποχρέωση του υπευθύνου επεξεργασίας να λαμβάνει κατάλληλα μέτρα ώστε να τηρεί ενήμερα τα υποκείμενα των δεδομένων σχετικά με τον τρόπο χρήσης των δεδομένων τους.

Πρακτικά, η πρώτη αρχή του ΓΚΠΔ καταλήγει να αφορά κυρίως τη διαφάνεια, σε όλες τις πτυχές της επεξεργασίας. Πλήρης ενημέρωση κατά το στάδιο συλλογής των δεδομένων για μια σειρά στοιχείων όπως ο σκοπός της επεξεργασίας και τα στοιχεία του υπεύθυνου επεξεργασίας, της νομικής βάσης αυτής, με χρήση απλής και κατανοητής γλώσσας. Στόχος είναι οι πράξεις επεξεργασίας να εξηγούνται στα υποκείμενα των δεδομένων έτσι ώστε να κατανοούν τι συμβαίνει με τα δεδομένα τους. Πλήρης διαφάνεια σημαίνει επίσης και ότι τα υποκείμενα των δεδομένων δικαιούνται να έχουν πλήρη πρόσβαση στα δεδομένα τους, αν το ζητήσουν. Εκτός εάν επιτρέπεται ειδικά από τον νόμο, δεν θα πρέπει να γίνεται μυστική ή



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

συγκεκαλυμμένη επεξεργασία προσωπικών δεδομένων.

☞ Ο στόχος της διάταξης είναι σαφής: Η οικοδόμηση εμπιστοσύνης μεταξύ υπευθύνου επεξεργασίας και υποκειμένου των δεδομένων.

Άλλωστε, το ορθά ενημερωμένο υποκείμενο των δεδομένων είναι εξαιρετικά απίθανο να προβάλλει αντιρρήσεις για μια νόμιμη επεξεργασία.

## 4.2 Περιορισμός του σκοπού

Με βάση το κείμενο του ΓΚΠΔ η αρχή αυτή επιβάλλει τα δεδομένα να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Αμέσως μετά, ο Κανονισμός, ήδη από τις βασικές του αρχές, διευκολύνει την περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς. Συνεπώς, τέτοια επεξεργασία δεν θα πρέπει να θεωρείται κατ' αρχήν ασύμβατη με τους αρχικούς σκοπούς. Αλλά ας προσπαθήσουμε να αναλύσουμε τι σημαίνει στην πράξη ο ορισμός αυτός.

Η εν λόγω αρχή συνδέεται άμεσα με την αρχή της διαφάνειας. Όταν ο σκοπός της επεξεργασίας είναι συγκεκριμένος και σαφής, τα άτομα γνωρίζουν τι να περιμένουν και αυξάνονται η διαφάνεια και η ασφάλεια δικαίου, ενώ τα υποκείμενα των δεδομένων να μπορούν να ασκούν αποτελεσματικά τα δικαιώματά τους. Τέσσερις είναι οι παράμετροι της αρχής αυτής:

1) Καθορισμένοι σκοποί: Με άλλα λόγια, η επεξεργασία για μη προσδιορισμένο σκοπό δεν είναι νόμιμη. Η τήρηση δεδομένων προσωπικού χαρακτήρα απλώς με το σκεπτικό ότι ενδέχεται να είναι χρήσιμα κάποια στιγμή στο μέλλον, παραβιάζει την εν λόγω αρχή.
2) Ρητοί σκοποί: Ο σκοπός της επεξεργασίας πρέπει να καθορίζεται (να δηλώνεται) σαφώς πριν από την έναρξη της επεξεργασίας.
3) Νόμιμοι σκοποί: Ο σκοπός δεν μπορεί να παραβιάζει το νόμο. Κάθε νέος σκοπός επεξεργασίας δεδομένων που ήδη τηρούμε νόμιμα, απαιτεί νέα, δική του νομική βάση και νομική εκτίμηση.
4) Περαιτέρω επεξεργασία: Μπορεί να επιτρέπεται η περαιτέρω επεξεργασία



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

δεδομένων που ήδη τηρούμε νόμιμα για ένα σκοπό, μόνο αν ο νέος σκοπός είναι συμβατός με τον αρχικό. Όμως, η περαιτέρω επεξεργασία δεν πρέπει να πραγματοποιείται με τρόπο μη αναμενόμενο από το υποκείμενο των δεδομένων ή με τρόπο στον οποίο ενδέχεται να διαφωνεί το υποκείμενο των δεδομένων.

Ο ΓΚΠΔ αναγνωρίζει, κατά κάποιο τρόπο, «προβάδισμα» στους σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, επιστημονικής ή ιστορικής έρευνας και στατιστικής. Με τον Κανονισμό η Ε.Ε. θέλει να διευκολύνει την υλοποίηση των σκοπών αυτών, αφαιρώντας πιθανά εμπόδια για τους ερευνητές ή άλλους επιστήμονες. Αυτό αποτελεί μια επιλογή πολιτικής της Ε.Ε. η οποία αποσκοπεί στην προώθησης της έρευνας και της καινοτομίας σε όλους τους τομείς, αλλά και στην υποβοήθηση της χρήσης ανωνυμοποιημένων στατιστικών δεδομένων, π.χ. για χάραξη πολιτικών.

Θα δούμε ότι η περαιτέρω επεξεργασία για συμβατό σκοπό αναλύεται ειδικότερα στο άρθρο 6 παρ. 4 του Κανονισμού. Εκεί αναλύονται τα κριτήρια, οι προϋποθέσεις και οι εγγυήσεις για να θεωρηθεί συμβατή μια περαιτέρω επεξεργασία.

**Παράδειγμα:** Δήμος τηρεί δεδομένα πολιτών τα οποία συλλέγει από αιτήσεις τους για τοποθέτηση προηγμένων κάδων ανακύκλωσης. Η περαιτέρω χρήση των δεδομένων αυτών από τον ίδιο το Δήμο για στατιστική ανάλυση της συμπεριφοράς των πολιτών κατ΄ αρχήν επιτρέπεται, καθώς η κατάρτιση στατιστικών συνιστά συμβατό σκοπό. Δεν απαιτείται πρόσθετη νομική βάση, όπως η συγκατάθεση των υποκειμένων των δεδομένων, αρκεί να υπάρχει μια γενική αρμοδιότητα στο Δήμο για τις πολιτικές ανακύκλωσης. Ωστόσο, για την περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα για στατιστικούς σκοπούς ο Δήμος πρέπει να παρέχει κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων (π.χ. ενημέρωση και δικαιώματα ΓΚΠΔ, εφαρμογή ανωνυμοποίησης ή ψευδωνυμοποίησης).

## 4.3 Ελαχιστοποίηση των δεδομένων

Η αρχή αυτή αναφέρει τα εξής για τα δεδομένα προσωπικού χαρακτήρα: «*είναι*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία».* Παρατηρούμε λοιπόν τις εξής παραμέτρους για τον ακριβή προσδιορισμό της αρχής αυτής:

1) Κατάλληλα δεδομένα: Οι κατηγορίες δεδομένων που επιλέγονται προς επεξεργασία πρέπει να είναι κατάλληλες ώστε να επιτευχθεί ο σκοπός. Αν κάποια δεδομένα δεν είναι πρόσφορα, δηλαδή δεν συμβάλλουν για την επίτευξη του σκοπού, δεν είναι νόμιμη η συλλογή τους.
2) Συναφή δεδομένα: Τα δεδομένα που συλλέγονται πρέπει να έχουν λογική συνάφεια με τον επιδιωκόμενο σκοπό.
3) Αναγκαία για τους σκοπούς δεδομένα: Οι κατηγορίες δεδομένων που επιλέγονται προς επεξεργασία πρέπει να είναι απαραίτητες για την επίτευξη του διακηρυγμένου γενικού στόχου της επεξεργασίας. Δηλαδή, αν κάποιο προσωπικό δεδομένο δεν είναι απαραίτητο για το συγκεκριμένο σκοπό, π.χ. αν ο σκοπός επιτυγχάνεται χωρίς αυτή την πληροφορία, τότε αυτό το δεδομένο δεν πρέπει να χρησιμοποιείται!

Ο υπεύθυνος επεξεργασίας οφείλει να περιορίζει αυστηρά τη συλλογή δεδομένων σε όσα πληρούν την παραπάνω αρχή. Η ικανοποίηση της αρχής της ελαχιστοποίησης δεν περιορίζεται μόνο στην επιλογή των κατηγοριών των δεδομένων, αλλά και σε τρόπους μείωσης των πληροφοριών που χρησιμοποιούνται για μια επεξεργασία. Αξιοποιώντας προηγμένες τεχνολογίες για την προστασία της ιδιωτικότητας, είναι δυνατόν να επιλέγονται φιλικές για την προστασία της ιδιωτικότητας λύσεις και έτσι:

- Να αποφεύγεται πλήρως η χρήση προσωπικών δεδομένων ή
- Να χρησιμοποιούνται ψευδωνυμοποιημένα δεδομένα

**Παράδειγμα:** Δήμος προσφέρει κάρτα με μικροεπεξεργαστή στους τακτικούς χρήστες των λεωφορείων του έναντι συγκεκριμένου τιμήματος. Στην επιφάνεια της κάρτας αναγράφεται το ονοματεπώνυμο του χρήστη, το οποίο περιέχεται σε ηλεκτρονική μορφή και στο μικροεπεξεργαστή. Κάθε φορά που ο χρήστης χρησιμοποιεί ένα λεωφορείο, περνά την κάρτα μπροστά από μία συσκευή ανάγνωσης που έχει εγκατασταθεί στο όχημα. Τα δεδομένα που διαβάζονται από τη συσκευή ανάγνωσης συγκρίνονται ηλεκτρονικά με μια βάση δεδομένων, η οποία περιέχει τα ονοματεπώνυμα των προσώπων που έχουν αγοράσει την κάρτα.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Το εν λόγω σύστημα δεν τηρεί την αρχή της ελαχιστοποίησης με το βέλτιστο δυνατό τρόπο: ο έλεγχος του κατά πόσον το πρόσωπο δικαιούται να χρησιμοποιήσει τα μέσα μαζικής μεταφοράς θα μπορούσε να γίνεται χωρίς να συγκρίνονται προσωπικά δεδομένα του μικροεπεξεργαστή της κάρτας με τη βάση δεδομένων. Θα αρκούσε, για παράδειγμα, να υπάρχει μια ειδική ηλεκτρονική εικόνα, π.χ. γραμμωτός κώδικας, στον μικροεπεξεργαστή της κάρτας. Με το πέρασμα της κάρτας μπροστά από τη συσκευή ανάγνωσης θα μπορούσε να επιβεβαιώνεται αν είναι έγκυρη ή όχι. Ένα σύστημα σαν αυτό δεν θα κατέγραφε ποιος χρησιμοποίησε ποιο μέσο μαζικής μεταφοράς σε ποια χρονική στιγμή.

☞ Η ρητή αναφορά της ψευδωνυμοποίησης στο ΓΚΠΔ υποδεικνύει την αυξημένη σημασία των τεχνολογικών επιλογών για την ικανοποίηση των βασικών αρχών της νομοθεσίας.

## 4.4 Ακρίβεια

Στο ΓΚΠΔ ακρίβεια ως προς τα δεδομένα σημαίνει ότι αυτά πρέπει να «*είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας*»

Υπεύθυνος επεξεργασίας ο οποίος κατέχει προσωπικές πληροφορίες δεν πρέπει να τις χρησιμοποιεί αν δεν λάβει μέτρα που να διασφαλίζουν (με εύλογη βεβαιότητα) ότι τα δεδομένα είναι ακριβή και επικαιροποιημένα. Η υποχρέωση όμως αυτή δεν είναι απόλυτη, αλλά πρέπει να εξετάζεται στο πλαίσιο του εκάστοτε σκοπού επεξεργασίας.

Κατ΄ αρχήν λοιπόν, εφόσον ένας υπεύθυνος επεξεργασίας προτίθεται να χρησιμοποιήσει προσωπικά δεδομένα, οφείλει να έχει εξασφαλίσει ότι αυτά είναι σωστά. Αν διαπιστώσει ότι τα δεδομένα είναι ανακριβή, οφείλει να τα διαγράψει ή να τα διορθώσει, χωρίς καθυστέρηση και χωρίς να απαιτείται αίτημα από το υποκείμενο των δεδομένων. Μάλιστα, οφείλει να διασφαλίζει την ακρίβεια των δεδομένων που χρησιμοποιεί προ βαίνοντας σε τακτικό έλεγχο και επικαιροποίησή τους.

Η επικαιροποίηση αποθηκευμένων δεδομένων μπορεί να περιορίζεται ανάλογα με το



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σκοπό, αλλά μόνο σε πολύ ειδικές περιπτώσεις.

**Παράδειγμα:** Ιατρικά δεδομένα τα οποία έχουν ήδη χρησιμοποιηθεί για μια ιατρική πράξη ή γνωμάτευση, δεν πρέπει να διαγράφονται και να αντικαθίστανται από τα ορθά, όπως προκύπτουν στο μέλλον. Είναι ορθότερο να γίνονται μόνο προσθήκες π.χ. ως παρατηρήσεις στον ιατρικό φάκελο που προστέθηκαν σε μεταγενέστερο στάδιο, ώστε να προκύπτει η εικόνα που οι θεράποντες ιατροί είχαν κατά το χρόνο μιας ιατρικής πράξης.

Η υποχρέωση ελέγχου της ακρίβειας των δεδομένων σε τακτά χρονικά διαστήματα και επικαιροποίησής τους, είναι απόλυτη, όταν από την επεξεργασία μπορεί να υπάρξει ζημία για το υποκείμενο των δεδομένων.

**Παράδειγμα:** Τα τραπεζικά ιδρύματα ελέγχουν τη φερεγγυότητα των πελατών τους σε πολλές περιπτώσεις (π.χ. ΤΕΙΡΕΣΙΑΣ). Η χρήση ανακριβών οικονομικών δεδομένων μπορεί να έχει δυσμενείς συνέπειες για τον πελάτη της τράπεζας, όπως με την άρνηση δανείου ή με τη χορήγηση δανείου σε πελάτη που δεν έχει την οικονομική δυνατότητα να αποπληρώσει.

Τέλος, η αρχή της ακρίβειας, δεν επιβάλλει την σε κάθε περίπτωση επικαιροποίηση των δεδομένων, όταν ο σκοπός της επεξεργασίας δεν δύναται να επιφέρει δυσμενείς συνέπειες σε ένα υποκείμενο των δεδομένων.

**Ερώτηση δραστηριότητας.** Δήμος δίνει τη δυνατότητα σε δημότες του να λαμβάνουν ειδοποιήσεις για νέα και εκδηλώσεις της γειτονιάς τους, στο κινητό τους τηλέφωνο. Ο Δήμος έχει συλλέξει για το σκοπό αυτό μόνο ένα ονοματεπώνυμο και ένα αριθμό τηλεφώνου. Μετά από ένα έτος ο Δήμος αντιλαμβάνεται ότι κάποιοι αριθμοί τηλεφώνου δεν αντιστοιχούν σε συνδρομητή.
Θεωρείτε ότι η αρχή της ακρίβειας επιβάλλει στο Δήμο να επικαιροποιήσει τους αριθμούς τηλεφώνου μέσω αναζήτησης και διασταύρωσης με τα αρχεία των παρόχων κινητής τηλεφωνίας;



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 4.5 Περιορισμός της περιόδου αποθήκευσης

Ο ΓΚΠΔ ορίζει ότι «*Τα δεδομένα προσωπικού χαρακτήρα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.*» Η εφαρμογή της αρχής αυτής σημαίνει ότι τα δεδομένα πρέπει να διαγράφονται ή να ανωνυμοποιούνται όταν δεν είναι πλέον αναγκαία για τους σκοπούς για τους οποίους συλλέχθηκαν.

Η αρχή του (χρονικού) περιορισμού της περιόδου αποθήκευσης επιβάλλει λοιπόν στο υπεύθυνο επεξεργασίας να προσδιορίζει σε αρχικό στάδιο τον χρόνο τον οποίο προβλέπει ότι θα τηρήσει τα δεδομένα. Ο χρόνος αυτός είναι σημαντική παράμετρος σε ένα σύστημα αρχειοθέτησης, καθώς είναι ο χρόνος στον οποίο πρέπει να εκτελεστεί η διαδικασία διαγραφής δεδομένων.

**Παράδειγμα:** Δημόσιος φορέας συλλέγει δηλώσεις πολιτών (email - ονοματεπώνυμο) για τη συμμετοχή τους σε μια διαδικτυακή ημερίδα. Μετά τη διαδικτυακή ημερίδα, πρέπει κανονικά να διαγράψει ή να ανωνυμοποιήσει τα δεδομένα των συμμετεχόντων.

Αν όμως ο φορέας εκδίδει βεβαιώσεις παρακολούθησης, το οποίο είναι ένας νέος σκοπός επεξεργασίας, οφείλει να προσδιορίσει για πόσο χρόνο θα τηρήσει τα στοιχεία παρακολούθησης, ώστε να μπορεί να επιβεβαιώσει την πιστότητα της βεβαίωσης. Στην περίπτωση αυτή ο χρόνος θα μπορούσε π.χ. να οριστεί σε 5 ή 10 έτη και το λογισμικό συλλογής των δηλώσεων να ρυθμιστεί ώστε τα δεδομένα να διαγραφούν/ανωνυμοποιηθούν μετά το διάστημα αυτό.

Μετά την πάροδο του χρόνου τήρησης, ο ΓΚΠΔ προβλέπει τήρηση για αρχειακούς, ιστορικούς ή επιστημονικούς σκοπούς. Συγκεκριμένα αναφέρει: «*τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, (...) και εφόσον εφαρμόζονται τα*



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.*» Η ρύθμιση αυτή είναι στη λογική της επεξεργασίας δεδομένων για έναν περαιτέρω, συμβατό με τον αρχικό, σκοπό, καθώς πρακτικά αναγνωρίζει ότι μετά το τέλος του καθορισμένου χρόνου τήρησης, τα δεδομένα μπορεί να χρησιμοποιηθούν για σκοπούς αρχειοθέτησης, έρευνας και στατιστικής, οι οποίοι θεωρούνται κατ' εξοχήν συμβατοί με τον αρχικό σκοπό.

Ο δημόσιος τομέας έχει μια επιπλέον δυσκολία για την εφαρμογή της αρχής αυτής. Καθώς οι δραστηριότητες επεξεργασίας ενός δημόσιου φορέα οριοθετούνται από τις διατάξεις που ρυθμίζουν τις αρμοδιότητές του, ο προβλεπόμενος χρόνος τήρησης πρέπει να αναζητείται μέσω των διατάξεων αυτών καθώς και των γενικών αρχών του δικαίου. Ο προσδιορισμός αυτός, με δεδομένο ότι οι διατάξεις που διέπουν τη λειτουργία ενός φορέα του δημοσίου είναι, πολλές φορές, δυσερμήνευτες, μπορεί να είναι ένα δύσκολο έργο. Είναι όμως πολύ σημαντικός ειδικά όταν σχεδιάζονται νέα πληροφοριακά συστήματα για την εξυπηρέτηση των αρμοδιοτήτων ενός δημόσιου φορέα. Κι αυτό καθώς, κατά το χρόνο αυτό, είναι δυνατό να ενσωματωθούν αυτοματισμοί για την διαγραφή ή την ανωνυμοποίησης των δεδομένων που δεν είναι πλέον απαραίτητα για το σκοπό που έχουν συλλεγεί, οι οποίοι να λειτουργούν μετά από καθορισμένο χρόνο.

☞ Η αρχή του περιορισμού της περιόδου αποθήκευσης υποδεικνύει ότι σε κάθε πληροφοριακό σύστημα που σχεδιάζεται για το δημόσιο τομέα πρέπει να ενσωματώνονται λειτουργίες για την αυτόματη διαχείριση των προσωπικών δεδομένων, μετά την πάροδο του χρόνου για τον οποίο απαιτείται να τηρούνται.

**Ερώτηση δραστηριότητας.** Υπουργείο σχεδιάζει νέα εφαρμογή μέσω της οποίας οι πολίτες αιτούνται τη λήψη απλού πιστοποιητικού με ισχύ χρήσης ενός μήνα. Το Υπουργείο, κατά την ανάλυση που κάνει, υπολογίζει επίσης ότι πρέπει να είναι σε θέση να επιβεβαιώσει την εγκυρότητα του πιστοποιητικού για έως και πέντε έτη μετά τη λήψη του.

Ποια θεωρείτε ότι πρέπει να είναι μια βέλτιστη σχεδίαση του συστήματος, όσον αφορά την τήρηση των πιστοποιητικών;



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Μπορεί το Υπουργείο να διατηρήσει κάποια από τα δεδομένα, για να γνωρίζει διαχρονικά στατιστικά στοιχεία για τη χρήση της υπηρεσίας;

## 4.6 Ακεραιότητα και εμπιστευτικότητα

Οι πέντε προηγούμενες αρχές ήταν, λίγο έως πολύ, βασικές αρχές της νόμιμης επεξεργασίας δεδομένων και με βάση την οδηγία 95/46/ΕΚ. Η αρχή της ασφαλούς επεξεργασίας των προσωπικών δεδομένων, αν και υπήρχε πάντα ως υποχρέωση των υπευθύνων επεξεργασίας, πλέον στο ΓΚΠΔ έχει «αναβαθμιστεί» σε βασική αρχή. Ακριβολογώντας, ιδίως η ακεραιότητα και η εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα, δύο από τις τρεις πτυχές της έννοιας της ασφάλειας στα πληροφοριακά συστήματα όπως θα δούμε και στην Ενότητα 10 (δηλαδή όχι η διαθεσιμότητα) είναι καθοριστικές για την αποφυγή αρνητικών συνεπειών για το υποκείμενο των δεδομένων. Όπως ορίζει ο Κανονισμός τα δεδομένα προσωπικού χαρακτήρα «*υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων*».

Οι κανόνες για την ασφάλεια της επεξεργασίας υποχρεώνουν τόσο τον υπεύθυνο επεξεργασίας όσο και τον εκτελούντα την επεξεργασία να εφαρμόζουν τα κατάλληλα μέτρα ασφάλειας (τεχνικά και οργανωτικά μέτρα) με σκοπό την αποτροπή κάθε μη εξουσιοδοτημένης επέμβασης στις πράξεις επεξεργασίας. Ο Κανονισμός δεν καθορίζει συγκεκριμένα μέτρα ασφάλειας, αλλά, όπως θα δούμε και αργότερα, το αναγκαίο επίπεδο ασφάλειας των δεδομένων πρέπει να κρίνεται κατά περίπτωση από:

- Τις τρέχουσες σύγχρονες τεχνικές (state of the art) για τα μέτρα ασφάλειας
- Το κόστος εφαρμογής των μέτρων και
- Το βαθμό «ευαισθησίας» των δεδομένων που υφίστανται επεξεργασία, δηλαδή τους κινδύνους που μπορεί να ανακύψουν για τα δεδομένα.

Στο κείμενο του κανονισμού προτείνονται κάποια ενδεδειγμένα μέτρα (όπως η κρυπτογράφηση και η ψευδωνυμοποίηση) τα οποία όμως δεν αποτελούν πανάκεια, αλλά πρέπει να εφαρμόζονται όταν μπορεί να είναι κατάλληλα εν όψει του σκοπού και των κινδύνων από την επεξεργασία.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Πρόσθετη εγγύηση της ασφαλούς επεξεργασίας των δεδομένων συνιστά το γενικό καθήκον όλων των προσώπων, είτε πρόκειται για υπευθύνους επεξεργασίας είτε για εκτελούντες την επεξεργασία, να διασφαλίζουν το απόρρητο των δεδομένων.
Αναλυτικότερα για τα μέτρα ασφάλειας θα δούμε στη σχετική Ενότητα 10, σε σχέση με τις υποχρεώσεις του άρθρου 32 του ΓΚΠΔ.

☞ Οι διατάξεις για τις υποχρεώσεις λήψης μέτρων ασφάλειας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα έχουν αναβαθμιστεί με το ΓΚΠΔ.

## 4.7 Λογοδοσία

Η μεγαλύτερη ίσως καινοτομία του ΓΚΠΔ, είναι η προσθήκη της αρχής της λογοδοσίας ως βασική του αρχή. Κι αυτό γιατί δεν είναι μόνο μια αναφορά σε αρχή επεξεργασίας, η οποία θα ήταν –λίγο ή πολύ- εύκολο να γίνει αντιληπτή ακόμα κι αν δεν υπήρχε ένα αναλυτικό νομικό κείμενο, αλλά εισάγει μια αλλαγή στη φιλοσοφία ελέγχου συμμόρφωσης με τις διατάξεις για την προστασία των προσωπικών δεδομένων.

Το «μοντέλο συμμόρφωσης», έως το ΓΚΠΔ βασιζόταν σε ένα σύστημα γνωστοποιήσεων (ανακοινώσεων) στην εποπτική αρχή όλων των δραστηριοτήτων με επεξεργασία προσωπικών δεδομένων. Πρακτικά, ο υπεύθυνος επεξεργασίας συμπλήρωνε τυποποιημένα έντυπα με τα βασικά χαρακτηριστικά της επεξεργασίας και τα κατέθετε στην αρμόδια εποπτική αρχή (προστασίας δεδομένων). Μόνο αν η επεξεργασία αφορούσε δεδομένων ειδικών κατηγοριών έπρεπε να λάβει απάντηση (άδεια) από την εποπτική αρχή. Η τυποποιημένη γνωστοποίηση αρκούσε για την έναρξη της επεξεργασίας. Το μοντέλο αυτό ήταν γραφειοκρατικό, τόσο για τους υπευθύνους επεξεργασίας οι οποίοι για κάποιες επεξεργασίες (ακόμα και τυπικές, π.χ. δεδομένα υγείας από ένα νοσοκομείο) έπρεπε να λάβουν άδεια από τις εποπτικές αρχές, ενώ ήταν δυσκίνητο σε περιπτώσεις καινοτόμων εφαρμογών καθώς και σε κάθε τροποποίηση της επεξεργασίας. Για τις δε εποπτικές αρχές, ήταν πρακτικά αδύνατο να ελέγχονται όλες οι γνωστοποιήσεις (ειδικά αν δεν απαιτούνται άδεια). Σε κάθε περίπτωση, μετά την υποβολή μιας γνωστοποίησης, η ευθύνη για την απόδειξη της «μη συμμόρφωσης» με τη νομοθεσία ήταν στις εποπτικές αρχές.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Με το ΓΚΠΔ πραγματοποιείται μια ουσιαστική αντιστροφή της ευθύνης απόδειξης της συμμόρφωσης με τη νομοθεσία. Η διάταξη της παρ. 2 του άρθρου 5 ρητά αναφέρει ότι «Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1» δηλαδή με τις έξι προαναφερθείσες αρχές επεξεργασίας.

Σύμφωνα με την Ο.Ε. του άρ. 29 [28][7], στον πυρήνα της λογοδοσίας βρίσκεται η υποχρέωση του υπεύθυνου επεξεργασίας:

- να εφαρμόζει μέτρα τα οποία –σε κανονικές συνθήκες– διασφαλίζουν την τήρηση των κανόνων για την προστασία των δεδομένων
- να διαθέτει κατάλληλα έγγραφα προς απόδειξη της νομιμότητας τόσο προς τις εποπτικές αρχές όσο και προς τα υποκείμενα των δεδομένων

Ο υπεύθυνος επεξεργασίας θα πρέπει να είναι ανά πάσα στιγμή σε θέση να καταδείξει στα υποκείμενα των δεδομένων, στο ευρύ κοινό και στις εθνικές εποπτικές αρχές ότι συμμορφώνεται με τους κανόνες προστασίας των δεδομένων. Η συμμόρφωσή του πρέπει να καταδεικνύεται ενεργά και να μην περιμένει απλώς να του υποδείξουν τυχόν αδυναμίες τα υποκείμενα των δεδομένων ή οι εθνικές αρχές ελέγχου. Για το σκοπό αυτό, ο Κανονισμός προβλέπει μια σειρά συγκεκριμένων υποχρεώσεων που στόχο έχουν την τεκμηρίωση της νομιμότητας των δραστηριοτήτων αλλά και τον αυξημένο εσωτερικό έλεγχο, ώστε ο υπεύθυνος επεξεργασίας να είναι σε θέση (προληπτικά) να διασφαλίζει συνεχώς τη συμμόρφωσή του, ακόμα και σε μεταβαλλόμενες δραστηριότητες. Τέτοιες υποχρεώσεις είναι:

- Τα αρχεία δραστηριοτήτων επεξεργασίας
- Ο θεσμός του (εσωτερικού) Υπεύθυνου Προστασίας Δεδομένων
- Οι Εκτιμήσεις Αντικτύπου σχετικά με την Προστασία Δεδομένων
- Οι υποχρεώσεις διασφάλισης της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού
- Η εθελοντική τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή μηχανισμών πιστοποίησης

Οι υποχρεώσεις αυτές προκύπτουν μεν από τις διατάξεις του Κανονισμού, αλλά δεν είναι οι μόνες. Ανάλογα με τη φύση μιας επεξεργασίας και τους κινδύνους που

[7] Η εν λόγω γνώμη ήταν μέρος των προτάσεων των αρχών για τις αλλαγές στο θεσμικό πλαίσιο προστασίας δεδομένων.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μπορεί να ανακύψουν για τα υποκείμενα των δεδομένων, είναι επίσης απαραίτητο να τεκμηριώνονται οι εσωτερικές διαδικασίες και τα μέτρα που λαμβάνει ένας υπεύθυνος επεξεργασίας, ώστε να είναι σε θέση να τα χρησιμοποιήσει τόσο εσωτερικά όσο και για την απόδειξη προς την εποπτική αρχή ότι αυτά έχουν προκύψει με συστηματικό τρόπο και είναι κατάλληλα. Τα εσωτερικά αυτά έγγραφα αποτελούν ουσιαστικά τις εφαρμοζόμενες **πολιτικές** του υπεύθυνου επεξεργασίας. Ήδη, άλλωστε, από το 2009 η Ε.Ε. είχε προβλέψει την ύπαρξη πολιτικών ασφάλειας με ρητή αναφορά στην τροποποίηση της Οδηγίας e-Privacy (με την Οδηγία 2009/136/ΕΚ).

☞ Η ύπαρξη εγγράφων πολιτικών είναι βασικό στοιχείο της αρχής της λογοδοσίας.

Αν και η λογοδοσία δεν καταλαμβάνει ευθέως τους εκτελούντες την επεξεργασία, ακόμα και αυτοί οφείλουν να συμμορφώνονται με ορισμένες υποχρεώσεις οι οποίες συνδέονται αυστηρά με την εν λόγω αρχή (όπως η τήρηση αρχείου δραστηριοτήτων επεξεργασίας και ο διορισμός υπευθύνου προστασίας δεδομένων).

Συμπερασματικά, το νέο μοντέλο συμμόρφωσης φαίνεται, αρχικά, περισσότερο δύσκολο στην εφαρμογή, ειδικά για όσους υπεύθυνους επεξεργασίας του δημοσίου δεν έχουν προβεί σε έλεγχο της νομιμότητας των δραστηριοτήτων τους. Αν και αναμένεται η πλειονότητα των δραστηριοτήτων να μην έχει ουσιαστικά ζητήματα νομιμότητας, σίγουρα υπάρχουν δραστηριότητες που γίνονται άτυπα, οι οποίες δύναται να επιφέρουν κυρώσεις για ένα φορέα, ακόμα και αν στην ουσία δεν υπάρχει παράβαση νομιμότητας. Από την άλλη πλευρά όμως, η εφαρμογή της αρχής της λογοδοσίας στην πράξη, θα βοηθήσει κάθε φορέα να «τακτοποιήσει» τις δραστηριότητές του, να προβεί σε μικρές ή μεγάλες προσαρμογές, θα αυξήσουν τη διαφάνεια των πράξεών του προς τους πολίτες και θα ελαχιστοποιήσουν τους κινδύνους που μπορεί να προκύψουν από αμελή εφαρμογή διατάξεων του ΓΚΠΔ, με αποτέλεσμα μεσο-μακροπρόθεσμα να βελτιώσουν την εικόνα του.

☞ Η αρχή της λογοδοσίας επιβάλλει στους υπευθύνους επεξεργασίας να αποδεικνύουν ενεργά τη συμμόρφωση και όχι να αναμένουν απλώς από τα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

υποκείμενα των δεδομένων ή τις εποπτικές αρχές να επισημάνουν αδυναμίες.

## 4.8 Βιβλιογραφία για περισσότερη μελέτη

Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης (FRA - CoE) – Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων (έκδοση 2018) [21]

Ο.Ε. άρθρου 29 - Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας [28]



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 5. Νομιμότητα

Η πρώτη αρχή του άρθρου 5 του ΓΚΠΔ αναφέρει ότι η επεξεργασία των προσωπικών δεδομένων πρέπει να είναι νόμιμη. Στο επόμενο άρθρο (το άρθρο 6) το κείμενο του Κανονισμού εξειδικεύει τις προϋποθέσεις υπό τις οποίες μια επεξεργασία μπορεί να είναι νόμιμη. Και ήδη από το άρθρο αυτό, αίρεται μια συνηθισμένη παρανόηση σε σχέση με τα προσωπικά δεδομένα. Αν μια πληροφορία είναι προσωπικό δεδομένο, δεν σημαίνει, αυτόματα, ότι κανείς δεν δικαιούται να την χρησιμοποιήσει. Για να ακριβολογούμε μάλιστα, είναι πολύ πιθανό ότι κάποιος μπορεί να την χρησιμοποιήσει νόμιμα, αλλά υπό προϋποθέσεις.
Αυτό ακριβώς δηλώνει το άρθρο 6 παρ. 1 του ΓΚΠΔ, το οποίο στην ουσία απαριθμεί τις πιθανές προϋποθέσεις που επιτρέπουν την επεξεργασία:

1. Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:
«*α) το υποκείμενο των δεδομένων έχει παράσχει συγκατάθεση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,*
*β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,*
*γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,*
*δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,*
*ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,*
*στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του*


Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.*

*Το στοιχείο στ) του πρώτου εδαφίου δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.*»

Είναι ίσως η πιο συχνά χρησιμοποιούμενη διάταξη του ΓΚΠΔ καθώς καθορίζει τις έξι **νομικές βάσεις** για την επεξεργασία προσωπικών δεδομένων.

☞ **Νομική βάση** είναι η απάντηση στο ερώτημα: Για ποιο νόμιμο λόγο επεξεργάζεται ένας υπεύθυνος επεξεργασίας δεδομένα προσωπικού χαρακτήρα;

Ο κανονισμός θέτει έξι (και μόνο) πιθανές απαντήσεις. Συνοπτικά ας τις αναφέρουμε ως:

α) Συγκατάθεση,

β) Σύμβαση,

γ) Έννομη υποχρέωση,

δ) Ζωτικό συμφέρον,

ε) Δημόσιο καθήκον και

στ) Υπέρτερο έννομο συμφέρον.

## 5.1 Επιλογή νομικής βάσης

Κάθε υπεύθυνος επεξεργασίας οφείλει να επιλέξει (τουλάχιστον) μία νομική βάση για κάθε ξεχωριστή δραστηριότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Η επιλογή αυτή γίνεται με τα εξής χαρακτηριστικά:

- Ο υπεύθυνος επεξεργασίας οφείλει να δηλώνει, εκ των προτέρων, ποια είναι η νομική βάση για την επεξεργασία, επιλέγοντας από τις έξι διαθέσιμες.
- Δεν υπάρχει ιεραρχία των νομικών βάσεων, δηλαδή, δεν υπάρχει κάποια προτιμώμενη. Ο υπεύθυνος πρέπει να καταλήξει στο ποια είναι η καταλληλότερη για τη συγκεκριμένη επεξεργασία.
- Ένας υπεύθυνος επεξεργασίας που επεξεργάζεται τα ίδια δεδομένα για διαφορετικό σκοπό, μπορεί κάλλιστα να πρέπει να επιλέξει διαφορετική



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

νομική βάση για κάθε σκοπό.

- Η «συγκατάθεση» είναι η πιο γνωστή νομική βάση, αλλά δεν είναι ούτε η μόνη νομική βάση, ούτε η πλέον κατάλληλη στις περισσότερες περιπτώσεις. Λόγω του ορισμού της συγκατάθεσης στο ΓΚΠΔ, είναι μάλλον δύσκολη στην εφαρμογή της κι ακόμα πιο δύσκολη για το δημόσιο τομέα.
- Στη θεωρία, υπάρχει η δυνατότητα να επιλέγονται δύο ή και παραπάνω νομικές βάσεις για μια συγκεκριμένη επεξεργασία. Στην πράξη όμως, θα πρέπει η εφαρμογή των εν λόγω νομικών βάσεων να μην είναι ασύμβατη μεταξύ τους. Π.χ. η συγκατάθεση είναι εκ του ορισμού της, ασύμβατη με κάθε άλλη νομική βάση, ενώ η σύμβαση θα μπορούσε, υπό προϋποθέσεις, να είναι συμβατή και με έννομη υποχρέωση.
- Δεν επιτρέπεται αλλαγή της νομικής βάσης, όταν έχει ξεκινήσει η επεξεργασία.
- Σε περίπτωση που η δραστηριότητα περιλαμβάνει επεξεργασία δεδομένων ειδικών κατηγοριών, η επιλογή νομικής βάσης δεν αρκεί από μόνη της, καθώς πρέπει επίσης, να αναζητηθεί και μια επιπλέον προϋπόθεση για την επεξεργασία αυτών των ειδικών δεδομένων (όπως επεξηγείται στη συνέχεια).

Φυσικά η επιλογή της νομικής βάσης είναι μόνο μια από τις υποχρεώσεις του υπευθύνου επεξεργασίας, ο οποίος οφείλει πάντα να συμμορφώνεται με τις αρχές του άρθρου 5 του Κανονισμού.

☞ Για να είναι νόμιμη μία επεξεργασία προσωπικών δεδομένων, αναγκαία προϋπόθεση είναι να πληροί όλες τις αρχές του άρθρου 5 του ΓΚΠΔ, καθώς επίσης και να εμπίπτει σε μία (τουλάχιστον) εκ των νομικών βάσεων του άρθρου 6.

## 5.2 Βασικά χαρακτηριστικά των έξι νομικών βάσεων

Προκειμένου να είμαστε σε θέση να αναγνωρίζουμε πότε είναι καλό να χρησιμοποιούμε μια νομική βάση, είναι απαραίτητο να αναλύσουμε τα βασικά τους χαρακτηριστικά.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

### 5.2.1 Συγκατάθεση

Η περίπτωση α' είναι εξαιρετικά απλή στον ορισμό «*το υποκείμενο των δεδομένων έχει παράσχει συγκατάθεση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς*». Όμως, η έννοια της «συγκατάθεσης» του υποκειμένου των δεδομένων έχει ήδη ορισθεί στο άρθρο 4 περ. 11 του Κανονισμού ως: «*κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*».

Επομένως, η συγκατάθεση δεν είναι μια αφηρημένη και γενική συναίνεση του υποκειμένου των δεδομένων. Αντίθετα, είναι μια νομική έννοια, με συγκεκριμένο ορισμό και πολλά συστατικά στοιχεία. Έγκυρη συγκατάθεση και άρα έγκυρη νομική βάση προϋποθέτει ικανοποίηση όλων των στοιχείων του παραπάνω ορισμού. Ο ΓΚΠΔ αφιερώνει το άρθρο 7 ειδικά για τον προσδιορισμό των προϋποθέσεων για τη συγκατάθεση. Επομένως, ένας υπεύθυνος επεξεργασίας, για να μπορέσει να χρησιμοποιήσει αυτή τη νομική βάση, οφείλει να είναι εξαιρετικά προσεχτικός καθώς είναι έγκυρη μόνο εάν στο υποκείμενο των δεδομένων παρέχεται έλεγχος και πραγματική επιλογή όσον αφορά την αποδοχή ή την απόρριψη των προσφερόμενων όρων ή την απόρριψη αυτών χωρίς ζημία.

☞ **Συγκατάθεση:** ένα από τα πιο συνηθισμένα λάθη υπευθύνων επεξεργασίας είναι να θεωρούν ότι κάθε επεξεργασία μπορεί να υλοποιηθεί με νομική βάση τη συγκατάθεση.

Όπως θα αναλύσουμε στην ειδική ενότητα για τη συγκατάθεση, είναι μια «δύσκολη» στην εφαρμογή νομική βάση, ενώ είναι ακατάλληλη για τις περισσότερες δραστηριότητες δημοσίων φορέων.

### 5.2.2 Εκτέλεση ή σύναψη σύμβασης

Σε σχέση με αυτή τη νομική βάση, ο Κανονισμός ορίζει «*η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των*



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*δεδομένων πριν από τη σύναψη σύμβασης*». Αμέσως κατανοούμε ότι:

- Η νομική βάση αυτή είναι κατάλληλη σε περιπτώσεις που το υποκείμενο των δεδομένων συμβάλλεται με τον υπεύθυνο επεξεργασίας. Άρα δεν είναι κατάλληλη όταν για την εκτέλεση μιας σύμβασης ο υπεύθυνος επεξεργασίας πρέπει να επεξεργαστεί και δεδομένα τρίτου.
- Εφαρμόζεται επίσης και κατά το προσυμβατικό στάδιο μετά από αίτηση του υποκειμένου των δεδομένων, π.χ. για να γίνουν από τον υπεύθυνο επεξεργασίας οι απαιτούμενοι έλεγχοι για την ορθότητα της σύμβασης ή για να εκδοθεί μια προσφορά. Αυτό δεν καλύπτει περιπτώσεις που δεν υπάρχει αίτηση του υποκειμένου των δεδομένων.
- Τα δεδομένα πρέπει να είναι **απαραίτητα για την εκτέλεση της σύμβασης** και δεν αρκεί να σχετίζονται με αυτή.
- Χρειάζεται προσοχή από τους υπεύθυνους επεξεργασίας όταν χρησιμοποιούν αυτή τη νομική βάση, καθώς πρέπει να σέβονται το εθνικό δίκαιο σε σχέση με αυτές (π.χ. για την προστασία των καταναλωτών).

Στη σημερινή εποχή η νομική βάση αυτή είναι πολύ συνηθισμένη στην παροχή επιγραμμικών υπηρεσιών, με τη χρήση, μάλιστα, τυποποιημένων συμβάσεων οι οποίες δεν αποτελούν αντικείμενο διαπραγμάτευσης. Το ΕΣΠΔ έχει εκδώσει σχετική καθοδήγηση [29].

### 5.2.3 Συμμόρφωση με έννομη υποχρέωση

Η νομική βάση αυτή είναι εύκολα κατανοητή. Εφαρμόζεται όταν ένας υπεύθυνος επεξεργασίας οφείλει να επεξεργαστεί προσωπικά δεδομένα επειδή το ορίζει νόμος. Γι' αυτό και «*η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας*». Οι φορείς του δημοσίου, σε σημαντικό βαθμό, επεξεργάζονται δεδομένα επειδή το ορίζει ρητά ένας νόμος[8]. Αλλά, εκτός από το δημόσιο, υπάρχουν πολλές περιπτώσεις στις οποίες οι υπεύθυνοι επεξεργασίας του ιδιωτικού τομέα υποχρεούνται εκ του νόμου να επεξεργάζονται δεδομένα: π.χ. οι γιατροί και τα νοσοκομεία, είτε δημόσιου είτε ιδιωτικού τομέα, τηρούν ιατρικούς φακέλους, οι εργοδότες τηρούν δεδομένα για σκοπούς ασφαλιστικούς και

[8] Με την ευρύτερη έννοια, όπου νόμος μπορεί να είναι Κανονισμός της ΕΕ, Ελληνικός Νόμος, Προεδρικό Διάταγμα ή Υπουργική Απόφαση μετά από κατάλληλη εξουσιοδότηση.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

φορολογικούς, όλες οι επιχειρήσεις και οι επιτηδευματίες τηρούν δεδομένα πελατών για φορολογικούς λόγους κ.ά.

Για ορθή εφαρμογή της νομικής βάσης, οι υπεύθυνοι επεξεργασίας πρέπει να είναι σε θέση να προσδιορίζουν από ποια διάταξη προκύπτει η υποχρέωση τήρησης προσωπικών δεδομένων. Η υποχρέωση τήρησης συγκεκριμένων κατηγοριών δεδομένων πρέπει να προκύπτει από το νόμο. Αν ένας υπεύθυνος επεξεργασίας έχει την ευχέρεια να αποφασίσει αν ο επιδιωκόμενος σκοπός μπορεί να επιδιωχθεί με προσωπικά δεδομένα ή να επιδιωχθεί χωρίς αυτά, τότε είναι πολύ πιθανό ότι δεν μπορεί να εφαρμοστεί η εν λόγω νομική βάση. Είναι επίσης σαφές, ότι στην έννοια του νόμου δεν εμπίπτουν διατάξεις δικαίου τρίτων χωρών, εκτός Ε.Ε..

### 5.2.4 Ζωτικό συμφέρον

Όπως έχουμε αναφέρει εξ αρχής, η προστασία των προσωπικών δεδομένων δεν είναι απόλυτο δικαίωμα. Πρέπει να συνδυάζεται ώστε να εξυπηρετούνται καλύτερα τα συμφέροντα των πολιτών. Προφανώς δεν είναι ανώτερη από άλλα δικαιώματα, ιδίως της προστασίας της ζωής. Συνεπώς η αναφορά «*η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου*» επισημαίνει ακριβώς αυτό. Ζωτικό συμφέρον σημαίνει προστασία της ζωής ή αντιμετώπιση μια σοβαρής απειλής για τα θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων ή και για τρίτο φυσικό πρόσωπο.

Η χρήση αυτής της νομικής βάσης είναι εφικτή σε φορείς ή και ιδιώτες που ασχολούνται με την υγεία, σε έκτακτες περιστάσεις (υπάρχει και σχετική εξαίρεση για τα δεδομένα υγείας, τα οποία είναι ειδικών κατηγοριών, στο άρθρο 9 του ΓΚΠΔ).

**Παράδειγμα:** Ασθενοφόρο του ΕΚΑΒ φτάνει σε χώρο ατυχήματος. Ο τραυματίας δεν έχει τις αισθήσεις του ώστε να παράσχει ο ίδιος τις πληροφορίες. Καθώς είναι απαραίτητο για τη ζωή του, οι νοσηλευτές και τραυματιοφορείς μπορούν να ενημερωθούν για το ιατρικό ιστορικό του τραυματία από τρίτους ή από άλλα διαθέσιμα έγγραφα.

Φυσικά η νομική βάση αυτή δεν εφαρμόζεται σε όλα τα δεδομένα υγείας, αλλά μόνο όταν είναι απαραίτητο για την προστασία της ζωής ενός υποκειμένου των δεδομένων



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

και είναι πρόδηλο ότι η επεξεργασία δεν μπορεί να έχει άλλη νομική βάση. Επίκληση της νομικής βάσης αυτής μπορεί να γίνει επίσης για ανθρωπιστικούς σκοπούς, μεταξύ άλλων για την παρακολούθηση επιδημιών και της εξάπλωσής τους ή σε καταστάσεις επείγουσας ανθρωπιστικής ανάγκης, ιδίως δε σε περιπτώσεις φυσικών και ανθρωπογενών καταστροφών (βλ. αιτιολογική σκέψη υπ' αριθμ. 46 του ΓΚΠΔ). Επίκληση αυτής της νομικής βάσης μπορεί να γίνει, επίσης, και σε περίπτωση εξαφάνισης προσώπου το οποίο αναζητείται και θεωρείται ότι κινδυνεύει.

### 5.2.5 Απαραίτητη για εκπλήρωση δημοσίου καθήκοντος

Η νομική βάση της «έννομης υποχρέωσης» (περίπτωση γ΄) χρησιμοποιείται για την τεκμηρίωση δραστηριοτήτων τις οποίες επιβάλει μια διάταξη στον υπεύθυνο επεξεργασίας. Αλλά ακόμα πιο συχνό είναι, ειδικά στο δημόσιο τομέα, μια διάταξη να απονέμει αρμοδιότητα σε ένα φορέα, χωρίς να κάνει αναφορά σε προσωπικά δεδομένα. Στην πράξη όμως, ο φορέας (συνήθως μάλιστα δημόσιος), όταν θα πρέπει να εκτελέσει την αρμοδιότητά του, θα χρειαστεί να επεξεργαστεί προσωπικά δεδομένα πολιτών.

Η νομική βάση ορίζεται ότι χρησιμοποιείται όταν «*η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας*». Γίνεται επομένως κατανοητό ότι αυτή αφορά: α) το δημόσιο, καθώς κατ' εξοχήν σε αυτό ανατίθενται δημόσια καθήκοντα και εξουσίας και β) περιορισμένο αριθμό ιδιωτικών φορέων στους οποίους εκ του νόμου ανατίθενται συγκεκριμένες δραστηριότητες δημοσίου συμφέροντος. Τέτοιες είναι η δημόσια υγεία, η κοινωνική προστασία και η διαχείριση των υπηρεσιών υγειονομικής περίθαλψης, επαγγελματικές οργανώσεις (όσες δεν είναι ήδη ΝΠΔΔ) αλλά και εταιρείες διοδίων ή η καταπολέμηση της απάτης ή του παράνομου περιεχομένου στο διαδίκτυο (βλ. αιτιολογική σκέψη υπ' αριθμ. 45 του ΓΚΠΔ). Η νομική βάση αυτή προσφέρει ευελιξία ειδικά στους δημόσιους φορείς (οι οποίοι όπως θα δούμε δεν μπορούν να χρησιμοποιήσουν τη νομική βάση του υπέρτερου έννομου συμφέροντος για δραστηριότητες που σχετίζονται με την άσκηση των αρμοδιοτήτων τους).

Για την άσκηση των αρμοδιοτήτων του, ένας δημόσιος φορέας θα χρειαστεί συχνά να



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επεξεργαστεί προσωπικά δεδομένα. Ιδανικά, οι αρμοδιότητες του φορέα θα έπρεπε να προδιαγράφονται τόσο αναλυτικά σε νόμους (συμπεριλαμβανομένων και εκτελεστικών αποφάσεων κατ' εξουσιοδότηση) ώστε κάθε επεξεργασία προσωπικών δεδομένων να προκύπτει ευθέως από το νόμο. Αλλά και το σκεπτικό του Ευρωπαίου Νομοθέτη, κατά την κατάρτιση του Κανονισμού, βασίστηκε στο ότι, ως γνωστόν, λίγοι φορείς έχουν τόσο αναλυτικά προδιαγεγραμμένες διατάξεις, ενώ απαιτείται να έχουν και την ευελιξία να προσαρμόζουν τη δράση τους στις σύγχρονες συνθήκες, διαφοροποιώντας προς τούτο και τις δραστηριότητές τους. Όπως φαίνεται και από την αιτιολογική σκέψη υπ΄ αριθμ. 45, ο Κανονισμός δεν απαιτεί συγκεκριμένο νόμο για κάθε μεμονωμένη επεξεργασία. Μπορεί να αρκεί ένας μόνο νόμος ως βάση για περισσότερες από μία πράξεις επεξεργασίας ή εάν η επεξεργασία είναι **αναγκαία** για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας. Βέβαια, βασικά χαρακτηριστικά της επεξεργασίας, όπως ο καθορισμός του σκοπού θα πρέπει να προκύπτουν από νόμο, ο οποίος (δυνητικά και όχι υποχρεωτικά) μπορεί να τα εξειδικεύει περαιτέρω.

☞ Ένας φορέας, για να ασκήσει μια αρμοδιότητα του, μπορεί να χρησιμοποιήσει προσωπικά δεδομένα, αν αυτό είναι **πραγματικά αναγκαίο** για το συγκεκριμένο σκοπό, ακόμα και αν η διάταξη δεν προβλέπει ρητά επεξεργασία προσωπικά δεδομένων.

Για την εφαρμογή της εν λόγω νομικής βάσης έχει ιδιαίτερη βαρύτητα η **αρχή της αναγκαιότητας**. Η επεξεργασία προσωπικών δεδομένων πρέπει να είναι **στοχευμένη**, **αιτιολογημένη** και να σέβεται την αρχή της **αναλογικότητας**. Ο σκοπός δεν θα πρέπει να μπορεί να επιτευχθεί με άλλα ηπιότερα μέσα, όπως επιβάλει και η αρχή της ελαχιστοποίησης των δεδομένων. Ιδιαίτερη προσοχή απαιτείται για την ικανοποίηση των αρχών του ΓΚΠΔ, ενώ καθώς η επεξεργασία δεν προκύπτει άμεσα από μια διάταξη, είναι απαραίτητο να τεκμηριώνεται κατάλληλα η εφαρμογή της με βάση την αρχή της λογοδοσίας.

**Παράδειγμα:** Δημόσια Ελεγκτική Αρχή έχει αρμοδιότητα να χειρίζεται καταγγελίες



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

για παραβάσεις της εργατικής νομοθεσίας. Ο νόμος δεν προσδιορίζει επακριβώς ποια στοιχεία πρέπει να περιέχουν οι καταγγελίες, ούτε ποια είναι απαραίτητα για το παραδεκτό μιας καταγγελίας. Για την επεξεργασία των προσωπικών δεδομένων που θα χρησιμοποιήσει για την εξέταση, η Δημόσια Αρχή μπορεί για να χρησιμοποιήσει τη νομική βάση του άρθρου 6 παρ. 1 ε' του ΓΚΠΔ. Οφείλει όμως να προσδιορίσει ποια στοιχεία είναι απαραίτητα για την ορθή εξέταση της καταγγελίας, με βάση την αρχή της ελαχιστοποίησης των δεδομένων.

### 5.2.6 Υπέρτερο έννομο συμφέρον

Η τελευταία (αλλά όχι λιγότερο σημαντική) νομική βάση του ΓΚΠΔ αναφέρει ότι η επεξεργασία πρέπει να «*είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί*». Η νομική αυτή βάση είναι μέγιστης σημασίας για τον ιδιωτικό τομέα, καθώς μπορεί να νομιμοποιήσει την επεξεργασία ακόμα και χωρίς συγκατάθεση, αν υπάρχουν κατάλληλες διασφαλίσεις για τα συμφέροντα, τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Στο δημόσιο όμως τομέα, ο ΓΚΠΔ ρητά αναφέρει ότι η εν λόγω νομική βάση «*δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους*».

Η νομική βάση προβλέπει τη διενέργεια στάθμισης: τα έννομα συμφέροντα του υπευθύνου της επεξεργασίας (ή τρίτων) πρέπει να σταθμίζονται έναντι των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του προσώπου στο οποίο αναφέρονται τα δεδομένα. Το αποτέλεσμα της στάθμισης καθορίζει σε μεγάλο βαθμό το κατά πόσον το άρθρο 6 παρ. 1 στ' μπορεί να αποτελέσει νομική βάση για την επεξεργασία.

Αξίζει να αναφερθεί, ότι δεν πρόκειται για απλή στάθμιση δύο εύκολα ποσοτικοποιήσιμων και συγκρίσιμων μεταξύ τους μεγεθών. Αντιθέτως, η εφαρμογή του κριτηρίου στάθμισης μπορεί να απαιτεί μια περίπλοκη αξιολόγηση, στην οποία λαμβάνεται υπόψη μια σειρά παραγόντων. Η ορθή εφαρμογή της στάθμισης αυτής



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προϋποθέτει τρία στάδια:

#### 5.2.6.1 Έννομο συμφέρον του υπευθύνου επεξεργασίας (ή τρίτων)

Η έννοια του «συμφέροντος» είναι στενά συνδεδεμένη με την έννοια του «σκοπού» της επεξεργασίας, όμως ταυτόχρονα διακριτή από αυτήν.

> ☞ Συμφέρον νοείται το ευρύτερο διακύβευμα το οποίο ενδέχεται να υπαγορεύει στον υπεύθυνο επεξεργασίας την επεξεργασία ή το όφελος που αποκομίζει ο υπεύθυνος επεξεργασίας από την επεξεργασία, καθώς και το συναφές δυνητικό όφελος της κοινωνίας

Η φύση των συμφερόντων μπορεί να ποικίλλει. Ορισμένα συμφέροντα μπορεί να είναι επιτακτικά και επωφελή για την κοινωνία στο σύνολό της, (π.χ. διεξαγωγή επιστημονικής έρευνας). Άλλα συμφέροντα μπορεί να είναι λιγότερο επιτακτικά για την κοινωνία στο σύνολό της, και οι συνέπειες τους για την κοινωνία να είναι πιο πολύπλοκες και αμφιλεγόμενες (π.χ. δημιουργία προφίλ για στοχευμένη διαφήμιση). Μια επιχείρηση μπορεί να έχει συμφέρον την εξασφάλιση της υγείας και της ασφάλειας του προσωπικού της ενώ σίγουρα έχει οικονομικό συμφέρον. Κατά την Ο.Ε. του άρ. 29 [30], η έννοια του έννομου συμφέροντος είναι δυνατόν να περιλαμβάνει ένα ευρύ φάσμα συμφερόντων, επουσιώδους αξίας ή άκρως επιτακτικών, σαφών ή πιο αμφιλεγόμενων, αρκεί αυτά να είναι αποδεκτά από το νόμο. Έτσι το έννομο συμφέρον θα πρέπει να:

- να είναι σύννομο
- να προσδιορίζεται με επαρκή σαφήνεια ώστε να επιτρέπεται η στάθμισή του έναντι των συμφερόντων και των θεμελιωδών δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα (δηλ. να είναι αρκούντως σαφές)
- να αφορά ένα πραγματικό και υφιστάμενο συμφέρον (δηλαδή να μην είναι υποθετικό)

#### 5.2.6.2 Συμφέρον ή θεμελιώδη δικαιώματα και ελευθερίες του υποκειμένου των δεδομένων

Όσον αφορά τα υποκείμενα των δεδομένων, για τη στάθμιση πρέπει να λαμβάνονται υπόψη τα «συμφέροντα» των προσώπων στα οποία αναφέρονται τα δεδομένα και όχι



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μόνο τα θεμελιώδη δικαιώματα και οι ελευθερίες τους. Εάν ο υπεύθυνος επεξεργασίας (ή ο τρίτος) δικαιούται να επιδιώκει οποιοδήποτε συμφέρον, αρκεί να μην είναι παράνομο, θα πρέπει επίσης να λαμβάνονται υπόψη κατά τη στάθμιση όλες οι κατηγορίες συμφερόντων τα οποία **μπορεί να επικαλεστεί** το πρόσωπο στο οποίο αναφέρονται τα δεδομένα, αρκεί να εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού. Σε μια περίοδο που χαρακτηρίζεται από το γεγονός ότι κυβερνήσεις και μεγάλες επιχειρήσεις συγκεντρώνουν πρωτοφανείς όγκους προσωπικών δεδομένων, είναι ακόμη πιο σημαντική η κατοχύρωση των συμφερόντων των φυσικών προσώπων που συνδέονται με τη διατήρηση του απορρήτου της ιδιωτικής τους ζωής και της ατομικής τους αυτονομίας. Μάλιστα, όσον αφορά τα συμφέροντα του υποκειμένου των δεδομένων, η διάταξη δεν κάνει αναφορά σε «έννομα» συμφέροντα, υποδεικνύοντας ότι ακόμα και τα άτομα που ασκούν παράνομες δραστηριότητες δεν θα πρέπει να υπόκεινται σε δυσανάλογες παρεμβάσεις σε σχέση με τα δικαιώματα και τα συμφεροντά τους. Για παράδειγμα, τα συμφέροντα ενός ατόμου που κατηγορείται ότι έχει διαπράξει κλοπή υπερισχύουν του συμφέροντος που επιτάσσει τη δημοσίευση της φωτογραφίας του και των στοιχείων της διεύθυνσής του, απουσία συγκεκριμένης διάταξης.

#### 5.2.6.3 Διενέργεια στάθμισης

Για τη διενέργεια της στάθμισης, πρέπει να λαμβάνονται υπόψη τα έννομα συμφέροντα του υπευθύνου της επεξεργασίας και ο αντίκτυπός τους στα συμφέροντα και στα δικαιώματα του προσώπου στο οποίο αναφέρονται τα δεδομένα. Η στάθμιση αυτή σε κάποιες περιπτώσεις είναι απλή, ενώ σε άλλες περιπτώσεις μπορεί να αποβεί ιδιαίτερα περίπλοκη ενώ η μεθοδολογία που ακολουθείται μοιάζει με αυτή της Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (άρθρο 35 του ΓΚΠΔ – βλ. Ενότητα 10). Καθώς στο δημόσιο τομέα η εν λόγω νομική βάση πρακτικά δεν εφαρμόζεται, για περαιτέρω ανάλυση μπορείτε να δείτε τη σχετική καθοδήγηση της Ο.Ε. του άρθρου 29 [30].

Οι υπεύθυνοι επεξεργασίας οφείλουν να λαμβάνουν υπόψη τις θεμιτές προσδοκίες των υποκειμένων των δεδομένων βάσει της σχέσης τους με τον υπεύθυνο επεξεργασίας. Από τον Κανονισμό αναγνωρίζεται ένα προβάδισμα για τις εταιρείες στο να επεξεργαστούν δεδομένων των πελατών τους ή όσων βρίσκονται στην



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

υπηρεσία τους. Επίσης, γίνεται ειδική αναφορά σε σκοπούς πρόληψης απάτης και σε σκοπούς άμεσης εμπορικής προώθησης.

Ισχυρό κριτήριο αποτελεί το κατά πόσον το υποκείμενο των δεδομένων, κατά τη χρονική στιγμή και στο πλαίσιο της συλλογής των δεδομένων προσωπικού χαρακτήρα, μπορεί εύλογα να αναμένει ότι για τον σκοπό αυτό μπορεί να πραγματοποιηθεί επεξεργασία. Σε περιπτώσεις κατά τις οποίες το υποκείμενο των δεδομένων δεν αναμένει ευλόγως περαιτέρω επεξεργασία των δεδομένων του, δεν θα πρέπει να εφαρμόζεται η εν λόγω νομική βάση.

Τέλος επισημαίνουμε ότι, με βάση την αρχή της λογοδοσίας, είναι απαραίτητο για ένα υπεύθυνο επεξεργασίας να μπορεί να αποδείξει με ποιο τρόπο έκανε την στάθμιση. Συνεπώς, θα πρέπει να τηρεί κατάλληλη έγγραφη τεκμηρίωση.

## 5.3 Επιλογή νομικών βάσεων στο δημόσιο τομέα

Ο δημόσιος τομέας οφείλει να λειτουργεί με βάση την αρχή της νομιμότητας. Η αρχή αυτή εγγυάται την υποχρέωση της δημόσιας διοίκησης να σέβεται τις επιταγές, απαγορεύσεις και ρυθμίσεις που θεσπίζει ο νομοθέτης, ενώ διασφαλίζει τον έλεγχο των πράξεων των διοικητικών οργάνων από τα δικαστήρια. Οι δημόσιες αρχές οφείλουν να ενεργούν στο πλαίσιο του νόμου και δεν επιτρέπεται, να περιορίζουν τα δικαιώματα, τις ελευθερίες, καθώς και την ιδιοκτησία των πολιτών παρά μόνο βάσει επιφύλαξης του νόμου.

Επιγραμματικά, μπορούμε να πούμε ότι οι δημόσιοι φορείς μπορούν να κάνουν:

- ότι τους επιτάσσει ο νόμος (δέσμια αρμοδιότητα), ή
- ότι τους επιτρέπει ο νόμος (διακριτική ευχέρεια)

Η δημόσια διοίκηση απαγορεύεται να ενεργήσει εκτός ή πέρα από το νόμο και επιβάλλεται να ενεργεί σύμφωνα με το νόμο. Οι πράξεις της ελέγχονται δικαστικά (κυρίως), και όταν ενεργεί με διακριτική ευχέρεια πραγματοποιείται έλεγχος ακραίων ορίων. Αντίθετα, ένα ιδιώτης ή μια επιχείρηση έχει ευρύτερο πεδίο δράσης καθώς μπορεί να κάνει ό,τι δεν απαγορεύει κανόνας δικαίου ή ό,τι δεν αντίκειται σε αυτόν.

Η αρχή της νομιμότητας της δημόσιας διοίκησης έχει αποτυπωθεί και στο άρθρο 6 του ΓΚΠΔ, με:

1. την ρητή πρόβλεψη ότι η νομική βάση του υπέρτερου εννόμου συμφέροντος δεν μπορεί να εφαρμοστεί στην επεξεργασία που διενεργείται από δημόσιες



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αρχές κατά την άσκηση των καθηκόντων τους.

2. Τη διάταξη της παραγράφου 3 του άρθρου αυτού η οποία προσδιορίζει με ποιο τρόπο πρέπει να χρησιμοποιούνται από δημόσιες φορείς οι νομικές βάσεις της «συμμόρφωσης με έννομη υποχρέωση» (άρ. 6 παρ. 1 γ') και της «επεξεργασίας απαραίτητης για την εκπλήρωση δημοσίου καθήκοντος» (άρ. 6 παρ. 1 γ').

Για την εφαρμογή των δύο παραπάνω νομικών βάσεων (οι οποίες είναι αυτές που κατά κανόνα χρησιμοποιούνται από τους δημόσιους φορείς) απαιτείται η επεξεργασία να προκύπτει από το εθνικό ή το ευρωπαϊκό δίκαιο, άρα να προβλέπεται σε διάταξη νόμου[9]. Η διάταξη ακολουθεί τη νομολογία του ΕΔΔΑ και προσδιορίζει χαρακτηριστικά τα οποία πρέπει να πληροί η εν λόγω διάταξη νόμου. Συγκεκριμένα:

- Ο σκοπός της επεξεργασίας πρέπει να καθορίζεται στη διάταξη.
    - Σε περίπτωση που η βάση είναι η περ. γ΄, ο σκοπός πρέπει να προκύπτει ευθέως από τη διάταξη.
    - Σε περίπτωση όμως που είναι η περ. ε' ο σκοπός της επεξεργασίας μπορεί να προκύπτει από μια διάταξη που αποδίδει σε ένα δημόσιο φορέα μια αρμοδιότητα, εφόσον η επεξεργασία είναι αναγκαία για την εκπλήρωση του καθήκοντος του δημοσίου φορέα, το οποίο πρέπει να εκτελείται προς το δημόσιο συμφέρον, ή κατά την άσκηση δημόσιας εξουσίας.
- Με βάση το ΓΚΠΔ, στη νομική βάση της περ. ε' γίνεται αναφορά ότι «*μπορεί*» να περιλαμβάνει ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του κανονισμού. Οι διατάξεις αυτές «μπορεί» να προσδιορίζουν αναλυτικότερα τα χαρακτηριστικά της επεξεργασίας και συγκεκριμένα:
    - τις γενικές προϋποθέσεις που διέπουν τη σύννομη επεξεργασία
    - τα είδη των δεδομένων που υποβάλλονται σε επεξεργασία
    - τις κατηγορίες υποκειμένων των δεδομένων τα οποία αφορά η επεξεργασία
    - τις οντότητες στις οποίες μπορούν να κοινοποιούνται τα δεδομένα και

[9] Υπενθυμίζουμε ότι εδώ χρησιμοποιούμε την ευρεία ερμηνεία που συμπεριλαμβάνει π.χ. και Υπουργικές Αποφάσεις οι οποίες εκδίδονται με κατάλληλη εξουσιοδότηση.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τους σκοπούς της κοινοποίησης

- τον περιορισμό του σκοπού
- τις περιόδους αποθήκευσης
- τις πράξεις επεξεργασίας και τις διαδικασίες επεξεργασίας, συμπεριλαμβανομένων των μέτρων για τη διασφάλιση σύννομης και θεμιτής επεξεργασίας (π.χ. μέτρα ασφάλειας)

Η αναφορά «*μπορεί να περιλαμβάνει*» δεν εισάγει υποχρέωση του Κ-Μ ώστε κάθε διάταξη στην οποία βασίζεται μια επεξεργασία προσωπικών δεδομένων να διαθέτει τα παραπάνω χαρακτηριστικά, αλλά είναι μια ισχυρή παρότρυνση στα Κ-Μ να νομοθετούν κατ' αυτόν τον τρόπο. Θα δούμε όμως στη συνέχεια, ότι όσον αφορά τις ειδικές κατηγορίες προσωπικών δεδομένων, είναι σχεδόν απαραίτητο μια διάταξη να έχει τα παραπάνω χαρακτηριστικά.

Η ΑΠΔΠΧ, όταν γνωμοδοτεί για διατάξεις που εισάγουν υποχρεώσεις για επεξεργασία δεδομένων προσωπικού χαρακτήρα, ακολουθεί παρόμοια λογική. Η Αρχή επισημαίνει (βλ. ενδεικτικά [31]) ότι η επεξεργασία, στο βαθμό που συνιστά περιορισμό του ατομικού δικαιώματος του πληροφοριακού αυτοκαθορισμού, πρέπει να ορίζεται γενικώς και αντικειμενικώς με τυπικό νόμο ή κατόπιν ειδικής νομοθετικής εξουσιοδότησης με διάταγμα, να δικαιολογείται από αποχρώντες λόγους δημοσίου συμφέροντος, να τελεί σε πρόδηλη λογική συνάφεια με τον επιδιωκόμενο σκοπό, να είναι πρόσφορη, κατάλληλη και αναγκαία για την επίτευξη του σκοπού αυτού, να μην θίγει τον πυρήνα του δικαιώματος και να μην απονέμει στη Διοίκηση ευρεία διακριτική ευχέρεια. Κατά συνέπεια, είναι απαραίτητο η επεξεργασία να προβλέπεται σε νομοθετική διάταξη, η οποία θα προσδιορίζει τα βασικά χαρακτηριστικά της επεξεργασίας, δηλαδή:

- τον υπεύθυνο επεξεργασίας,
- το σκοπό της επεξεργασίας,
- τις κατηγορίες των δεδομένων τα οποία θα τύχουν επεξεργασίας
- το χρόνο τήρησης των δεδομένων ή τα κριτήρια για τον προσδιορισμό του και
- τους αποδέκτες των δεδομένων.

Με ειδικότερη νομοθετική εξουσιοδότηση επιτρέπεται να ανατεθεί στον κανονιστικό νομοθέτη (π.χ. Υπουργική Απόφαση) η ρύθμιση ειδικότερων, τεχνικών



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ή λεπτομερειακών θεμάτων, όπως ο σχεδιασμός και οι τεχνικές και λειτουργικές προδιαγραφές συγκεκριμένων συστημάτων, τα οργανωτικά και τεχνικά μέτρα για την ασφάλεια της επεξεργασίας των δεδομένων, και κάθε άλλη αναγκαία λεπτομέρεια.

Συνεπώς, με βάση τα παραπάνω, η διαδικασία επιλογής νομικής βάσης ενός δημόσιου φορέα, για τις δραστηριότητες που εντάσσονται στις αρμοδιότητές του, είναι ευκολότερη από ενός ιδιωτικού. Από τις έξι πιθανές νομικές βάσεις, έχει τελικά να αξιολογήσει ποια είναι η κατάλληλη νομική βάση από …

- …Πέντε νομικές βάσεις, γιατί κατά κανόνα εξαιρείται το υπέρτερο έννομο συμφέρον[10],
- …Τέσσερις νομικές βάσεις, γιατί η συγκατάθεση έχει σπάνια εφαρμογή[11].
- …Τρεις, γιατί το ζωτικό συμφέρον εφαρμόζεται σε περιορισμένες και συγκεκριμένες επείγουσες περιπτώσεις
- …Δύο, γιατί η σύμβαση έχει συγκεκριμένο πλαίσιο εφαρμογής, όταν ο δημόσιος φορέας συμβάλλεται με φυσικά ή νομικά πρόσωπα (αλλά και πάλι οι υποχρεώσεις του προκύπτουν από διατάξεις νόμου).

Συνεπώς, ένας δημόσιος φορέας πρέπει, κατά κανόνα, να επιλέγει είτε τη νομική βάση της έννομης υποχρέωσης, είτε της άσκησης δημόσιου καθήκοντος.

☞ Συμπερασματικά: όταν Δημόσιος Φορέας εκτελεί επεξεργασία προσωπικών δεδομένων με δέσμια αρμοδιότητα (επειδή το ορίζει ρητά ο νόμος) είναι πολύ πιθανό να εφαρμόζεται η νομική βάση της «έννομης υποχρέωσης» (αρ. 6 παρ, 1 γ' ΓΚΠΔ), ενώ όταν εκτελεί επεξεργασία προσωπικών δεδομένων επειδή κρίνει ότι αυτή είναι απαραίτητη για την εκτέλεση της αρμοδιότητάς του, ακόμα κι αν δεν το ορίζει ρητά ο νόμος, εφαρμόζεται η νομική βάση της «εκπλήρωση δημοσίου καθήκοντος» (αρ. 6 παρ, 1 γ' ΓΚΠΔ).

[10]Η εν λόγω νομική βάση εξαιρείται για επεξεργασίες που διενεργούνται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους. Ενδεχομένως να μπορεί να χρησιμοποιηθεί

[11] Δεν αποκλείεται η συγκατάθεση ως νομική βάση, αλλά δεν είναι συνήθης (π.χ. είναι η περίπτωση όπου πολίτης δηλώνει την ηλεκτρονική του διεύθυνση για να λαμβάνει ενημερωτικά δελτία που εκδίδει τακτικά ο φορέας). Πάντως, εάν νόμος περιγράφει μία επεξεργασία και την καθιστά προαιρετική για τους πολίτες, με βάση την επιθυμία τους, τότε η νομική βάση για την επεξεργασία δεν είναι η συγκατάθεση αλλά η εκπλήρωση εκ του νόμου υποχρέωσης.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Ερώτηση δραστηριότητας**: Οι Οικονομικοί Ελεγκτές του Δημοσίου έχουν τη δυνατότητα διενέργειας ελέγχων περιουσιακής κατάστασης σε υπαλλήλους του Δημοσίου. Μετά από καταγγελία στην αρμόδια ελεγκτική αρχή, αποκαλύπτεται ότι υπάλληλος ο οποίος είχε πρόσφατα παραιτηθεί, ενδέχεται να έχει αύξηση στην περιουσιακή του κατάσταση η οποία δεν δικαιολογείται από τις δηλώσεις του.
Θεωρείτε ότι είναι νόμιμη η επεξεργασία των προσωπικών δεδομένων του πρώην υπαλλήλου ώστε να του καταλογιστεί (πειθαρχική) παράβαση κατά την άσκηση των καθηκόντων του;
Αν ναι, ποια είναι η καταλληλότερη νομική βάση;
Αν όχι, ποια ενέργεια θα μπορούσε να γίνει;
Για βοήθεια δείτε τη γνωμοδότηση 3/2013 της ΑΠΔΠΧ.

### 5.3.1 Επεξεργασία για άλλους σκοπούς από δημόσιο φορέα

Ήδη κατά την παρουσίαση της αρχής του περιορισμού του σκοπού είδαμε ότι η επεξεργασία των προσωπικών δεδομένων δεν μπορεί να επεκταθεί σε σκοπούς διαφορετικούς από αυτόν για τον οποίο έχει γίνει η αρχική συλλογή, εκτός κι αν ο νέος σκοπός είναι συμβατός με τον αρχικό. Στο άρθρο 6 παρ. 4 του ΓΚΠΔ η αρχή αυτή προσδιορίζεται ακόμα περισσότερο, καθώς παραθέτονται κριτήρια για να μπορεί ένας υπεύθυνος επεξεργασίας να κρίνει αν ο νέος σκοπός είναι συμβατός με τον αρχικό. Βέβαια, αν το υποκείμενο των δεδομένων παράσχει συγκατάθεση ή αν επεξεργασία βασίζεται σε νόμο για συγκεκριμένους σκοπούς υψηλής σπουδαιότητας (όπως αναφέρονται στο άρθρο 23 του ΓΚΠΔ), επιτρέπεται στον υπεύθυνο επεξεργασία να προβαίνει στην περαιτέρω επεξεργασία, ανεξάρτητα από τη συμβατότητα των σκοπών. Διαφορετικά η συμβατότητα του «νέου» σκοπού εξετάζεται με τα εξής (ενδεικτικά) κριτήρια αλλά με την ίδια νομική βάση όπως σε σχέση με την αρχική συλλογή των δεδομένων:

- τη σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας
- το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία
- τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων
- την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση (βλ. σχετικώς την Ενότητα 10).

Η παραπάνω στάθμιση πρέπει να γίνεται κατά περίπτωση και είναι αρκετές φορές δυσχερής. Επισημαίνεται ότι στα άρθρα 24 και 26 του νόμου 4624/2019 ο εθνικός νομοθέτης προσπάθησε να εισάγει περιπτώσεις κατά τις οποίες είναι νόμιμη η περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα από δημόσιους φορείς, δημιουργώντας στην πράξη νέες νομικές βάσεις. Η Αρχή με τη γνωμοδότηση 1/2020 [18] έκρινε ότι οι εν λόγω διατάξεις του νόμου αυτού δεν έχουν θεσπιστεί σύμφωνα με τις διατάξεις του ΓΚΠΔ, συνεπώς δεν θα πρέπει να λαμβάνονται υπόψη για την κρίση σε σχέση με την συμβατότητα μιας περαιτέρω επεξεργασίας. Οι διατάξεις των άρθρων αυτών μπορεί να χρησιμεύσουν ως ενδεικτικές περιπτώσεων στις οποίες ένας δημόσιος φορέας μπορεί να προβεί σε περαιτέρω επεξεργασία προσωπικών δεδομένων αλλά

α) η περαιτέρω επεξεργασία προσωπικών δεδομένων από δημόσιους φορείς δεν μπορεί να περιοριστεί μόνο στις περιπτώσεις που αναφέρουν τα εν λόγω άρθρα, και

β) η περαιτέρω επεξεργασία προσωπικών δεδομένων από δημόσιους φορείς ακόμα και για περιπτώσεις που ρητά αναγράφονται στα άρθρα 24 και 26 του ν. 4624/2019 θα πρέπει να αξιολογείται ειδικά με βάση τα κριτήρια που προαναφέρθηκαν.

Συνεπώς, ένας δημόσιος φορέας, όταν επιθυμεί να χρησιμοποιήσει δεδομένα που ήδη διαθέτει για ένα συγκεκριμένο σκοπό πρέπει να αξιολογήσει αυτή την περαιτέρω επεξεργασία απαντώντας στα πιο κάτω ερωτήματα:

1) Είναι η νομική βάση για τη νέα επεξεργασία η ίδια με αυτή της αρχικής συλλογής δεδομένων; Εξαιρούνται η συγκατάθεση (καθώς απαιτείται πάντα νέα συγκατάθεση) και οι νομικές βάσεις (περιπτώσεις γ' και ε') που βασίζονται σε διάταξη νόμου όταν ο νόμος αυτός αφορά επεξεργασία για την οποία μπορεί να περιοριστούν δικαιώματα με βάση το άρθρο 23 του ΓΚΠΔ.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

2) Είναι αναμενόμενο για το υποκείμενο των δεδομένων ότι τα δεδομένα που έχουν αρχικά συλλεγεί για ένα σκοπό, θα χρησιμοποιηθούν και για το νέο σκοπό;
3) Αφορά η επεξεργασία δεδομένα προσωπικού χαρακτήρα τα οποία δεν περιλαμβάνονται στα δεδομένα ειδικών κατηγοριών ή στα δεδομένα ποινικών καταδικών και αδικημάτων;
4) Ποιες είναι οι συνέπειες σε σχέση με τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων; Έχει εξεταστεί ότι δεν ενδέχεται να τους δημιουργηθεί απρόβλεπτη συνέπεια ή βάρος;
5) Λαμβάνονται μέτρα για την προστασία των δεδομένων, ιδίως με τη λογική της αρχής της ελαχιστοποίησης των δεδομένων;

Ανάλογα με τις απαντήσεις στις παραπάνω ερωτήσεις, αν για παράδειγμα οι απαντήσεις στα παραπάνω ερωτήματα είναι καταφατικές, ο δημόσιος φορέας μπορεί να προχωρήσει στη νέα επεξεργασία. Με βάση την αρχή της λογοδοσίας είναι, επίσης. απαραίτητο να τηρηθεί έγγραφη τεκμηρίωση της αξιολόγησης του συμβατού της περαιτέρω επεξεργασίας.

Υπενθυμίζουμε ότι επεξεργασίες για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς θεωρούνται κατ' αρχήν συμβατοί σκοποί, αρκεί να λαμβάνονται κατάλληλες διασφαλίσεις.

**Παράδειγμα 1:** Δήμος διατηρεί ιστοσελίδα στην οποία υποβάλλονται αιτήσεις δημοτών και κατοίκων. Οι πολίτες ενημερώνονται ότι τα δεδομένα τους θα τηρηθούν για πέντε έτη, για το σκοπό της διεκπεραίωσης των αιτημάτων τους καθώς η ορθότητα της απάντησης στην αίτηση μπορεί να ελεγχθεί για το χρονικό διάστημα αυτό. Τρία χρόνια μετά τη λειτουργία της ιστοσελίδας, ο Δήμος επιθυμεί να προβεί σε στατιστική ανάλυση της συμπεριφοράς των δημοτών και πολιτών της. Καθώς η κατάρτιση στατιστικών συνιστά κατά κανόνα, συμβατό σκοπό, η περαιτέρω επεξεργασία επιτρέπεται. Δεν απαιτείται διαφορετική νομική βάση. Ωστόσο, για την περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα ο Δήμος πρέπει να παρέχει κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Στα τεχνικά και οργανωτικά μέτρα τα οποία πρέπει να εφαρμόσει ο Δήμος μπορεί να περιλαμβάνεται η ψευδωνυμοποίηση.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Παράδειγμα 2:** Δήμος διατηρεί ιστοσελίδα στην οποία υποβάλλονται αιτήσεις δημοτών και κατοίκων. Οι πολίτες ενημερώνονται ότι τα δεδομένα τους θα τηρηθούν για πέντε έτη, για το σκοπό της διεκπεραίωσης των αιτημάτων τους καθώς η ορθότητα της απάντησης στην αίτηση μπορεί να ελεγχθεί για το χρονικό διάστημα αυτό. Τρεις μήνες πριν τις δημοτικές εκλογές ο Δήμος εξετάζει αν μπορεί να χορηγήσει τα email των δημοτών στους υποψηφίους των συνδυασμών, ώστε όλοι αυτοί να αποστείλουν προωθητικό υλικό για την υποψηφιότητά τους. Η διαβίβαση δεδομένων από το Δήμο για σκοπούς πολιτικής επικοινωνίας των υποψηφίων του Δήμου (που είναι όμως τρίτοι) συνιστά μετέπειτα χρήση των δεδομένων για νέο σκοπό, ο οποίος είναι ασύμβατος με την αρχική συλλογή και τήρηση των δεδομένων. Επομένως, η διαβίβαση των δεδομένων σε υποψηφίους για το Δήμο (ακόμα και αν ήταν προς όλους) απαιτεί χωριστή νομική βάση και δεν μπορεί να εκτελεστεί.

## 5.4 Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων

Όπως είδαμε νωρίτερα, κάποιες κατηγορίες προσωπικών δεδομένων αποτελούν τις «ειδικές κατηγορίες» δεδομένων προσωπικού χαρακτήρα. Αυτές, καθώς θεωρούνται ότι μόνο από τη φύση τους, ενδέχεται να ενέχουν κίνδυνο για τα υποκείμενα των δεδομένων όταν υποβάλλονται σε επεξεργασία, και απαιτούν αυξημένη προστασία. Ο ΓΚΠΔ, ακολουθώντας τη λογική της οδηγίας 95/46/ΕΚ, έχει ειδική διάταξη για το χειρισμό των δεδομένων αυτών – συγκεκριμένα, το άρθρο 9.

### 5.4.1 Προϋποθέσεις για την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων

Η βασική διαφορά της διάταξης αυτής είναι ότι δηλώνεται ότι «κατ' αρχήν», η επεξεργασία των ειδικών κατηγοριών προσωπικών δεδομένων απαγορεύεται! Για να μπορεί ένας υπεύθυνος επεξεργασίας να επεξεργαστεί τέτοια δεδομένα θα πρέπει να χρησιμοποιήσει μια από τις εξαιρέσεις από την απαγόρευση οι οποίες περιγράφονται στην παράγραφο 2 του άρθρου 9 του ΓΚΠΔ. Μάλιστα, καθώς ο κανόνας είναι η απαγόρευση, οι εξαιρέσεις αυτές, που επιτρέπουν την επεξεργασία, πρέπει να ερμηνεύονται «στενά» συσταλτικά. Πρόκειται για δέκα συνολικά «προϋποθέσεις» για την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων τις οποίες θα δούμε



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

πιο αναλυτικά στη συνέχεια:

#### 5.4.1.1 Συγκατάθεση

Η περίπτωση α' του άρθρου 9 παρ. 2 αναφέρει: «*…το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων*».

Πρακτικά, η διάταξη αναφέρει το προφανές: Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων μπορεί να γίνει όταν το υποκείμενο των δεδομένων έχει συγκατατεθεί. Προσοχή όμως: γίνεται αναφορά σε «ρητή» (explicit) συγκατάθεση[12]. Δηλαδή, απαιτείται μια πιο «ισχυρή» μορφή συγκατάθεσης, η οποία να δηλώνεται απόλυτα, ξεκάθαρα και με λεπτομέρεια, και να μην αφήνει κανένα περιθώριο παρερμηνείας. Δεν αρκεί δηλαδή να είναι σε θέση να την αποδείξει ο υπεύθυνος επεξεργασίας. Η καλύτερη απόδειξη για τη συγκατάθεση σε περίπτωση ειδικών κατηγοριών προσωπικών δεδομένων είναι η γραπτή συγκατάθεση. Βέβαια, όπως και στα «απλά» προσωπικά δεδομένα, η συγκατάθεση για το δημόσιο τομέα δεν είναι κατάλληλη προϋπόθεση, στις πιο πολλές περιπτώσεις. Στην ενότητα για τη συγκατάθεση που ακολουθεί, θα αναλύσουμε περισσότερο την έννοια της συγκατάθεσης.

#### 5.4.1.2 Δεδομένα για σκοπούς εργατικού δικαίου, δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας

Η περίπτωση β' του άρθρου 9 παρ. 2 αναφέρει: «*…η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία*

[12] Στο αρχικό ελληνικό κείμενο του ΓΚΠΔ, δεν διακρίνεται διαφορά μεταξύ του ορισμού της συγκατάθεσης στο άρθρο 4 και της αναφοράς στη συγκατάθεση του άρθρου 9 (και στα δύο σημεία, γινόταν αναφορά σε ρητή συγκατάθεση). Ωστόσο, το πρωτότυπο κείμενο στα αγγλικά του ΓΚΠΔ αναφέρεται σε «unambiguous» συγκατάθεση στο άρθρο 4 και σε «explicit» συγκατάθεση στο άρθρο 9. Η διαφορά διορθώθηκε με το Διορθωτικό, ΕΕ L 074, 4.3.2021, σ. 35 (2016/679)



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων*».

Η προϋπόθεση αυτή διευκολύνει την επεξεργασία ειδικών κατηγοριών δεδομένων όταν αυτό είναι απαραίτητο με βάση:

- διατάξεις νόμου που αφορούν ζητήματα εργατικά, κοινωνικής ασφάλισης ή κοινωνικής προστασίας ή
- από συλλογική συμφωνία, όπως π.χ. στη χώρα μας για τους σκοπούς της σύμβασης εργασίας βάσει συλλογικών συμβάσεων εργασίας.

Διευκολύνει επίσης την επεξεργασία δεδομένων από δημόσιους φορείς για σκοπούς όμως οι αναρρωτικές άδειες, γονικές, άδειες, άδειες ή παροχές για ΑΜΕΑ, ηλικιωμένους, παροχές σε σχέση με εργατικά ατυχήματα, ανεργία, κοινωνικά μειονεκτήματα κ.ά. Δεν είναι όμως η καταλληλότερη προϋπόθεση για ζητήματα υγείας ή περίθαλψης, καθώς υπάρχει ειδικότερη προϋπόθεση.

**Παράδειγμα**: Δημόσιος φορέας που τηρεί αρχείο προσωπικού, χρησιμοποιεί την εξαίρεση αυτή, καθώς του δίνεται η δυνατότητα επεξεργασίας δεδομένων υγείας για την παροχή αναρρωτικών αδειών ή πληροφοριών για ένα συνδικαλιστή, ώστε να του παρέχονται οι διευκολύνσεις που παρέχει η σχετική νομοθεσία.

#### 5.4.1.3 Ζωτικό συμφέρον

Η περίπτωση γ' του άρθρου 9 παρ. 2 αναφέρει: *«…η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να παράσχει συγκατάθεση».*

Η προϋπόθεση αυτή μοιάζει πάρα πολύ με τη νομική βάση του άρθρου 6 παρ. 1 εδαφ. δ', για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου. Η διαφορά σε σχέση με τη νομική βάση είναι ότι η εξαίρεση μπορεί να εφαρμοστεί μόνο εφόσον το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να παράσχει συγκατάθεση.

**Παράδειγμα**: Με την εξαίρεση αυτή δίνεται η δυνατότητα επεξεργασίας δεδομένων

υγείας όταν ο ασθενής δεν είναι σε θέση να παράσχει συγκατάθεση, όπως σε ένα ατύχημα. Αντίθετα, δεν μπορεί να γίνει χρήση της εξαίρεσης, αν, ακόμα κι αν διακυβεύεται το ζωτικό συμφέρον του υποκειμένου των δεδομένων αυτό μπορεί να επικοινωνήσει ώστε να είναι σε θέση να συγκατατεθεί. Βέβαια, αυτό δεν σημαίνει ότι δεν μπορεί να εφαρμοστεί άλλη εξαίρεση για την επεξεργασία δεδομένων υγείας, όμως της περίπτωσης η'.

#### 5.4.1.4 Μη κερδοσκοπικές ενώσεις, σωματεία, πολιτικά κόμματα

Η περίπτωση δ' του άρθρου 9 παρ. 2 αναφέρει: «*...η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων*».

Η προϋπόθεση αυτή δίνει τη δυνατότητα σε ιδρύματα και οργανώσεις μη κερδοσκοπικού χαρακτήρα των οποίων οι δραστηριότητες συνδέονται άμεσα με ειδικές κατηγορίες δεδομένων, να επεξεργάζονται τα δεδομένα των μελών τους ή των φίλων τους. Επιπλέον προϋπόθεση για την επεξεργασία αποτελεί το ότι τα δεδομένα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα παρά μόνο αν συγκατατεθεί το υποκείμενο των δεδομένων. Με τον τρόπο αυτό διευκολύνεται η λειτουργία, συνδικαλιστικών οργανώσεων, πολιτικών κόμματων, ιδρυμάτων και ενώσεων κ.α. άλλων μη κερδοσκοπικών φορέων, η συμμετοχή και μόνο στους οποίους αποκαλύπτει ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.

**Παράδειγμα**: Η συμμετοχή ενός εργαζόμενου σε συνδικαλιστικό σωματείο, συνεπάγεται την επεξεργασία ειδικής κατηγορίας προσωπικών δεδομένων. Αν η πληροφορία των προσώπων που συμμετέχουν στο σωματείο παραμένει εντός του σωματείου, δεν υφίσταται κανένα πρόβλημα από τη νομοθεσία για τα προσωπικά δεδομένα.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

#### 5.4.1.5 Πρόδηλη δημοσιοποίηση

Η περίπτωση ε' του άρθρου 9 παρ. 2 αναφέρει: «*...η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων*». Για την εφαρμογή αυτής της εξαίρεσης, πρέπει να ισχύουν τα παρακάτω:

- Τα δεδομένα να έχουν καταστεί διαθέσιμα δημόσια. Δημόσια σημαίνει ότι ο οποιοσδήποτε να είναι σε θέση να τα προσπελάσει, χωρίς κάποια ιδιαίτερη προϋπόθεση.
- Η δημοσιοποίηση να έχει γίνει από το ίδιο το υποκείμενο των δεδομένων. Αν έχει γίνει από άλλο πρόσωπο, δεν μπορεί να εφαρμοστεί η εξαίρεση.
- Να είναι σαφές ότι το υποκείμενο των δεδομένων είχε πλήρη επίγνωση ότι κατέστησε τα δεδομένα δημόσια. Αν η δημοσιοποίηση είναι αποτέλεσμα λάθους ή έγινε από ακούσια ενέργεια του υποκειμένου των δεδομένων, δεν θεωρείται ότι είναι «προδήλως» δημοσιοποιημένα.
-

**Παράδειγμα 1**: Φυσικό πρόσωπο ανακοινώνει στα μέσα κοινωνικής δικτύωσης ότι θα επιδιώξει την υποψηφιότητά του με συγκεκριμένο πολιτικό κόμμα. Στην περίπτωση αυτή, αν και τα δεδομένα πολιτικών πεποιθήσεων ανήκουν στις ειδικές κατηγορίες, είναι προφανές ότι το υποκείμενο των δεδομένων επέλεξε να τα δημοσιοποιήσει.

**Παράδειγμα 2**: Συνδικαλιστικός φορέας του δημοσίου αναρτά από λάθος (ακούσια παραβίασης δεδομένων προσωπικού χαρακτήρα) τα ονόματα κάποιων μελών του σε δημόσια ιστοσελίδα. Καθώς τα δεδομένα δεν έχουν δημοσιοποιηθεί από τα υποκείμενα των δεδομένων, δεν μπορεί να εφαρμοστεί η εν λόγω εξαίρεση.

Επισημαίνουμε ότι σε περίπτωση που υπεύθυνος επεξεργασίας χρησιμοποιεί τέτοια δεδομένα, οφείλει, με βάση την αρχή της λογοδοσίας, να τηρεί στοιχεία για την προέλευση των δεδομένων. Επίσης, η πρόδηλη δημοσιοποίηση παρέχει μόνο την



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προϋπόθεση για την επεξεργασία των ειδικών κατηγοριών δεδομένων, χωρίς αυτό να σημαίνει ότι ο υπεύθυνος επεξεργασίας δεν οφείλει να ικανοποιεί και τις λοιπές προϋποθέσεις νομιμότητας, π.χ. την αρχή της διαφάνειας.

#### 5.4.1.6 Νομικές αξιώσεις

Η περίπτωση στ' του άρθρου 9 παρ. 2 αναφέρει: «*...η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαστική τους ιδιότητα*». Η εξαίρεση αυτή δίνει τη δυνατότητα σε υπευθύνους επεξεργασίας οι οποίοι είναι απαραίτητο να επεξεργαστούν ειδικές κατηγορίες προσωπικών δεδομένων (τις οποίες συνήθως κατέχουν ως μέρος νόμιμης επεξεργασίας για διαφορετικό σκοπό) σε νομικές διαδικασίες στα δικαστήρια, να τα χρησιμοποιήσουν ανεμπόδιστα. Κρίσιμο για την εφαρμογή της εξαίρεσης αυτής είναι να μπορεί να αποδειχθεί η αναγκαιότητα της χρήσης των δεδομένων για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

**Παράδειγμα**: Δημόσιο νοσοκομείο πρέπει να υπερασπιστεί σε δικαστήριο την ιατρική διαδικασία που ακολούθησε, κατόπιν αγωγής ασθενούς του. Το Νοσοκομείο, δια των δικηγόρων του, μπορεί να χρησιμοποιήσει στοιχεία από το φάκελο του συγκεκριμένου ασθενούς ώστε να αποδείξει ότι παρείχε την ενδεδειγμένη ιατρική φροντίδα, δεδομένων των συνθηκών.

Η εν λόγω προϋπόθεση αφορά επίσης την επεξεργασία ειδικών κατηγοριών δεδομένων από δικαστήρια. Όπως είναι προφανές, εφόσον ειδικές κατηγορίες προσωπικών δεδομένων αποτελούν αντικείμενο επεξεργασίας από δικαστήρια, στο πλαίσιο δικαστικών διαδικασιών, μπορεί να εφαρμοστεί η εν λόγω εξαίρεση.

#### 5.4.1.7 Ουσιαστικό δημόσιο συμφέρον

Η περίπτωση ζ' του άρθρου 9 παρ. 2 αναφέρει «*...η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*συμφερόντων του υποκειμένου των δεδομένων*». Για την εφαρμογή της προϋπόθεσης αυτής απαιτείται:

- Νομοθετική διάταξη
- Η διάταξη να προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων (αντίστοιχα με το άρθρο 6 παρ. 4 του Κανονισμού).
- Σκοπό ουσιαστικού δημοσίου συμφέροντος. Ο ΓΚΠΔ δεν προσδιορίζει ρητά ποιοι είναι αυτοί οι σκοποί, αν και μπορεί να γίνει αναφορά στο άρθρο 23 παρ. 1 του Κανονισμού για να σκοπούς που κατά κανόνα θεωρούνται «ουσιαστικού» δημοσίου συμφέροντος[13].

Ο υπεύθυνος επεξεργασίας του δημόσιου τομέα που επιθυμεί να χρησιμοποιήσει την εν λόγω προϋπόθεση οφείλει, με βάση την αρχή της λογοδοσίας, να έχει τεκμηριώσει εγγράφως σε κατάλληλη πολιτική τη συνδρομή της προϋπόθεσης αυτής.

**Παράδειγμα**: Δημόσιοι φορείς μπορεί να έχουν συγκεκριμένες υποχρεώσεις, που τίθενται με διατάξεις νόμου, για την προστασία εθνικών μειονοτήτων. Στο πλαίσιο των υποχρεώσεων αυτών μπορεί με νόμο να προβλέπεται και επεξεργασία ειδικών κατηγοριών δεδομένων.

#### 5.4.1.8 Υγεία – κοινωνική πρόνοια

Η περίπτωση η' του άρθρου 9 παρ. 2 αναφέρει «*...η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει*

[13] Βλ. και υποθέσεις C-340/14 and C-341/14 του ΔΕΕ, για τους επιτακτικούς λόγους δημοσίου συμφέροντος όπου ως "επιτακτικοί λόγοι δημόσιου συμφέροντος" νοούνται οι λόγοι που αναγνωρίζονται ως τέτοιοι στη νομολογία του Δικαστηρίου, συμπεριλαμβανομένων των ακόλουθων λόγων: δημόσια τάξη· δημόσια ασφάλεια· δημόσια υγεία· προστασία της χρηματοοικονομικής ισορροπίας του συστήματος κοινωνικών ασφαλίσεων· προστασία των καταναλωτών, των αποδεκτών υπηρεσιών και των εργαζομένων· δικαιοσύνη των εμπορικών συναλλαγών· καταπολέμηση της απάτης· προστασία του περιβάλλοντος, περιλαμβανομένου του αστικού περιβάλλοντος· υγεία των ζώων· διανοητική ιδιοκτησία· διατήρηση της εθνικής ιστορικής και καλλιτεχνικής κληρονομιάς· στόχοι κοινωνικής πολιτικής και στόχοι πολιτιστικής πολιτικής·

*σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3*».

Οι φορείς (δημόσιοι και ιδιωτικοί) που ασχολούνται με την παροχή υπηρεσιών υγείας και κοινωνικής πρόνοιας επεξεργάζονται κατά κανόνα δεδομένα υγείας, καθώς τα δεδομένα αυτά βρίσκονται στον πυρήνα των δραστηριοτήτων τους. Η προϋπόθεση αυτή δίνει τη δυνατότητα στους εν λόγω φορείς να επεξεργάζονται τα δεδομένα υγείας που τους είναι απαραίτητα είτε βάσει νόμου (π.χ. κώδικας ιατρικής δεοντολογίας) είτε/και λόγω της σύμβασης του ασθενούς/λήπτη υπηρεσιών υγείας με τον φορέα. Μάλιστα καλύπτει όλο το εύρος των δραστηριοτήτων των εν λόγω φορέων, καθώς καλύπτονται σκοποί επεξεργασίας που αφορούν σε προληπτική ιατρική, αξιολόγηση ικανότητας εργασίας ενός εργαζομένου, ιατρική διάγνωση, παροχή υγειονομικής περίθαλψης ή θεραπείας, παροχή κοινωνικής φροντίδας, διαχείριση συστημάτων ή υπηρεσιών υγειονομικής περίθαλψης ή συστημάτων και υπηρεσιών κοινωνικής φροντίδας, κ.ά.. Ο φορέας μπορεί να βασιστεί στην εξαίρεση αυτή μόνο εφόσον τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία από επαγγελματία που υπόκειται σε υποχρέωση επαγγελματικού απορρήτου ή από άλλο πρόσωπο (π.χ. βοηθό) το οποίο ενεργεί υπό την ευθύνη του επαγγελματία.

**Παράδειγμα**: Δημόσιο νοσοκομείο οφείλει να τηρεί τα δεδομένα υγείας των ασθενών του με βάση την ιατρική νομοθεσία. Η καταλληλότερη προϋπόθεση για την επεξεργασία των δεδομένων αυτών είναι η περ. η' του άρθρου 9 παρ. 2. Για την εφαρμογή της, η επεξεργασία πρέπει να γίνει υπό την ευθύνη ιατρικού ή νοσηλευτικού προσωπικού (ή άλλου προσωπικού που υπόκειται σε ειδικό επαγγελματικό απόρρητο).

#### 5.4.1.9 Δημόσιο συμφέρον στον τομέα της δημόσιας υγείας

Η περίπτωση θ' του άρθρου 9 παρ. 2 αναφέρει «*...η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου*».

Η προϋπόθεση αυτή αφορά επίσης τα δεδομένα υγείας, αλλά στοχεύει σε άλλους φορείς από αυτούς της παροχής υπηρεσιών υγείας στο υποκείμενο των δεδομένων. Για την εφαρμογή της απαιτείται η επεξεργασία να είναι απαραίτητη για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας. Ο όρος «δημόσιο συμφέρον» δεν ορίζεται στο ΓΚΠΔ αν και επισημαίνεται ότι δεν γίνεται χρήση του όρου «ουσιαστικό δημόσιο συμφέρον» που θα ήταν πιο περιοριστικός. Ο εκάστοτε υπεύθυνος επεξεργασίας, πρέπει να είναι σε θέση να τεκμηριώσει ότι το όφελος από την επεξεργασία αφορά το ευρύτερο κοινό ή την κοινωνία στο σύνολό της και όχι τα δικά του συμφέροντα ή τα συμφέροντα συγκεκριμένου ατόμου. Είναι μια εξαίρεση που μπορεί να χρησιμοποιείται κυρίως από δημόσιους φορείς όπως ο Ε.Ο.Δ.Υ., το Υπουργείο Υγείας, ο Ε.Ο.Φ. αλλά και φαρμακευτικές εταιρίες, καθώς μπορεί να περιλαμβάνει την παρακολούθηση της δημόσιας υγείας και σχετικές στατιστικές, το σχεδιασμό πόρων των νοσοκομείων, τα δημόσια προγράμματα εμβολιασμού, την ανταπόκριση του κράτους σε νέες απειλές για τη δημόσια υγεία (π.χ. επιδημίες, πανδημίες ή νέα ερευνητικά ευρήματα), τη φαρμακοεπαγρύπνηση, τις κλινικές δοκιμές φαρμάκων ή ιατροτεχνολογικών προϊόντων κ.ά.

**Παράδειγμα**: Για την αντιμετώπιση της πανδημίας του κορονοϊού από τον ΕΟΔΥ και τη λειτουργία σχετικών βάσεων δεδομένων για την επιδημιολογική επιτήρηση του πληθυσμού, ο Ε.Ο.Δ.Υ. είναι καταλληλότερο να χρησιμοποιεί την εν λόγω εξαίρεση, καθώς αποτελεί τον κατ' εξοχήν φορέα για την προάσπιση της δημόσιας υγείας έναντι τέτοιων απειλών.

#### 5.4.1.10 Αρχειοθέτηση, έρευνα, στατιστική

Η περίπτωση ι' του άρθρου 9 παρ. 2 αναφέρει *«…η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων*».

Η τελευταία προϋπόθεση για την επεξεργασία ειδικών κατηγοριών δεδομένων επιβεβαιώνει ότι η Ε.Ε θέλει να διευκολύνει την επεξεργασία προσωπικών δεδομένων για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, οι οποίοι θεωρούνται κατ' αρχήν συμβατοί σκοποί. Και τούτο ακόμα και αν στα δεδομένα περιλαμβάνονται και ειδικές κατηγορίες δεδομένων. Η αναφορά στο άρθρο 89 του Κανονισμού δείχνει, ξανά, τη σημασία των μέτρων όπως η ψευδωνυμοποίηση για την ικανοποίηση των εν λόγω σκοπών, καθώς συνδέει τη νομιμότητα της επεξεργασίας με την υλοποίηση μέτρων για την ελαχιστοποίηση των δεδομένων.

**Παράδειγμα**: Νοσοκομείο διενεργεί έρευνα για νέες ιατρικές θεραπείες. Το νοσοκομείο είναι προτιμότερο να επιλέξει να επεξεργαστεί τα δεδομένα υγείας με την προϋπόθεση της επιστημονικής έρευνας. Για το σκοπό αυτό εφαρμόζει κατάλληλη διαδικασία ψευδωνυμοποίησης. Τηρώντας τα αναγνωριστικά των ασθενών που συμμετέχουν στην έρευνα σε διαχωρισμένα αρχεία, μπορεί να αντιστοιχεί τα νεότερα δεδομένα με τα παλαιότερα. Η συγκατάθεση δεν είναι κατάλληλη για τις περιπτώσεις αυτές, καθώς τυχόν ανάκλησή της θα οδηγούσε σε αλλαγή του δείγματος της έρευνας και θα δυσχέραινε την επίτευξη του σκοπού αυτής.

#### 5.4.1.11 Προσπάθεια για προσθήκη προϋποθέσεων για την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων στο άρθρο 22 του ν. 4624/2019.

Στο άρθρο 22 του ν. 4624/2019 ο εθνικός νομοθέτης προσπάθησε να διευκρινίσει υπό ποιες προϋποθέσεις και για ποιους λόγους είναι δυνατή η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, τα οποία αναφέρονται στα στοιχεία β, ζ, η, και θ, της παραγράφου 2 του άρθρου 9 ΓΚΠΔ, θεωρώντας ότι παρέχεται η δυνατότητα στα κράτη μέλη να καθορίζουν μέσω εθνικών ρυθμίσεων τις εξαιρέσεις στις εν λόγω περιπτώσεις. Η προσέγγιση αυτή κατακρίθηκε από την ΑΠΔΠΧ στη γνωμοδότηση 1/2020 (βλ. σελ. 11-14 [18]). Οι διατάξεις του εν λόγω άρθρου έχουν κριθεί ανεπαρκείς και, ως εκ τούτου. η συμβουλή των συγγραφέων είναι να γίνεται



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ορθή ανάλυση των προϋποθέσεων για την επεξεργασία των ειδικών κατηγοριών προσωπικών δεδομένων, όπως αναλυτικά ορίζονται στο άρθρο 9 παρ. 2 του ΓΚΠΔ. Άλλωστε οι εθνικές διατάξεις μόνο συμπληρωματικό ρόλο μπορούν να έχουν, ενώ σε πολλές από τις διατάξεις του άρθρου απλά επαναλαμβάνονται εδάφια του Κανονισμού - και μάλιστα όχι ολόκληρα.

Άλλωστε, τα Κ-Μ , με βάση την παρ. 4 του άρθρου 9, είχαν την δυνατότητα «*να διατηρούν ή να θεσπίζουν* ***περαιτέρω όρους****, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γ****ενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία****.*»

Η προσθήκη που με βεβαιότητα εφαρμόζεται έχει περιληφθεί στο άρθρο 23 του ν. 4624/2019 όπου ορίζεται ότι «*απαγορεύεται η επεξεργασία γενετικών δεδομένων για σκοπούς ασφάλισης υγείας και ζωής*». Αυτή είναι μια ρύθμιση που δεν αφορά, άμεσα τουλάχιστον, το δημόσιο τομέα, αλλά περιορίζει το αντικείμενο επεξεργασίας προσωπικών δεδομένων από ασφαλιστικές εταιρείες. Ακόμα όμως και για το δημόσιο τομέα, δεν επιτρέπεται να συνδεθεί η ασφάλιση υγείας με γενετικά δεδομένα.

#### 5.4.1.12 Πως εξασφαλίζεται η νομιμότητα της επεξεργασίας όταν έχουμε δεδομένα ειδικών κατηγοριών.

Ο κανόνας του ΓΚΠΔ είναι απλός. Χρειάζεται:

- Μια (τουλάχιστον) νομική βάση στο άρθρο 6 παρ. 1 και
- Μια (τουλάχιστον) προϋπόθεση για την επεξεργασία ειδικών κατηγοριών δεδομένων στο άρθρο 9 παρ. 2

Βέβαια, αν υπάρχει προϋπόθεση για την επεξεργασία ειδικών κατηγοριών δεδομένων, είναι μάλλον εύκολο να εντοπιστεί η κατάλληλη νομική βάση στο άρθρο 6. Η αντιστοιχία στις περισσότερες περιπτώσεις δεν είναι δύσκολη, αν και υπάρχουν περιπτώσεις οι οποίες δεν είναι προφανείς. Φυσικά, όπως θα δούμε αργότερα, με βάση την αρχή της διαφάνειας, η επιλογή αυτή υποχρεώνει τον υπεύθυνο επεξεργασίας να ενημερώσει κατάλληλα τα υποκείμενα των δεδομένων, άρα είναι δεσμευτική και πρέπει να γίνεται με προσοχή.

## 5.5 Επεξεργασία δεδομένων ποινικών καταδικών και αδικημάτων

Στο πλαίσιο του ΓΚΠΔ, τα δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας δεν αναφέρονται αυτά καθαυτά στον κατάλογο των ειδικών κατηγοριών δεδομένων, αλλά εξετάζονται σε χωριστό άρθρο. Τα δεδομένα αυτά υπόκεινται σε ακόμα μεγαλύτερο περιορισμό σε σχέση με τις ειδικές κατηγορίες του άρθρου 9. Το άρθρο 10 του ΓΚΠΔ προβλέπει ότι η επεξεργασία τέτοιων δεδομένων μπορεί να διενεργείται μόνο «*υπό τον έλεγχο επίσημης αρχής*» ή εάν η επεξεργασία επιτρέπεται από νόμο, ο οποίος πρέπει να προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Πλήρες ποινικό μητρώο μπορεί να τηρείται μόνο υπό τον έλεγχο ειδικών επίσημων αρχών.

Η εν λόγω διάταξη περιορίζει εξαιρετικά την επεξεργασία δεδομένων ποινικού μητρώου. Στην πράξη, ιδιωτικοί φορείς μπορεί να επεξεργαστούν δεδομένα ποινικού μητρώου μόνο εφόσον προβλέπεται σε νόμο ή σε κάποια κανονιστική διάταξη που έχει εκδοθεί από δημόσια (με την ερμηνεία του επίσημη) αρχή ή αρχή που η λειτουργία της διέπεται από νόμο, όπως η Τράπεζα της Ελλάδος.

☞ Δημόσιοι φορείς, αν ληφθεί υπόψη και η αρχή της νομιμότητας της δράσης της δημόσιας διοίκησης, επιτρέπεται να επεξεργάζονται δεδομένα ποινικού μητρώου μόνο εφόσον υπάρχει σχετική διάταξη.

Επισημαίνεται βέβαια ότι, η επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των διαδικασιών της επιβολής του νόμου διέπεται από την Οδηγία (ΕΕ) 2016/680 και όχι τον ΓΚΠΔ. Η οδηγία προβλέπει ειδικούς κανόνες για την προστασία δεδομένων, οι οποίοι είναι δεσμευτικοί για τις αρμόδιες αρχές όταν αυτές επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ειδικά για την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων. Για τη νομιμότητα των πράξεων επεξεργασίας αυτών των φορέων εφαρμόζεται το κεφάλαιο Δ του ν. 4624/2019 που ενσωματώνει την ως άνω Οδηγία. Επεξεργασία από τις αρχές αυτές για άλλους σκοπούς (εκτός της οδηγίας 2016/680) εμπίπτει όμως στο πεδίο εφαρμογής του ΓΚΠΔ. Ιδιωτικοί όμως φορείς εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ (π.χ. έλεγχος για «ξέπλυμα» χρήματος ή δραστηριότητες εγκληματολογικών εργαστηρίων).



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 5.6 Στοιχεία της έγκυρης συγκατάθεσης

Η έννοια της συγκατάθεσης στο ΓΚΠΔ έχει εξελιχθεί σε σχέση με την Οδηγία 95/46/ΕΚ, ακολουθώντας τη νομολογία που είχε διαμορφωθεί από τις Ευρωπαϊκές Εποπτικές Αρχές. Ο ορισμός της συγκατάθεσης, τον οποίο είδαμε νωρίτερα, δεν έχει μεταβληθεί ουσιαστικά. Επιπλέον, οι απαιτήσεις για την εξασφάλιση και την απόδειξη μιας έγκυρης συγκατάθεσης έχουν συγκεκριμενοποιηθεί και αναφέρονται, σε μεγάλο βαθμό, μέσα στο κείμενο του κανονισμού, στο άρθρο 7. Αν δούμε ξανά τον ορισμό, τέσσερα είναι τα βασικά στοιχεία της έγκυρης συγκατάθεσης: «ελεύθερη», «συγκεκριμένη», «εν πλήρει επιγνώσει» και «αδιαμφισβήτητη». Η κατανόηση αυτών των χαρακτηριστικών θα μας βοηθήσει να κατανοήσουμε αν και πότε είναι η συγκατάθεση κατάλληλη επιλογή ως νομική βάση.

### 5.6.1 Ελεύθερη

Ελεύθερη συγκατάθεση σημαίνει ότι υπάρχει αληθινή δυνατότητα επιλογής και ελέγχου για τα υποκείμενα των δεδομένων. Το ΕΣΠΔ στις κατευθυντήριες γραμμές του για τη συγκατάθεση [32] επισημαίνει ότι όταν υπάρχει σαφής ανισορροπία ισχύος μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας δεν μπορεί να θεωρηθεί ελεύθερη συγκατάθεση. Έτσι, στις περιπτώσεις που ο υπεύθυνος επεξεργασίας είναι δημόσια Αρχή, κατά κανόνα, δεν μπορεί να υπάρχει ελεύθερη συγκατάθεση και άρα θα πρέπει να υπάρχει άλλη νομική βάση. Υπάρχουν βέβαια περιπτώσεις που η συγκατάθεση μπορεί να χρησιμοποιηθεί και από φορείς του δημοσίου. Μια άλλη περίπτωση σαφούς ανισορροπίας ισχύος εδράζεται στον εργασιακό τομέα, όπου ο εργαζόμενος δύσκολα θα αρνηθεί να παράσχει την έγκριση του για μια επεξεργασία, εφόσον του ζητηθεί από τον εργοδότη του. Γενικά, κάθε στοιχείο ανάρμοστης πίεσης ή επιρροής στο υποκείμενο των δεδομένων η οποία δεν επιτρέπει στο υποκείμενο των δεδομένων να ασκήσει ελεύθερα τη βούλησή του καθιστά τη συγκατάθεση ανίσχυρη. Για παράδειγμα, αυτό συμβαίνει όταν κατά την υπογραφή μιας σύμβασης τίθεται ως προϋπόθεση η συγκατάθεση που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης. Συγκατάθεση ενσωματωμένη σε τμήμα κειμένου «όρων και προϋποθέσεων» χωρίς χωριστή δυνατότητα διαπραγμάτευσης, δεν είναι έγκυρη.

Τελικά, το κρίσιμο στοιχείο για να κρίνει κανείς αν η συγκατάθεση του υποκειμένου



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

των δεδομένων μπορεί να είναι πραγματικά ελεύθερη είναι ένα:

☞ Μπορεί το υποκείμενο των δεδομένων να αρνηθεί ή να ανακαλέσει τη συγκατάθεσή του χωρίς να υποστεί δυσμενείς συνέπειες;

Ο παραπάνω έλεγχος είναι ο πιο βασικός ώστε να μπορούμε να κρίνουμε την ορθότητα της ελευθερίας της συγκατάθεσης.

**Παράδειγμα:** Δημόσιο σχολείο ζητεί τη συγκατάθεση των μαθητών[14] για να χρησιμοποιήσει τις φωτογραφίες τους σε έντυπο μαθητικό περιοδικό. Η συγκατάθεση στην περίπτωση αυτή αποτελεί πραγματικά ελεύθερη επιλογή των υποκειμένων των δεδομένων καθώς οι μαθητές δεν θα στερηθούν εκπαιδευτικές ή άλλες υπηρεσίες και μπορούν να αρνηθούν να συγκατατεθούν στη χρήση των εν λόγω φωτογραφιών χωρίς να ζημιωθούν.

### 5.6.2 Συγκεκριμένη

Όταν στο πλαίσιο των δραστηριοτήτων ενός υπευθύνου επεξεργασίας η συγκατάθεση του υποκειμένου των δεδομένων αφορά παραπάνω από ένα σκοπούς, αυτή πρέπει να παρέχεται για «*έναν ή περισσότερους συγκεκριμένους*» σκοπούς και το υποκείμενο των δεδομένων πρέπει να έχει ξεχωριστή επιλογή για κάθε ένα από τους σκοπούς αυτούς. Επομένως, για να είναι συγκεκριμένη η συγκατάθεση πρέπει:

1) Ο (κάθε) σκοπός να είναι πλήρως προσδιορισμένος (με βάση και την αρχή του περιορισμού του σκοπού). Αυτό είναι ένα απαραίτητο αντιστάθμισμα των τεχνολογικών δυνατοτήτων και της πιθανής αλλαγής σκοπού.
2) Να παρέχεται διαφορετική συγκατάθεση για διαφορετικούς σκοπούς.
    - Καθώς πολλές φορές οι σκοποί μπορεί να είναι παρεμφερείς ή συναφείς, απαιτείται ικανό επίπεδο διαφοροποίησης ώστε να αποφεύγεται η χρήση γενικών διατυπώσεων για τους σκοπούς.
    - Η συγκατάθεση μπορεί όμως να καλύπτει διαφορετικές λειτουργίες (πράξεις επεξεργασίας), αρκεί να είναι για τον ίδιο σκοπό.

[14] Εφόσον πρόκειται για ανήλικους, τα δικαιώματά τους (όπως η δήλωση συγκατάθεσης) ασκούνται από τους ασκούντες τη γονική μέριμνα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

3) Σαφής διαχωρισμός της πληροφόρησης που δίδεται σε σχέση με την παροχή συγκατάθεσης για επεξεργασία δεδομένων από την πληροφόρηση για άλλα ζητήματα. Η απόκρυψη της ενημέρωσης για τη συγκατάθεση μέσα σε ένα γενικό κείμενο ενημέρωσης αποτελεί κακή πρακτική.

### 5.6.3 Εν πλήρει επιγνώσει

Βασικό χαρακτηριστικό της ορθής συγκατάθεσης είναι η πλήρης ικανοποίηση της αρχής της διαφάνειας, σε σχέση με το συγκεκριμένο σκοπό επεξεργασίας. Επομένως, πρέπει:

1) Να παρέχονται, κατ' ελάχιστον, πληροφορίες καθοριστικής σημασίας για το υποκείμενο των δεδομένων προκειμένου να κρίνει αν συναινεί, όπως:
   - Ταυτότητα υπευθύνου επεξεργασίας
   - Σκοπός κάθε πράξης επεξεργασίας για την οποία ζητείται συγκατάθεση
   - Είδος δεδομένων που συλλέγονται και χρησιμοποιούνται
   - Η δυνατότητα άρσης της συγκατάθεσης
   - Τυχόν χρήση για αυτοματοποιημένες αποφάσεις ή δημιουργίας προφίλ (profiling)
   - Σε περίπτωση διαβίβασης εκτός Ε.Ε., ενημέρωση για τους πιθανούς κινδύνους
2) Ο τρόπος παροχής της πληροφόρησης να διασφαλίζει στα υποκείμενα των δεδομένων τη δυνατότητα να προσδιορίσουν με ευκολία ποιος είναι ο υπεύθυνος επεξεργασίας και να κατανοήσουν σε τι συναινούν.
   - Αν και δεν προσδιορίζεται συγκεκριμένη μέθοδος, ορίζεται ότι η ενημέρωση πρέπει να είναι σαφής και με απλή διατύπωση.
   - Η γλώσσα και το κείμενο πρέπει να είναι κατανοητό από το μέσο πολίτη και όχι μόνο από νομικούς.
   - Απαιτείται μελέτη του κοινού στο οποίο απευθύνεται η πρόσκληση για συγκατάθεση και προσαρμογή της γλώσσας (π.χ. ανήλικοι)
   - Σε ηλεκτρονικές εφαρμογές πρέπει να ακολουθείται κατάλληλη μέθοδος ώστε να μην «κουράζεται» ο χρήστης. Προτείνεται πολυεπίπεδη προσέγγιση.

   Οι υποχρεώσεις για τον τρόπο παροχής της πληροφόρησης σχετίζονται άμεσα



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

με την ικανοποίηση της αρχής της διαφάνειας, και θα εξεταστούν αναλυτικότερα σε επόμενο κεφάλαιο, όταν θα εξετάσουμε τις υποχρεώσεις παροχής κατάλληλης ενημέρωσης στα άρθρα 12, 13 και 14 του ΓΚΠΔ.

### 5.6.4 Η αδιαμφισβήτητη συγκατάθεση – θετική δήλωση συναίνεσης

Σύμφωνα με το ΓΚΠΔ η συγκατάθεση απαιτεί δήλωση του υποκειμένου των δεδομένων ή σαφή θετική ενέργεια, το οποίο σημαίνει ότι η συγκατάθεση πρέπει να παρέχεται πάντοτε μέσω «θετικής» ενέργειας ή δήλωσης. Πρόκειται για τη λεγόμενη «opt-in» συγκατάθεση (δηλαδή, αν ο χρήστης δεν κάνει καμία ενέργεια, τεκμαίρεται η μη συγκατάθεσή του). Συνεπώς:

- Απαιτείται ενσυνείδητη, εσκεμμένη ενέργεια του υποκειμένου των δεδομένων.
- Η σιωπηρή αποδοχή του υποκειμένου των δεδομένων, έστω και μετά από κατάλληλη ενημέρωση, αλλά χωρίς κάποια ενέργεια, δεν νοείται ως έγκυρη συγκατάθεση.
    - Προσυμπληρωμένα κουτιά αποδοχής συγκατάθεσης δεν αποτελούν έγκυρη μέθοδο
    - «Opt-out» κουτιά επιλογής δεν αποτελούν έγκυρη μέθοδο (π.χ. «αν δεν συμφωνείτε με την επεξεργασία, επιλέξτε εδώ», το οποίο υποδηλώνει ότι ο υπεύθυνος επεξεργασίας θα εκλάβει ως συγκατάθεση του χρήστη τη μη ενέργεια).

Τεχνικά, η συγκατάθεση μπορεί να λαμβάνεται με οποιοδήποτε μέσο, αρκεί να μπορεί ο υπεύθυνος επεξεργασίας να αποδείξει ότι έχει δοθεί από το υποκείμενο των δεδομένων. Στον ιδανικό κόσμο, η συγκατάθεση θα δινόταν πάντα γραπτά. Αλλά μπορεί να γίνεται και με καταγραφή συνομιλίας, αν παρέχεται κατάλληλη πληροφόρηση. Σήμερα, είναι πιο συχνό η συγκατάθεση να παρέχεται με ηλεκτρονικά μέσα. Οι υπεύθυνοι επεξεργασίας μπορούν να υλοποιήσουν τα δικά τους συστήματα για την παροχή έγκυρης συγκατάθεσης, αρκεί αυτά να βασίζονται στις αρχές του ΓΚΠΔ και να είναι σε θέση να αποδείξουν ότι αυτή παρασχέθηκε, χωρίς να μπορεί να αμφισβητηθεί, από το υποκείμενο των δεδομένων. Τέτοιοι τρόποι παροχής ηλεκτρονικής συγκατάθεσης καλό είναι να υλοποιούνται με τρόπο που δεν διακόπτουν ή επιβαρύνουν αναίτια τη λήψη της υπηρεσίας που ζητάει το υποκείμενο



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

των δεδομένων, ενώ μπορεί να είναι και προσαρμοσμένοι στο μέσο, όπως με κινήσεις σάρωσης (swipe), χαιρετισμού σε κάμερα, περιστροφή κινητού σε μορφή «8» κλπ. Από την άλλο όμως πλευρά, η θετική ενέργεια πρέπει να διαφοροποιείται επαρκώς από την τυπική χρήση της υπηρεσίας από ένα χρήστη. Για παράδειγμα, η απλή κύλιση (scroll) σε κείμενο ενημέρωσης για τη συγκατάθεση δεν ικανοποιεί την απαίτηση αυτή.

### 5.6.5 Αδιαμφισβήτητη, σε σχέση με Ρητή συγκατάθεση

Όπως προαναφέραμε, στην περίπτωση που η συγκατάθεση χρησιμοποιείται ως προϋπόθεση για την επεξεργασία ειδικών κατηγοριών δεδομένων, δεν απαιτείται απλά να είναι αδιαμφισβήτητη («unambiguous»), αλλά ρητή («explicit»). Αυτό σημαίνει αυξημένες προϋποθέσεις για τη συγκατάθεση. Η γραπτή δήλωση είναι ένας τρόπος ικανοποίησης της απαίτησης για ρητή συγκατάθεση, αλλά όχι ο μόνος. Το υποκείμενο των δεδομένων μπορεί να είναι σε θέση να χορηγήσει ρητή συγκατάθεση συμπληρώνοντας ηλεκτρονικό έντυπο, αποστέλλοντας μήνυμα ηλεκτρονικού ταχυδρομείου, μεταφορτώνοντας σαρωμένο έγγραφο το οποίο φέρει την υπογραφή του, υπεύθυνη δήλωση από το gov.gr ή χρησιμοποιώντας ηλεκτρονική υπογραφή. Σε περιπτώσεις ηλεκτρονικής ρητής συγκατάθεσης, ενδείκνυται επίσης η χρήση επαλήθευσης σε δύο στάδια.

### 5.6.6 Πρόσθετα χαρακτηριστικά έγκυρης συγκατάθεσης

Στο άρθρο 7 του ΓΚΠΔ ορίζονται οι πρόσθετες προϋποθέσεις για την εγκυρότητα της συγκατάθεσης. Μάλιστα, με βάση το άρθρο 7 παράγραφος 1, **ο υπεύθυνος επεξεργασίας φέρει το βάρος της απόδειξης** (της ορθότητας) της συγκατάθεσης, ο οποίος θα πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε στην πράξη επεξεργασίας (αυτό εξάλλου συνάδει απόλυτα και με την αρχή της λογοδοσίας). Ο ΓΚΠΔ δεν καθορίζει με ποιο τρόπο ακριβώς πρέπει να γίνεται αυτό. Ωστόσο, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι, σε κάθε δεδομένη περίπτωση, το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του. Όσο διαρκεί η επίμαχη δραστηριότητα επεξεργασίας δεδομένων, υφίσταται υποχρέωση απόδειξης της συγκατάθεσης. Μετά το πέρας της δραστηριότητας επεξεργασίας, η απόδειξη της συγκατάθεσης θα πρέπει να διατηρείται για διάστημα το οποίο δεν υπερβαίνει το απολύτως αναγκαίο για την



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τήρηση νομικής υποχρέωσης ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Στον ΓΚΠΔ **δεν προβλέπεται συγκεκριμένο χρονικό όριο** όσον αφορά τη διάρκεια ισχύος της συγκατάθεσης. Αυτή εξαρτάται από παράγοντες όπως το πλαίσιο, το πεδίο εφαρμογής της αρχικής συγκατάθεσης και τις προσδοκίες του υποκειμένου των δεδομένων. Εάν οι πράξεις επεξεργασίας μεταβληθούν ή εξελιχθούν σημαντικά, η αρχική συγκατάθεση δεν θα είναι πλέον έγκυρη. Σε μια τέτοια περίπτωση, πρέπει να εξασφαλιστεί νέα συγκατάθεση. Μάλιστα, το ΕΣΠΔ συνιστά στις κατευθυντήριες γραμμές για τη συγκατάθεση [32] (αλλά ως βέλτιστη πρακτική κι όχι ως υποχρέωση) να ανανεώνεται η συγκατάθεση σε κατάλληλα χρονικά διαστήματα.

Η **δυνατότητα ανάκλησης της συγκατάθεσης** είναι άλλο ένα βασικό στοιχείο, όπως προκύπτει από το άρθρο 7 παρ. 3. Ο Κανονισμός ορίζει ότι η ανάκληση της συγκατάθεσης πρέπει να είναι εξίσου εύκολη με την παροχή της. Μάλιστα επισημαίνεται ότι δεν αναφέρει ότι πρέπει να δίδεται με το ίδιο μέσο, αλλά με την ίδια ευκολία. Συνεπώς, είναι ζήτημα του υπεύθυνου επεξεργασίας να βρει την κατάλληλη μέθοδο. Κατά την παροχή της συγκατάθεσης πρέπει να δίδεται κατάλληλη πληροφόρηση για τη μέθοδο ανάκλησης. Προφανώς, η ανάκληση της συγκατάθεσης δεν έχει αναδρομική ισχύ. Σε περίπτωση ανάκλησης, όλες οι προηγούμενες πράξεις επεξεργασίας δεδομένων που βασίζονταν στη συγκατάθεση εξακολουθούν να είναι νόμιμες. Όμως ο υπεύθυνος επεξεργασίας οφείλει πλέον να παύσει τις σχετικές πράξεις επεξεργασίας. Εάν δεν υπάρχει άλλη νόμιμη βάση η οποία να δικαιολογεί την επεξεργασία (π.χ. περαιτέρω αποθήκευση η οποία να βασίζεται σε άλλη νομική βάση) των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να διαγράψει τα δεδομένα, τηρώντας όμως τα στοιχεία για την απόδειξη της ορθής χορήγησης της αρχικής συγκατάθεσης.

Εάν ο υπεύθυνος επεξεργασίας επιλέξει να βασιστεί στη νομική βάση της συγκατάθεσης για οποιοδήποτε μέρος της επεξεργασίας, πρέπει να είναι έτοιμος να σεβαστεί την επιλογή αυτή και να διακόψει την επεξεργασία αν το φυσικό πρόσωπο ανακαλέσει τη συγκατάθεσή του. Ο υπεύθυνος επεξεργασίας **δεν μπορεί να μεταπηδήσει από τη συγκατάθεση σε άλλη νομική βάση**. Κυρίως, δεν επιτρέπεται να χρησιμοποιήσει αναδρομικά τη βάση του υπέρτερου έννομου συμφέροντος προκειμένου να δικαιολογήσει την επεξεργασία αν αντιμετωπίσει προβλήματα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σχετικά με την ισχύ της συγκατάθεσης. Οι υπεύθυνοι επεξεργασίας οφείλουν να έχουν αποφασίσει πριν από τη συλλογή των δεδομένων για το ποια είναι η εφαρμοστέα νόμιμη βάση, να ενημερώνουν γι' αυτό και να μην προβαίνουν σε αλλαγές.

**Ερώτηση δραστηριότητας**: Το 2017 ο ΟΑΣΑ προχώρησε σε εισαγωγή του ηλεκτρονικού εισιτηρίου. Αφού προχώρησε σε μελέτη του συστήματος, αναγνώρισε τους εξής 4 σκοπούς:

1) Πληρωμή και έλεγχος κομίστρου

2) Κοινωνική παροχή σε ευαίσθητες ομάδες (ΑΜΕΑ – άνεργοι – νέοι – υπερήλικες)

3) Στατιστικά στοιχεία κίνησης – συγκεντρωτικά στοιχεία κίνησης και διαδρομών

4) Επικοινωνία με επιβάτες

Ποια θεωρείτε ότι είναι η κατάλληλη νομική βάση για κάθε ένα από τους σκοπούς αυτούς;

Για ποιο σκοπό μπορεί να αξιοποιηθεί η συγκατάθεση;

Καθώς υπάρχουν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, ποια είναι η καταλληλότερη προϋπόθεση για την επεξεργασία αυτών; Μπορείτε να αναγνωρίσετε αν και τι είδους νομοθετικές διατάξεις απαιτούνται;

Ποια θεωρείτε ότι είναι τα σημαντικότερα προβλήματα για την ικανοποίηση της αρχής της ελαχιστοποίησης των δεδομένων;

## 5.7 Συγκατάθεση παιδιού

Ο ΓΚΠΔ έχει ως ειδικό στόχο την επαύξηση της προστασίας των δικαιωμάτων και ελευθεριών των παιδιών, όταν δικά τους δεδομένα είναι αντικείμενο επεξεργασίας. Αυτό ισχύει ειδικά στον επιγραμμικό κόσμο, σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών. Ο Κανονισμός αναγνωρίζει ότι τα παιδιά μπορεί να έχουν μικρότερη επίγνωση των κινδύνων, συνεπειών και εγγυήσεων και των δικαιωμάτων τους σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Στο σύγχρονο κόσμο, που είναι διαθέσιμες πάρα πολλές υπηρεσίες που στοχεύουν σε παιδιά, είναι αναμενόμενο να υπάρχει ενδιαφέρον για εμπορία ή δημιουργία προφίλ προσωπικότητας ή προφίλ χρηστών που είναι παιδιά, μέσω συλλογής δεδομένων



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προσωπικού χαρακτήρα.

Στο άρθρο 8 παρ. 1 ορίζεται ότι όταν η συγκατάθεση εφαρμόζεται «*σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε παιδί, η επεξεργασία δεδομένων προσωπικού χαρακτήρα παιδιού είναι σύννομη εάν το παιδί είναι τουλάχιστον 16 χρονών. Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού*». Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού. Τα κράτη μέλη μπορούν να προβλέπουν διά νόμου κατώτερο όριο, το οποίο δεν μπορεί να είναι κατώτερο των 13 ετών. Η Ελλάδα, στο άρθρο 21 του ν. 4624/2019 επέλεξε ως όριο τα 15 έτη. Ο τρόπος λήψης της έγκρισης του γονέα/κηδεμόνα του παιδιού δεν ορίζεται στη διάταξη και αφήνεται στην ευχέρεια του υπεύθυνου επεξεργασίας, ο οποίος οφείλει να διαθέτει κατάλληλες διαδικασίες προς τούτο.

Η εν λόγω διάταξη εφαρμόζεται μόνο όταν:

- Η επεξεργασία αφορά υπηρεσίες της κοινωνίας των πληροφοριών[15] που παρέχονται απευθείας σε παιδί
- Η επεξεργασία βασίζεται σε συγκατάθεση.

Συνεπώς, εφαρμόζεται μόνο σε συγκεκριμένες περιπτώσεις και όχι σε κάθε περίπτωση που γίνεται επεξεργασία δεδομένων παιδιών. Το όριο των 15 ετών για να θεωρείται η συγκατάθεση παιδιού έγκυρη δεν εφαρμόζεται όσον αφορά:

- Ηλεκτρονικές υπηρεσίες που μπορεί να παρέχει το δημόσιο σε παιδιά, όταν νομική βάση είναι οι περιπτώσεις γ' και ε' του άρθρου 6 παρ. 1 του ΓΚΠΔ.
- Ηλεκτρονικές υπηρεσίες προς παιδιά για τις οποίες νομική βάση είναι η σύμβαση. Στην περίπτωση αυτή, για τον έλεγχο της εγκυρότητας της σύμβασης εφαρμόζονται οι εκάστοτε εθνικές ρυθμίσεις. Για παράδειγμα, είναι πολύ πιθανό να την παροχή ηλεκτρονικών υπηρεσιών με βάση τη σύμβαση σε νέο 17 ετών να απαιτείται να συμβληθεί ο γονέας ή κηδεμόνας.
- Μη ψηφιακές υπηρεσίες που παρέχονται απευθείας σε παιδιά.

[15] Για τον ορισμό γίνεται παραπομπή στην οδηγία (ΕΕ) 2015/1535.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Παράδειγμα:** Δημόσιο σχολείο (Γυμνάσιο - Λύκειο) δημιουργεί κλειστό διαδικτυακό forum και παρέχει τη δυνατότητα χρήσης του στους μαθητές του. Η συμμετοχή είναι εθελοντική κι ελεύθερη και βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων.

Οι μαθητές οι οποίοι είναι άνω των 15 ετών μπορούν να εγγραφούν στο forum, παρέχοντας οι ίδιοι τη συγκατάθεση.

Για μαθητές που είναι κάτω των 15 ετών, το σχολείο οφείλει να φροντίσει ότι η εγγραφή θα γίνεται μόνο μετά από έγκριση των γονέων/κηδεμόνων.

**Παράδειγμα: Το** Υπουργείο Παιδείας παρέχει πλατφόρμα ασύγχρονης εξ αποστάσεως εκπαίδευσης η οποία απευθύνεται σε παιδιά όλων των ηλικιών. Παρ' ότι η εν λόγω πλατφόρμα αποτελεί υπηρεσία της Κοινωνίας των Πληροφοριών η συγκατάθεση δεν αποτελεί ορθή νομική βάση. Συνεπώς, το Υπουργείο δεν χρειάζεται να λάβει υπόψη τη διάταξη του άρθρου 8 στο σχεδιασμό της πλατφόρμας.

## 5.8 Διαβιβάσεις σε χώρες εκτός Ε.Ε.

Στη σημερινή παγκοσμιοποιημένη οικονομία, οι κανόνες για την προστασία των δεδομένων προσωπικού χαρακτήρα της Ε.Ε. δεν θα είχαν νόημα αν περιορίζονταν, εδαφικά, μόνο στο γεωγραφικό χώρο της Ε.Ε. Είναι σύνηθες φαινόμενο για επιχειρήσεις αλλά και για φορείς του δημοσίου τομέα, να συνεργάζονται με εταιρείες ή δημόσιους φορείς εκτός της Ε.Ε. είτε με σχέση υπευθύνου επεξεργασίας – εκτελούντος την επεξεργασία, είτε επειδή πρέπει να διαβιβάσουν σύνολα δεδομένων προσωπικού χαρακτήρα εκτός Ε.Ε. (σημειώνεται ότι η διαβίβαση δεδομένων εντός Ε.Ε. είναι ελεύθερη, δηλαδή χωρίς τις πρόσθετες διασφαλίσεις που συζητούνται στην παρούσα ενότητα για χώρες εκτός Ε.Ε.). Για παράδειγμα, οι δημόσιες φορολογικές αρχές, πρέπει να συνεργαστούν με αρχές κρατών εκτός Ε.Ε./Ε.Ο.Χ. για την καταπολέμηση της φοροδιαφυγής και της οικονομικής απάτης. Ως άλλο παράδειγμα, σε διαδικτυακές εφαρμογές μεγάλης κλίμακας, ένας δημόσιος φορέας μπορεί να επιλέξει να χρησιμοποιήσει υπηρεσίες υπολογιστικού νέφους, οι οποίες να μην βρίσκονται αποκλειστικά εντός Ε.Ε. Η Ευρωπαϊκή νομοθεσία όμως, προσπαθεί να



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εξασφαλίσει ότι ακόμα και αν δεδομένα προσωπικού χαρακτήρα βρεθούν εκτός του γεωγραφικού της χώρου, δεν θα μειώνονται τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων. Για το σκοπό αυτό, το κεφάλαιο V του Κανονισμού περιλαμβάνει ρυθμίσεις οι οποίες προσπαθούν να διασφαλίσουν ότι δεν υπονομεύεται το επίπεδο προστασίας των φυσικών προσώπων που εγγυάται η νομοθεσία.

Στην πράξη, αυτό σημαίνει ότι κάθε διαβίβαση δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό πρέπει:

- Να είναι νόμιμη με βάση τις λοιπές διατάξεις του Κανονισμού (ιδίως με τα άρθρα 5 και 6)
- Να πληροί τους όρους του κεφαλαίου V (άρθρα 44-50)

Το ΕΣΠΔ έχει αναγνωρίσει τρία κριτήρια για τον ορισμό της διαβίβασης εκτός Ε.Ε. [33]:

1) Ο υπεύθυνος ή ο εκτελών την επεξεργασία υπόκειται στο ΓΚΠΔ για τη συγκεκριμένη επεξεργασία
2) Ο υπεύθυνος ή ο εκτελών την επεξεργασία (που ορίζεται ως «εξαγωγέας») αποκαλύπτει μέσω μετάδοσης ή καθιστά προσωπικά δεδομένα διαθέσιμα σε άλλον υπεύθυνο, από κοινού υπεύθυνο ή εκτελούντα την επεξεργασία (ο οποίος ορίζεται ως «εισαγωγέας»).
3) Ο εισαγωγέας βρίσκεται σε τρίτη χώρα, ή είναι διεθνής οργανισμός, ανεξάρτητα από το αν αυτός υπόκειται στο ΓΚΠΔ σε σχέση με την συγκεκριμένη επεξεργασία.

Αν θεωρηθεί ότι υφίσταται διαβίβαση δεδομένων εκτός Ε.Ε., τότε ακολουθείται ο εξής «αλγόριθμος»:

1) Ελέγχεται αν η τρίτη χώρα παρέχει επαρκές επίπεδο προστασίας (άρθρο 45 ΓΚΠΔ). Αν ναι, η διαβίβαση μπορεί να εκτελεστεί.
2) Αν όχι, ο υπεύθυνος ή ο εκτελών πρέπει να παρέχει κατάλληλες εγγυήσεις για τη διαβίβαση, όπως προβλέπονται στο άρθρο 46 του ΓΚΠΔ.
3) Αν όμως δεν μπορούν να εφαρμοστούν οι μηχανισμοί των άρθρων 45 ή 46, τότε εξετάζεται αν μπορεί να εφαρμοστεί το άρθρο 49, στο οποίο περιλαμβάνονται (αρκετές) περιπτώσεις για μεμονωμένες παρεκκλίσεις οι οποίες εφαρμόζονται σε ειδικές καταστάσεις.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

### 5.8.1 Τρίτες χώρες που παρέχουν επαρκές επίπεδο προστασίας

Η Ευρωπαϊκή Επιτροπή μπορεί να αποφασίσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας:

- από τρίτη χώρα (πλήρως) ή
- από έδαφος τρίτης χώρας (συγκεκριμένο τμήμα της) ή
- από έναν ή περισσότερους συγκεκριμένους τομείς στην εν λόγω τρίτη χώρα (π.χ. στον Καναδά όσον αφορά τον εμπορικό τομέα) ή
- από διεθνή οργανισμό.

Για την απόφαση αυτή απαιτείται εκτελεστή πράξη της Ε. Επιτροπής, η οποία επανεξετάζεται περιοδικά ανά τετραετία. Όταν η τρίτη χώρα δεν διασφαλίζει πλέον το επαρκές επίπεδο η Ε. Επιτροπή μπορεί να προβεί σε κατάργησης αναστολή ή τροποποίηση της απόφασης. Η Απόφαση εκδίδεται μετά από γνωμοδότηση του ΕΣΠΔ.

Για διαβίβαση προς χώρα για την οποία υπάρχει απόφαση επάρκειας δεν απαιτείται ειδική άδεια από εποπτική αρχή. Έως τη στιγμή που γράφονται οι σημειώσεις έχουν αναγνωριστεί οι εξής: Ανδόρα, Αργεντινή, Καναδάς (εμπορικοί οργανισμοί), Νησιά Φερόε, Γκέρνσεϋ, Ισραήλ, Νήσος του Μαν, Ιαπωνία, Τζέρσεϋ, Νέα Ζηλανδία, Δημοκρατία της Κορέας (Νότια Κορέα), Ελβετία, Ηνωμένο Βασίλειο και Ουρουγουάη[16].

### 5.8.2 Διαβιβάσεις βάσει κατάλληλων εγγυήσεων

Στο άρθρο 46 του ΓΚΠΔ ορίζονται οι απαιτήσεις ώστε ένας υπεύθυνος ή εκτελών την επεξεργασία να παρέχει κατάλληλες εγγυήσεις. Στην πράξη απαιτείται να εξασφαλίζεται:

- ότι μετά τη διαβίβαση τα δικαιώματα που παρέχει ο ΓΚΠΔ μπορεί να εκτελεστούν και
- ότι υπάρχουν αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων, σε περίπτωση που επιθυμούν να προσφύγουν.

Συνοπτικά, υπάρχουν δύο κατηγορίες μεθόδων παροχής εγγυήσεων:

Α. Χωρίς άδεια της Εποπτικής Αρχής:

[16] Ανανεωμένος κατάλογος τηρείται στο **https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

1. **Με νομικά δεσμευτικό και εκτελεστό μέσο μεταξύ δημόσιων αρχών**. Αυτό προϋποθέτει την ύπαρξη διακρατικής συμφωνίας η οποία κυρώνεται επίσημα (με νόμο).
2. Δεσμευτικοί Εταιρικοί Κανόνες (BCR). Η διαδικασία αυτή περιγράφεται στο άρθρο 47 του ΓΚΠΔ και αφορά ομίλους επιχειρήσεων.
3. Τυποποιημένες ρήτρες προστασίας προσωπικών δεδομένων οι οποίες εκδίδονται από την Επιτροπή [34]. Η Επιτροπή παρέχει τυποποιημένα υποδείγματα συμβάσεων, οι οποίες, αν συμπληρωθούν σωστά, εξασφαλίζουν, κατ' αρχήν, τις προϋποθέσεις του ΓΚΠΔ.
4. Τυποποιημένες ρήτρες προστασίας προσωπικών δεδομένων εκδοθείσες από εποπτική αρχή οι οποίες ύστερα εγκρίνονται από την Επιτροπή.
5. Εγκεκριμένος κώδικας δεοντολογίας (με βάση το άρθρο 40 παρ. 3) μαζί με δεσμευτικές και εκτελεστές υποχρεώσεις του υπευθύνου ή του εκτελούντος στην τρίτη χώρα να εφαρμόζει τις κατάλληλες εγγυήσεις.
6. Εγκεκριμένος μηχανισμός πιστοποίησης (με βάση το άρθρο 42 παρ. 2) μαζί με δεσμευτικές και εκτελεστές υποχρεώσεις του υπευθύνου ή του εκτελούντος στην τρίτη χώρα να εφαρμόζει τις κατάλληλες εγγυήσεις.

Β. Με άδεια της Εποπτικής Αρχής:

1. Σύμβαση μεταξύ εξαγωγέα και εισαγωγέα, η οποία όμως είναι ad hoc και δεν ακολουθεί τα υποδείγματα της Ε. Επιτροπής.
2. **Μη δεσμευτικές διοικητικές ρυθμίσεις μεταξύ δημόσιων αρχών.** Τέτοιες είναι τα μνημόνια συνεργασίας τα οποία συνάπτει ένας φορέας του δημοσίου με όμορους φορείς δημοσίου τρίτης χώρας (τα λεγόμενα MOU – Memorandum of Understanding).

☞ Επομένως, όσον αφορά στους δημόσιους φορείς στην Ελλάδα, οι περιπτώσεις διαβίβασης δεδομένων σε δημόσιους φορείς τρίτης χώρας αντιμετωπίζονται είτε με διακρατική συμφωνία η οποία κυρώνεται με νόμο και δεν απαιτείται άδεια της ΑΠΔΠΧ ή με MOU μεταξύ των δημοσίων φορέων, οπότε και απαιτείται άδεια της ΑΠΔΠΧ.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Τυπικά παραδείγματα αδειών που έχει εκδώσει η ΑΠΔΠΧ αφορούν την Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες, η οποία ανταλλάσσει πληροφορίες με όμορες αρχές εντός και εκτός Ε.Ε. Για περισσότερες λεπτομέρειες σχετικά με τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και δημόσιων αρχών και φορέων εκτός ΕΟΧ μπορείτε να ανατρέχετε στην καθοδήγηση του ΕΣΠΔ [35].

Τέλος, επισημαίνουμε (αν και δεν αφορά το δημόσιο) ότι όσον αφορά τις διαδικασίες μη τυποποιημένων συμβάσεων της Ε. Επιτροπής και BCR, έχει εφαρμογή ο μηχανισμός συνεκτικότητας και απαιτείται γνώμη του ΕΣΠΔ.

### 5.8.3 Παρεκκλίσεις για ειδικές καταστάσεις

Ως έσχατη λύση, όταν δεν μπορούν να εφαρμοστούν τα άρθρα 45-47 του ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας μπορούν υπό προϋποθέσεις να χρησιμοποιούν το άρθρο 49 του Κανονισμού. Για παράδειγμα, η διαβίβαση μπορεί να εκτελεστεί όταν το υποκείμενο των δεδομένων έχει συγκατατεθεί «ρητώς» αφού έχει προηγουμένως ενημερωθεί για τους κινδύνους, ή όταν η διαβίβαση είναι απαραίτητη για σημαντικούς λόγους δημοσίου συμφέροντος.

Οι παρεκκλίσεις αποτελούν εξαιρέσεις από τον γενικό κανόνα απαίτησης επαρκούς επιπέδου προστασίας (του άρθρου 45) ή επαρκών εγγυήσεων και αποτελεσματικών δικαιωμάτων (του άρθρου 46). Οι διαβιβάσεις βάσει των παρεκκλίσεων του άρθρου 49 γίνονται χωρίς άδεια της εποπτικής αρχής, γι' αυτό θέτουν σε μεγαλύτερο κίνδυνο τα δικαιώματα των υποκειμένων. Η προσφυγή στο άρθρο 49 δεν πρέπει όμως να οδηγεί σε καταστρατήγηση θεμελιωδών δικαιωμάτων. Επομένως, πρέπει να ερμηνεύονται στενά, ώστε η εξαίρεση να μην καταστεί κανόνας.

Αναλυτική καθοδήγηση παρέχει το ΕΣΠΔ στη σχετική γνώμη [36].

### 5.8.4 Η ανάγκη για συμπληρωματικά μέτρα κατά τις διαβιβάσεις

Με την απόφαση του ΔΕΕ στην υπόθεση C-311/18 (Schrems II) το Δικαστήριο τόνισε ότι οι τυποποιημένες συμβατικές ρήτρες ως εργαλείο διαβίβασης, δεν επαρκούν για την εξασφάλιση της νομιμότητας της διαβίβασης. Οι συμβατικές ρήτρες δεσμεύουν τα συμβαλλόμενα μέρη και όχι τις αρχές της τρίτης χώρας και, ως εκ τούτου, ενδέχεται να απαιτείται η λήψη συμπληρωματικών μέτρων, προκειμένου



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

να εξασφαλίζεται η τήρηση του απαιτούμενου από δίκαιο της ΕΕ επιπέδου προστασίας. Στις περιπτώσεις κατά τις οποίες η νομοθεσία της τρίτης χώρας δεν εξασφαλίζει την απαιτούμενη από το δίκαιο της ΕΕ προστασία των διαβιβαζόμενων προσωπικών δεδομένων, το Δικαστήριο αφήνει ανοικτή τη δυνατότητα στους εξαγωγείς δεδομένων να εφαρμόσουν συμπληρωματικά μέτρα τα οποία εξασφαλίζουν το επίπεδο προστασίας που απαιτείται από το δίκαιο της ΕΕ. Οι εξαγωγείς θα πρέπει να προσδιορίζουν τα μέτρα αυτά κατά περίπτωση. Αυτό συνάδει με την αρχή της λογοδοσίας του άρθρου 5 παρ. 2 του ΓΚΠΔ.

Ο υπεύθυνος επεξεργασίας οφείλει να αξιολογεί τη νομοθεσία της τρίτης χώρας και να εξετάσει αν είναι προβληματική και αν τα διαβιβαζόμενα δεδομένα και/ή ο εισαγωγέας των δεδομένων εμπίπτει ή μπορεί να εμπίπτει στο πεδίο εφαρμογής της νομοθεσίας αυτής. Με βάση τις κατευθυντήριες γραμμές του ΕΣΠΔ, προβληματική νομοθεσία είναι αυτή που

1. επιβάλλει στον αποδέκτη των προσωπικών δεδομένων υποχρεώσεις ή/και επηρεάζει τα δεδομένα που διαβιβάζονται, με τέτοιο τρόπο ώστε να μπορεί να επηρεάσει τις συμβατικές εγγυήσεις των εργαλείων διαβίβασης οι οποίες εξασφαλίζουν ουσιαστικά ισοδύναμο επίπεδο προστασίας και
2. δεν σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών που αναγνωρίζονται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ ή υπερβαίνει αυτό που είναι απαραίτητο και ανάλογο σε μια δημοκρατική κοινωνία για τη διασφάλιση ενός από τους σημαντικούς στόχους που αναγνωρίζονται επίσης στο δίκαιο της Ένωσης ή των Κρατών Μελών, όπως αυτοί που αναφέρονται στο άρθρο 23 παρ. 1 του ΓΚΠΔ.

Ενδεικτικά, το ΔΕΕ στην απόφαση Schrems II έχει ήδη εκφράσει προβληματισμό για τη νομοθεσία των Η.Π.Α. και ειδικά για το άρθρο 702 του Foreign Intelligence Surveillance Act (FISA) και το εκτελεστικό διάταγμα 12333, βλ. σκ. 184, 192, 195 επ.

Σε περίπτωση που η νομοθεσία της τρίτης χώρας είναι προβληματική, ο εξαγωγέας οφείλει:

- Να αναστείλει τη διαβίβαση ή
- Να υλοποιήσει συμπληρωματικά μέτρα για να αποτρέψει τον κίνδυνο της πιθανούς εφαρμογής στον εισαγωγέα των δεδομένων ή στα διαβιβαζόμενα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

δεδομένα νομοθεσίας ή πρακτικών στη χώρα του εισαγωγέα, που δύναται να επηρεάσουν τις συμβατικές εγγυήσεις του εργαλείου διαβίβασης με τις οποίες επιχειρείται να εξασφαλιστεί ισοδύναμο επίπεδο προστασίας με αυτό του ΕΟΧ.

- Εναλλακτικά, ο εξαγωγέας μπορεί να αποφασίσει να προχωρήσει στην διαβίβαση χωρίς να υλοποιήσει συμπληρωματικά μέτρα, αν θεωρεί ότι δεν υπάρχει λόγος για να πιστεύει ότι η προβληματική νομοθεσία θα εφαρμοστεί στην πράξη στα διαβιβαζόμενα δεδομένα ή τον εισαγωγέα. Ο εξαγωγέας απαιτείται να είναι σε θέση να αποδείξει και να τεκμηριώσει μέσω της αξιολόγησής του, όπου ενδείκνυται σε συνεργασία με τον εισαγωγέα, ότι ο προβληματικός νόμος της τρίτης χώρας δεν ερμηνεύεται και/ή δεν εφαρμόζεται στην πράξη με τρόπο που να καταλαμβάνει τα διαβιβαζόμενα δεδομένα και τον εισαγωγέα, λαμβάνοντας επίσης υπόψη την εμπειρία άλλων φορέων που δραστηριοποιούνται στον ίδιο τομέα και/ή σχετίζονται με παρόμοια διαβιβαζόμενα προσωπικά δεδομένα και πρόσθετες πηγές πληροφοριών.

Το ΕΣΠΔ έχει παράσχει ειδική καθοδήγηση στο κείμενο συστάσεων 1/2020 για τη λήψη συμπληρωματικών μέτρων [37].

Τα συμπληρωματικά μέτρα για διαβιβάσεις δεδομένων σε τρίτες χώρες έχουν εφαρμογή και στο δημόσιο τομέα. Η εφαρμογή αυτή μπορεί να είναι πολύ πιο συχνή απ' όσο φαίνεται, καθώς καταλαμβάνει πολλές από τις «μεγάλες» εταιρείες του διαδικτύου, οι οποίες ενδέχεται να εμπίπτουν στο «προβληματικό» δίκαιο τρίτων χωρών, ιδίως των Η.Π.Α. για τις οποίες ήδη υπάρχει δεδικασμένο από το ΔΕΕ.

**Παράδειγμα:** Δημόσιος φορέας χρησιμοποιεί υπηρεσίες υπολογιστικού νέφους εταιρείας, η οποία ανήκει σε πολυεθνικό όμιλο που υπόκειται στο δίκαιο των Η.Π.Α.. Η εταιρεία διαβεβαιώνει ότι τα δεδομένα θα τηρηθούν σε servers εντός Ε.Ε. Ακόμα όμως και στην περίπτωση αυτή, δεν μπορεί να αποκλειστεί η πιθανότητα πρόσβασης των αρχών των Η.Π.Α. στα δεδομένα. Συνεπώς, ο δημόσιος φορέας οφείλει να προβεί σε αξιολόγηση της διαβίβασης και να εξετάσει τη λήψη συμπληρωματικών μέτρων κατά τη χρήση της υπηρεσίας.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 5.9 Η ενσωμάτωση της Οδηγίας 2016/680 με το ν. 4624/2019

Με το νόμο 4624/2019 ενσωματώθηκε η, γνωστή ως «αστυνομική», Οδηγία (ΕΕ) 2016/680 η οποία αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους. Οι σκοποί αυτοί μπορεί να επιδιώκονται από τις αρμόδιες κρατικές αρχές (αστυνομία, λιμενικό, πυροσβεστική κλπ). Οι αρχές της Οδηγίας όσον αφορά την επεξεργασία προσωπικών δεδομένων είναι ίδιες με αυτές του ΓΚΠΔ. Μάλιστα, όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία από τις εν λόγω αρμόδιες αρχές για διαφορετικούς σκοπούς εφαρμόζεται ο ΓΚΠΔ.

Με βάση την οδηγία, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές για τους σκοπούς της οδηγίας είναι νόμιμη μόνο όταν είναι απολύτως αναγκαία για την ενάσκηση των καθηκόντων του υπεύθυνου επεξεργασίας. Δηλαδή, η οδηγία προβλέπει μια και μόνη νομική βάση. Ο Ελληνικός νόμος έχει προσθέσει και τη νομική βάση της συγκατάθεσης, αλλά η ΑΠΔΠΧ με την γνωμοδότησή της 1/2020 [18] έχει επισημάνει τη μη ορθή μεταφορά της Οδηγίας (τόσο όσον αφορά τις νομικές βάσεις καθώς δεν επιτρέπεται να προστεθεί νομική βάση που δεν αναφέρεται στην Οδηγία όσο και σε άλλες διατάξεις).

Σε άλλες διατάξεις ο ν. 4624/2019 ακολουθεί το γράμμα της Οδηγίας. Προβλέπεται:

- Διάκριση μεταξύ διαφορετικών κατηγοριών υποκειμένων των δεδομένων
    - Όσοι υπάρχουν σοβαροί λόγοι να πιστεύεται ότι έχουν διαπράξει αδίκημα
    - Όσοι υπάρχουν σοβαροί λόγοι να πιστεύεται ότι πρόκειται να διαπράξουν αδίκημα
    - Καταδικασθέντες
    - Θυμάτων
    - Άλλων προσώπων (π.χ. μάρτυρες, πληροφοριοδότες)
- Διάκριση κατηγοριών πληροφοριών σε πραγματικά δεδομένα ή εκτιμήσεις.
- Περιορισμοί της διαβίβασης των δεδομένων σε τρίτους φορείς και της χρήσης των δεδομένων για άλλους σκοπούς.

Τα δικαιώματα και οι υποχρεώσεις λογοδοσίας του ΓΚΠΔ εφαρμόζονται και στην



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

περίπτωση της Οδηγίας, αλλά με ορισμένες διαφοροποιήσεις, οι οποίες είναι κατάλληλες για την περίπτωση των διωκτικών αρχών. Περαιτέρω, προβλέπονται ειδικά μέτρα ασφάλειας, όπως τήρηση καταχωρίσεων σε αυτοματοποιημένο σύστημα (log-files) για επαλήθευση νομιμότητας για κάθε ενέργεια συλλογής, μεταβολής, διαβούλευσης, κοινολόγησης, συνδυασμού ή διαγραφής δεδομένων.

Οι προβλεπόμενες κυρώσεις, σε περίπτωση παραβίασης των διατάξεων του κεφαλαίου Δ του ν. 4624/2019 περιλαμβάνουν πρόστιμα έως 2.000.000 ευρώ.

## 5.10 Βιβλιογραφία για περισσότερη μελέτη

- Irish Data Protection Commission -Guidance Note: Legal Bases for Processing Personal Data December 2019 [38]
- Ο.Ε. άρθρου 29 - Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ [30]
- ΕΣΠΔ - Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679 (Έκδοση 1.1) [32]
- ΕΣΠΔ - Κατευθυντήριες γραμμές 2/2019 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ στο πλαίσιο της παροχής επιγραμμικών υπηρεσιών σε υποκείμενα δεδομένων [29]
- ICO [39]
- Ευρωπαϊκή Επιτροπή: International dimension of data protection [40]



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 6. Τα δικαιώματα των υποκειμένων των δεδομένων

Με την Οδηγία (ΕΕ) 95/46/ΕΚ είχε ήδη καθιερωθεί ένα σύνολο εφαρμοστέων δικαιωμάτων για τα υποκείμενα των δεδομένων. Ο ΓΚΠΔ ξεκινάει από αυτή τη βάση, επισημαίνοντας στις αιτιολογικές του σκέψεις ότι η αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση απαιτεί την ενίσχυση και τον λεπτομερή καθορισμό των δικαιωμάτων των υποκειμένων των δεδομένων, καθώς και των υποχρεώσεων όσων επεξεργάζονται και καθορίζουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Τα δικαιώματα των υποκειμένων των δεδομένων συνδέονται άμεσα με τις αρχές του Κανονισμού και ιδιαίτερα με την αρχή της διαφάνειας. Όπως και με την Οδηγία, δίνουν τη δυνατότητα στο υποκείμενο των δεδομένων να έχει έλεγχο ως προς την επεξεργασία των δικών του δεδομένων και να μπορεί να τα προσπελάσει (πρόσβαση), να τα τροποποιήσει αν είναι λανθασμένα (διόρθωση), να τα διαγράψει αν δεν είναι απαραίτητα (διαγραφή) ή και σε κάποιες περιπτώσεις να απαιτήσει να μην χρησιμοποιούνται (εναντίωση). Ο ΓΚΠΔ καθιερώνει όμως και νεότερα δικαιώματα, όπως τη δυνατότητα (υπό προϋποθέσεις) μεταφοράς των δεδομένων σε άλλο υπεύθυνο επεξεργασίας και τη δυνατότητα «κλειδώματος» (περιορισμού) των δεδομένων ενώ ενισχύει την προστασία των υποκειμένων από αυτοματοποιημένες αποφάσεις οι οποίες βασίζονται σε προσωπικά δεδομένα και ενδέχεται να έχουν δυσμενείς συνέπειες (π.χ. διακρίσεις). Αυτόματα, η καθιέρωση των δικαιωμάτων των υποκειμένων των δεδομένων δημιουργεί υποχρέωση στον κάθε υπεύθυνο επεξεργασίας να είναι σε θέση να ανταποκρίνεται σε αυτά.

> ☞ Η υποχρέωση ικανοποίησης των δικαιωμάτων βαρύνει τους υπευθύνους επεξεργασίας και όχι τους εκτελούντες.

## 6.1 Διαφάνεια και άσκηση δικαιωμάτων

Η αρχή της διαφάνειας επιβάλει να παρέχεται στα υποκείμενα των δεδομένων η δυνατότητα να ζητούν από τους υπευθύνους επεξεργασίας να λογοδοτούν, καθώς και να ασκούν έλεγχο επί των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Μάλιστα, οι απαιτήσεις διαφάνειας που προβλέπονται στον ΓΚΠΔ (και συνδέονται με τις υποχρεώσεις ενημέρωσης, την άσκηση δικαιωμάτων και την υποχρέωση ενημέρωσης σε περίπτωση περιστατικού παραβίασης) ισχύουν ανεξάρτητα από τη νομική βάση για την επεξεργασία και εφαρμόζονται και καθ' όλη τη διάρκεια της επεξεργασίας. Ο Κανονισμός μπορεί να μην ορίζει ρητά τι είναι «διαφάνεια» αλλά έχει ένα ειδικό άρθρο, το άρθρο 12, στο οποίο προδιαγράφεται αναλυτικότατα ο τρόπος με τον οποίο ένας υπεύθυνος επεξεργασίας οφείλει να ενεργεί σε σχέση με την ενημέρωση που παρέχει προς τα υποκείμενα των δεδομένων και σε σχέση με τις διαδικασίες που οφείλει να ακολουθεί για την ανταπόκρισή του σε όλα τα δικαιώματα που καθιερώνει ο ΓΚΠΔ για τα υποκείμενα των δεδομένων. Μάλιστα, ένα από τα πρώτα κείμενα καθοδήγησης που εξέδωσαν οι ευρωπαϊκές εποπτικές αρχές κατά την προετοιμασία τους για την εφαρμογή του Κανονισμού, υπό την ομπρέλα της Ο.Ε. του άρθρου 29, ήταν οι Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679 [41]. Το κείμενο αυτό έχει υιοθετηθεί και από το ΕΣΠΔ.

Διαφάνεια σημαίνει ότι ο υπεύθυνος επεξεργασίας έρχεται σε επικοινωνία με το υποκείμενο των δεδομένων, είτε προληπτικά είτε κατόπιν αιτήματός του. Κατά την επικοινωνία αυτή, ο υπεύθυνος οφείλει να συμμορφώνεται με τους παρακάτω κανόνες:

- Οι πληροφορίες που παρέχει πρέπει να είναι **συνοπτικές, διαφανείς, κατανοητές και εύκολα προσβάσιμες** (άρθρο 12 παράγραφος 1)

  «Συνοπτικές και διαφανείς» σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να παρουσιάζουν τις πληροφορίες με τρόπο ώστε να αποφεύγεται η δημιουργία κούρασης λόγω της παροχής πληροφοριών. Οι πληροφορίες πρέπει να διαφοροποιούνται με σαφήνεια από άλλες σχετικές πληροφορίες που δεν αφορούν την προστασία των προσωπικών δεδομένων, όπως συμβατικές διατάξεις ή γενικοί όροι χρήσης.

  «Κατανοητές» σημαίνει ότι η γλώσσα πρέπει να κατάλληλη για το μέσο αναγνώστη του κοινού στο οποίο απευθύνονται. Λαμβάνεται υπόψη αν προορίζονται για άτομα με ελαφρά δυσκολία αναγνώσεως λόγω ηλικίας, χαμηλού μορφωτικού επιπέδου ή απλώς επειδή δεν έχουν ως μητρική γλώσσα την επίσημη γλώσσα του κράτους μέλους. Πρέπει να γίνεται χρήση της επίσημης γλώσσας του κράτους, αλλά αν οι πληροφορίες απευθύνονται, κατά

κανόνα, και σε αλλόγλωσσα υποκείμενα των δεδομένων πρέπει να παρέχεται ενημέρωση (σωρευτικά) και σε άλλη γλώσσα. Αυτό, για παράδειγμα, είναι υποχρέωση για συγκεκριμένες υπηρεσίες του Υπουργείου Εξωτερικών ή του Υπουργείου Μετανάστευσης και Ασύλου.

«Εύκολα προσβάσιμες» σημαίνει ότι το υποκείμενο των δεδομένων πρέπει να μπορεί άμεσα να βρει τις πληροφορίες, χωρίς να χρειαστεί να τις αναζητήσει.

☞ Κάθε φορέας που διατηρεί έναν ιστότοπο θα πρέπει να αναρτά μια δήλωση σχετικά με την προστασία των προσωπικών δεδομένων. Ένας απευθείας σύνδεσμος προς αυτή τη δήλωση θα πρέπει να είναι εμφανής σε κάθε σελίδα αυτού του ιστοτόπου με τη χρήση ενός ευρέως χρησιμοποιούμενου όρου (π.χ. «Πολιτική Προστασίας Δεδομένων»)

- Πρέπει να χρησιμοποιείται **απλή και σαφής διατύπωση** (άρθρο 12 παράγραφος 1)

  Οι πληροφορίες θα πρέπει να παρέχονται με τον απλούστερο δυνατό τρόπο, ενώ παράλληλα θα πρέπει να αποφεύγεται η χρήση σύνθετων προτάσεων και γλωσσικών δομών. Οι πληροφορίες θα πρέπει να είναι συγκεκριμένες και σαφείς, χωρίς να διατυπώνονται με αφηρημένους ή αμφιλεγόμενους όρους ή να αφήνουν περιθώριο για διαφορετικές ερμηνείες. Η χρήση γλωσσικών προσδιορισμών όπως «ενδέχεται», «ορισμένος», «συχνά» και «πιθανώς» θα πρέπει να αποφεύγεται. Αποφεύγεται επίσης η χρήση νομικής ορολογίας, ξενόγλωσσων και αόριστων όρων και η παροχή άσκοπης υπερπληροφόρησης.

**Παράδειγμα ανεπαρκούς πρακτικής:** «Ενδέχεται να χρησιμοποιήσουμε τα δεδομένα προσωπικού χαρακτήρα σας για ερευνητικούς σκοπούς»
Είναι ασαφές για τι είδους «έρευνα» πρόκειται και είναι ασαφές αν και υπό ποιες προϋποθέσεις θα υλοποιηθεί η έρευνα.

**Παράδειγμα ορθής πρακτικής:** «Θα διατηρήσουμε και θα αξιολογήσουμε τις πληροφορίες σχετικά με τις πρόσφατες επισκέψεις σας στον ιστότοπό μας και τον



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τρόπο πλοήγησής σας στον ιστότοπό μας για σκοπούς ανάλυσης, ώστε να κατανοήσουμε τον τρόπο με τον οποίο τα άτομα χρησιμοποιούν τον ιστότοπό μας και τον καταστήσουμε πιο λειτουργικό»
Είναι σαφές ποια είδη δεδομένων θα υποβληθούν σε επεξεργασία και είναι σαφής ο τύπος της ανάλυσης που θα διενεργήσει ο υπεύθυνος επεξεργασίας

- η απαίτηση για σαφή και απλή διατύπωση είναι ιδιαίτερης σημασίας κατά την παροχή πληροφοριών σε παιδιά (άρθρο 12 παράγραφος 1)
  Το λεξιλόγιο, ο τόνος και το ύφος της γλώσσας που χρησιμοποιείται, πρέπει να είναι κατάλληλα για παιδιά, ώστε το παιδί που είναι ο αποδέκτης των πληροφοριών να αναγνωρίζει ότι το μήνυμα και η πληροφορία απευθύνεται σε αυτό. Μάλιστα, το γεγονός ότι σε ανηλίκους η συγκατάθεση ή η σύμβαση απαιτεί την παρέμβαση του γονέα ή κηδεμόνα, δεν σημαίνει ότι τα παιδιά δεν είναι τα υποκείμενα των δεδομένων και ότι οι πληροφορίες δεν πρέπει να απευθύνονται προς αυτά.

- Οι πληροφορίες πρέπει να παρέχονται **γραπτώς** «ή με άλλα μέσα, μεταξύ άλλων, **εφόσον ενδείκνυται, ηλεκτρονικώς**» (άρθρο 12 παράγραφος 1)
  - όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά (άρθρο 12 παράγραφος 1)

  Η κατ΄ αρχήν θέση του ΓΚΠΔ, όσον αφορά την παροχή πληροφοριών σε υποκείμενα των δεδομένων ή τις επικοινωνίες με αυτά, είναι ότι οι πληροφορίες πρέπει να παρέχονται γραπτώς. Ο ΓΚΠΔ αφήνει περιθώριο για τη χρήση άλλων, απροσδιόριστων «μέσων», συμπεριλαμβανομένων των ηλεκτρονικών μέσων, όταν ενδείκνυται. Οι πληροφορίες μπορούν να δίνονται προφορικά σε ένα υποκείμενο των δεδομένων κατόπιν αιτήματος του, υπό την προϋπόθεση ότι η ταυτότητά του είναι αποδεδειγμένη με άλλα μέσα. Η προφορική παροχή πληροφοριών συνδέεται μόνο με την ανταπόκριση του υπευθύνου σε δικαιώματα του υποκειμένου των δεδομένων και όχι με την γενική ενημέρωση για την επεξεργασία.
- Οι πληροφορίες, εν γένει, πρέπει να παρέχονται **δωρεάν** (άρθρο 12 παράγραφος 5).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Οι υπεύθυνοι επεξεργασίας δεδομένων δεν επιτρέπεται να χρεώνουν τα υποκείμενα των δεδομένων για την παροχή των πληροφοριών και για την άσκηση των δικαιωμάτων. Οποιαδήποτε πληροφορία παρέχεται για σκοπούς διαφάνειας δεν μπορεί να εξαρτάται από οικονομικές συναλλαγές.

## 6.2 Κανόνες που εφαρμόζονται στην άσκηση των δικαιωμάτων

Καθώς η άσκηση των δικαιωμάτων θεωρείται βασικό συστατικό της αρχής της διαφάνειας, οι κανόνες της προηγούμενης ενότητας εφαρμόζονται όχι μόνο για την παροχή των αρχικών πληροφοριών σε υποκείμενα των δεδομένων αλλά και κατά την ανταπόκριση του υπεύθυνου επεξεργασίας σε αιτήματα του υποκειμένου των δεδομένων για άσκηση δικαιώματος του ΓΚΠΔ με βάση τα άρθρα 15 έως 22. Το άρθρο 12 προσδιορίζει, επιπλέον, και τους κανόνες που οφείλουν να τηρούν οι υπεύθυνοι επεξεργασίας όταν ανταποκρίνονται σε τέτοια αιτήματα του υποκειμένου των δεδομένων. Ειδικότερα:

- Ο υπεύθυνος επεξεργασίας **διευκολύνει την άσκηση των δικαιωμάτων** των υποκειμένων των δεδομένων που προβλέπονται στα άρθρα 15 έως 22. Στις περιπτώσεις που προβλέπονται στο άρθρο 11 παράγραφος 2, ο υπεύθυνος επεξεργασίας δεν αρνείται να ενεργήσει κατόπιν αιτήσεως του υποκειμένου των δεδομένων για να ασκήσει τα δικαιώματά του βάσει των άρθρων 15 έως 22, εκτός αν ο υπεύθυνος επεξεργασίας αποδείξει ότι δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων.
- Οι ενέργειες του υπευθύνου επεξεργασίας για την ανταπόκριση σε δικαιώματα γίνονται **δωρεάν** για το υποκείμενο των δεδομένων.

  Κατ΄ εξαίρεση, ο υπεύθυνος επεξεργασίας μπορεί να ζητήσει την καταβολή εύλογου τέλους ή να αρνηθεί να δώσει συνέχεια στο αίτημα, αν τα αιτήματα του υποκειμένου των δεδομένων είναι **προδήλως αβάσιμα ή υπερβολικά.** Ο Κανονισμός αναφέρει ειδικά ότι επαναλαμβανόμενα αιτήματα μπορεί να θεωρηθούν υπερβολικά, αλλά και ότι, σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας φέρει το βάρος της απόδειξης του προδήλως αβάσιμου ή του υπερβολικού χαρακτήρα του αιτήματος.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

☞ Ακόμα και σε προδήλως αβάσιμα ή υπερβολικά αιτήματα, ο υπεύθυνος επεξεργασίας οφείλει να απαντήσει (αρνητικά) στο υποκείμενο των δεδομένων, ενημερώνοντάς το για την κρίση του.

- Ο υπεύθυνος επεξεργασίας οφείλει να ανταποκρίνεται χωρίς καθυστέρηση στα αιτήματα άσκησης δικαιωμάτων και **το αργότερο σε ένα μήνα από την υποβολή** του αιτήματος. Η προθεσμία του ενός μηνός μπορεί να παραταθεί για δύο μήνες, εάν το αίτημα είναι πολύπλοκο ή ο αριθμός των αντιγράφων που πρέπει να χορηγήσει ο υπεύθυνος επεξεργασίας είναι μεγάλος. Ωστόσο, ο υπεύθυνος οφείλει να ενημερώσει το υποκείμενο για την παράταση αυτή εντός μηνός από την υποβολή του αιτήματος.
- Ο υπεύθυνος επεξεργασίας μπορεί να κρίνει ότι δεν απαιτείται να ενεργήσει επί του αιτήματος του υποκειμένου των δεδομένων. Τότε, είναι υποχρεωμένος να ενημερώσει το υποκείμενο των δεδομένων, χωρίς καθυστέρηση και το αργότερο εντός μηνός από την παραλαβή του αιτήματος, για τους λόγους για τους οποίους δεν ενήργησε και για τη δυνατότητα υποβολής καταγγελίας στην ΑΠΔΠΧ και για την άσκηση δικαστικής προσφυγής.
- Όταν ο υπεύθυνος επεξεργασίας αμφιβάλλει σχετικά με την ταυτότητα του προσώπου που υποβάλλει αίτημα άσκησης δικαιωμάτων, μπορεί να ζητήσει την παροχή πρόσθετων πληροφοριών αναγκαίων για την **επιβεβαίωση της ταυτότητας** του υποκειμένου των δεδομένων. Τέτοιες πληροφορίες μπορεί να είναι επίδειξη ή αντίγραφο ταυτότητας ή άλλου είδους βεβαίωση (π.χ. δήλωση από το gov.gr). Ο υπεύθυνος επεξεργασίας δεν υποχρεούται να τηρεί συμπληρωματικές πληροφορίες για την εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων αποκλειστικά και μόνο για την ικανοποίηση των δικαιωμάτων.

**Παράδειγμα:** Υπεύθυνος επεξεργασίας λειτουργεί διαδικτυακή εφαρμογή στην οποία φυσικά πρόσωπα μπορούν να εγγραφούν ως χρήστες με βασικό αναγνωριστικό το email τους. Ο υπεύθυνος επεξεργασίας δέχεται έγγραφο αίτημα άσκησης δικαιώματος πρόσβασης. Ο υπεύθυνος επεξεργασίας για την επιβεβαίωση της ταυτότητας του



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

υποκειμένου των δεδομένων, δεν μπορεί να ζητήσει αντίγραφο ταυτότητας, άλλωστε δεν τηρεί τα κατάλληλα στοιχεία για την αντιπαραβολή αυτή. Μπορεί όμως να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου προς την εγγεγραμμένη ηλεκτρονική διεύθυνση, στην οποία να ζητάει επιβεβαίωση του αιτήματος πρόσβασης.

**Παράδειγμα:** Δημόσιος φορέας διατηρεί ηλεκτρονική εφαρμογή σε ιστοσελίδα του, στην οποία επεξεργάζεται αιτήσεις πολιτών με χρήση κωδικών taxisnet. Ο φορέας δέχεται έγγραφο αίτημα για άσκηση δικαιώματος πρόσβασης με παραδοσιακό ταχυδρομείο. Ο αιτών έχει μάλιστα προσέλθει στα γραφεία του φορέα. Με αντιπαραβολή με τα διαθέσιμα στοιχεία, ο φορέας δεν μπορεί να επιβεβαιώσει ότι το έγγραφο αίτημα προέρχεται, με επαρκή βεβαιότητα, από το υποκείμενο των δεδομένων. Για το σκοπό αυτό, μπορεί να ζητήσει από τον αιτούντα να του επιδείξει ταυτότητα.

## 6.3 Παροχή ενημέρωσης σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Το πρώτο βήμα για την ικανοποίηση της αρχής της διαφάνειας είναι η παροχή κατάλληλης ενημέρωσης προς τα υποκείμενα των δεδομένων. Ο ΓΚΠΔ ορίζει συγκεκριμένες πληροφορίες τις οποίες, κατ' ελάχιστον, οφείλει να παρέχει ο υπεύθυνος επεξεργασίας στα υποκείμενα των δεδομένων. Ανάλογα με το αν τα δεδομένα συλλέγονται από το υποκείμενο των δεδομένων ή από άλλη πηγή εφαρμόζεται το άρθρο 13 του ΓΚΠΔ (από το υποκείμενο), ή το άρθρο 14 (από τρίτη πηγή). Οι κατηγορίες των πληροφοριών είναι όμως, σε μεγάλο βαθμό παρόμοιες. Οι πληροφορίες αναφέρονται ρητά στις παραγράφους 1 και 2 των άρθρων 13 και 14. Στην παράγραφο 2 γίνεται αναφορά σε επιπλέον πληροφορίες που είναι αναγκαίες για την εξασφάλιση θεμιτής και διαφανούς επεξεργασίας, αλλά το ΕΣΠΔ έχει επισημάνει ότι αυτό δεν διαφοροποιεί σε κάτι την υποχρέωση ενός υπεύθυνου επεξεργασίας να παρέχει όλες τις πληροφορίες. Οι πληροφορίες αυτές παρουσιάζονται στον παρακάτω πίνακα, με επισήμανση με το αν απαιτείται όταν συλλέγονται από το υποκείμενο ή από τρίτη πηγή.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

| **Πληροφορία** | **Αρ. 13** | **Αρ. 14** |
|---|---|---|
| Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας[17] | ✔ | ✔ |
| Στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων (DPO) | ✔ | ✔ |
| Σκοποί επεξεργασίας, και νομική βάση για κάθε σκοπό | ✔ | ✔ |
| Αν η επεξεργασία βασίζεται στο άρθρο 6 παρ. 1 στ' τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο | ✔ | ✔ |
| Κατηγορίες δεδομένων προσωπικού χαρακτήρα σε σχέση με συγκεκριμένο σκοπό | ✘ | ✔ |
| Αποδέκτες ή κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα | ✔ | ✔ |
| Αναλυτικές πληροφορίες για τις διαβιβάσεις σε τρίτες χώρες | ✔ | ✔ |
| Χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα ή, όταν αυτό δεν είναι δυνατό να προσδιοριστεί, τα κριτήρια που καθορίζουν το εν λόγω διάστημα | ✔ | ✔ |
| Ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για την άσκηση των δικαιωμάτων των άρθρων 15-21 του ΓΚΠΔ | ✔ | ✔ |
| Αν η επεξεργασία βασίζεται σε συγκατάθεση, την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσης. | ✔ | ✔ |
| Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (την ΑΠΔΠΧ στην Ελλάδα) | ✔ | ✔ |
| Αν η παροχή των προσωπικών δεδομένων αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα του και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών. | ✔ | ✘ |

[17] Και κατά περίπτωση του εκπροσώπου του υπευθύνου επεξεργασίας, αλλά χωρίς πρακτική εφαρμογή σε δημόσιο τομέα



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

| | | |
|---|---|---|
| Τις πηγές από τις οποίες προέρχονται τα προσωπικά δεδομένα με ειδική αναφορά στο εάν τα δεδομένα προήλθαν από πηγές στις οποίες έχει πρόσβαση το κοινό | ✗ | ✔ |
| Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, και βασικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων | ✔ | ✔ |

### 6.3.1 Τρόπος παροχής ενημέρωσης

Ενθυμούμενοι τις βασικές προϋποθέσεις της διαφάνειας που αναλύσαμε νωρίτερα, η ενημέρωση πρέπει να παρέχεται ενεργά από τον υπεύθυνο επεξεργασίας, και όχι να αναζητείται από το υποκείμενο των δεδομένων. Το ΕΣΠΔ, υιοθετώντας τις κατευθυντήριες γραμμές για τη διαφάνεια [41], συνιστά το σύνολο των πληροφοριών που απευθύνονται στα υποκείμενα των δεδομένων να διατίθεται σε αυτά σε ένα μόνο σημείο ή σε ένα πλήρες έγγραφο (την πολιτική για την προστασία των προσωπικών δεδομένων).

Καθώς υπάρχει η απαίτηση ο τρόπος ενημέρωσης να είναι ευδιάκριτος, κατανοητός και ευανάγνωστος, το ΕΣΠΔ επισημαίνει τη σημασία της πολυεπίπεδης προσέγγισης για την παροχή πληροφοριών στην πολιτική προστασίας προσωπικών δεδομένων (layered privacy statement/notice).

- Σε ψηφιακή εφαρμογή, βασικές πληροφορίες της πολιτικής προστασίας δεδομένων εμφανίζονται σε μια πρώτη οθόνη, ενώ οι λεπτομερειακές πληροφορίες εμφανίζονται σε επόμενες ιστοσελίδες, στις οποίες μπορεί να οδηγηθεί ο χρήστης με υπερσυνδέσμους. Έτσι αποφεύγεται η δημιουργία κούρασης λόγω της παροχής πληροφοριών. Οι πληροφορίες πρώτου επιπέδου προτείνεται να περιλαμβάνουν τους σκοπούς της επεξεργασίας, την ταυτότητα του υπευθύνου επεξεργασίας και μια περιγραφή των δικαιωμάτων του υποκειμένου των δεδομένων καθώς για την επεξεργασία που έχει το μεγαλύτερο αντίκτυπο στο υποκείμενο των δεδομένων ή που θα μπορούσε να του προκαλέσει έκπληξη. Βέβαια, σε ψηφιακές εφαρμογές, ο τρόπος παροχής



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

της ενημέρωσης μπορεί να βελτιώνεται με τη χρήση πρόσθετων μεθόδων, όμως αναδυόμενα παράθυρα, παροχή ενημέρωσης στο κατάλληλο σημείο (just-in-time), εικονίδια (icons), cartoons, infographics, βίντεο, πίνακες ιδιωτικότητας (privacy dashboards) κ.ά..

- Σε μη ψηφιακό περιβάλλον, ο υπεύθυνος επεξεργασίας θα πρέπει να εξασφαλίζει την ενημέρωση, ανάλογα με το μέσο. Για παράδειγμα, η ενημέρωση πρώτου επιπέδου με τα βασικά χαρακτηριστικά (σκοπός, υπεύθυνος επεξεργασίας, δικαιώματα) μπορεί να αποτυπώνεται σε μια πινακίδα όταν χρησιμοποιείται σύστημα βιντεοεπιτήρησης, να αναφέρεται προφορικά όταν γίνεται συλλογή δεδομένων μέσω τηλεφώνου, ή να αναγράφεται ευδιάκριτα σε έντυπο συλλογής στοιχείων, με παραπομπή σε αναλυτική ενημέρωση.
-

☞ Ο υπεύθυνος επεξεργασίας δεν πρέπει να επαναπαύεται στην κατάρτιση και ανάρτηση μια πολιτικής προστασίας δεδομένων, αλλά να φροντίζει ότι θα φτάσει στο υποκείμενο των δεδομένων με κατάλληλο τρόπο, συνυπολογίζοντας τον τρόπο με τον οποίο διενεργείται η επεξεργασία.

Οι υπεύθυνοι επεξεργασίας θα πρέπει να εξετάζουν τη χρήση διαφόρων εργαλείων απεικόνισης, τα οποία διευκολύνουν την κατανόηση των πληροφοριών. Τέτοια μπορεί να είναι: τυποποιημένα εικονίδια, μηχανισμοί πιστοποίησης, σφραγίδες και σήματα προστασίας δεδομένων. Βέβαια, έως σήμερα δεν έχουν αναπτυχθεί τέτοια εργαλεία.

**Παράδειγμα:** Δημόσιος φορέας επεκτείνει ηλεκτρονική εφαρμογή στην οποία επεξεργάζεται αιτήσεις πολιτών με χρήση κωδικών taxisnet, ώστε εκτός της χρήσης Η/Υ να παρέχει εφαρμογή (app) σε κινητά τηλέφωνα. Ο φορέας είχε ήδη κείμενο πολιτικής προστασίας δεδομένων σε ιστοσελίδα. Για την παροχή της πληροφόρησης σε συσκευές κινητών τηλεφώνων, ο φορέας οφείλει να ελέγξει ότι οι πληροφορίες εμφανίζονται ορθά και στις συσκευές αυτές και να προβεί σε κατάλληλες αλλαγές, ώστε να είναι εύκολη η ανάγνωση της πολιτικής από κινητά τηλέφωνα.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Παράδειγμα:** Δημόσιος φορέας χρησιμοποιεί τυποποιημένα έντυπα για την κατάθεση αιτήσεων. Καθώς με την κατάθεση της αίτησης γίνεται συλλογή προσωπικών δεδομένων, ο φορέας οφείλει να φροντίσει για την παροχή κατάλληλης πληροφόρησης. Το πρώτο επίπεδο της πληροφόρησης πρέπει να αναγράφεται στο έντυπο, ενώ για τα λοιπά στοιχεία μπορεί να υπάρχει παραπομπή σε αναλυτικότερο κείμενο, διαθέσιμο εντύπως ή/και ηλεκτρονικά.

### 6.3.2 Χρόνος παροχής ενημέρωσης

Οι πληροφορίες πρέπει να παρέχονται στο υποκείμενο των δεδομένων κατά το στάδιο έναρξης του κύκλου επεξεργασίας.

#### 6.3.2.1 Συλλογή από το υποκείμενο των δεδομένων

Στις περιπτώσεις που τα δεδομένα συλλέγονται από τα υποκείμενα των δεδομένων είναι σαφές ότι οι πληροφορίες πρέπει να παρέχονται κατά το χρόνο της συλλογής. Στην περίπτωση αυτή, που εφαρμόζεται το άρθρο 13 του Κανονισμού, η συλλογή μπορεί να γίνεται:

- Όταν το υποκείμενο των δεδομένων παρέχει συνειδητά σε έναν υπεύθυνο επεξεργασίας δεδομένων τις πληροφορίες (π.χ., κατά τη συμπλήρωση ενός διαδικτυακού εντύπου) ή
- Όταν ο υπεύθυνος επεξεργασίας δεδομένων συλλέγει τα δεδομένα από το υποκείμενο μέσω παρατήρησης (π.χ., χρησιμοποιώντας κάμερες, συσκευές καταγραφής δεδομένων ή λογισμικό καταγραφής δεδομένων, εξοπλισμό δικτύου, παρακολούθηση Wi-Fi, RFID κ.ά).

#### 6.3.2.2 Συλλογή από τρίτες πηγές

Σε περίπτωση μη απευθείας λήψης δεδομένων προσωπικού χαρακτήρα, οι προθεσμίες εντός των οποίων πρέπει να παρέχονται οι απαιτούμενες πληροφορίες στο υποκείμενο των δεδομένων ορίζονται στο άρθρο 14 παρ. 3:

i. Σε εύλογο χρόνο από τη συλλογή των δεδομένων προσωπικού χαρακτήρα, και το αργότερο εντός ενός μηνός.

   Λαμβάνονται υπόψη οι ειδικές συνθήκες υπό τις οποίες τα δεδομένα

προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία.

ii. Εάν όμως, τα δεδομένα προσωπικού χαρακτήρα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο των δεδομένων, το αργότερο κατά την πρώτη επικοινωνία με το υποκείμενο.

Στην περίπτωση αυτή δηλαδή, ο χρόνος επικοινωνίας είναι μικρότερος του μήνα. Έτσι εξασφαλίζεται ότι το αργότερο τη στιγμή που το υποκείμενο λάβει την επικοινωνία θα είναι σε θέση να αντιληφθεί τις πτυχές της επεξεργασίας των δεδομένων του.

iii. Εάν προβλέπεται γνωστοποίηση σε άλλον αποδέκτη, το αργότερο όταν τα δεδομένα προσωπικού χαρακτήρα γνωστοποιούνται για πρώτη φορά.

Και πάλι ο χρόνος επικοινωνίας είναι μικρότερος του μήνα. Έτσι εξασφαλίζεται ότι το υποκείμενο θα είναι σε θέση να αντιληφθεί τις πτυχές της επεξεργασίας των δεδομένων του (και ενδεχομένως να ασκήσει τα δικαιώματά του) το αργότερο πριν αυτά χρησιμοποιηθούν περαιτέρω.

### 6.3.3 Αλλαγές στις παρεχόμενες πληροφορίες

Ειδικά σε διαρκείς επεξεργασίες δεν είναι απίθανο να αλλάξει το περιεχόμενο των στοιχείων που περιλαμβάνονται στα άρθρα 13 και 14, όπως για παράδειγμα με την αλλαγή ενός αποδέκτη ή με την τροποποίηση μιας κατηγορίας δεδομένων. Σε περίπτωση που υπάρχει «ουσιώδης» αλλαγή στις παρεχόμενες στα υποκείμενα των δεδομένων πληροφορίες (π.χ. σε σχέση με τα δικαιώματά τους), ο υπεύθυνος επεξεργασίας οφείλει να προβεί σε ενημέρωση των υποκειμένων των δεδομένων σε σχέση με τις αλλαγές.

Τα περισσότερα υποκείμενα των δεδομένων αναμένεται να μη δώσουν προσοχή στις γνωστοποιήσεις των αλλαγών και να τις διαβάσουν επιδερμικά. Γι' αυτό, ο υπεύθυνος επεξεργασίας θα πρέπει να εξασφαλίσει ότι οι αλλαγές γνωστοποιούνται κατά τρόπο που οι περισσότεροι αποδέκτες όντως θα τις αντιληφθούν. Μια γνωστοποίηση αλλαγών θα πρέπει πάντα να πραγματοποιείται με τον κατάλληλο τρόπο ώστε να λάβει την προσοχή του υποκειμένου των δεδομένων (π.χ., μήνυμα ηλεκτρονικού ταχυδρομείου, έντυπη επιστολή, αναδυόμενο παράθυρο σε ιστοσελίδα ή άλλος τρόπος). Η ενημέρωση πρέπει να πληροί τις απαιτήσεις του άρθρου 12, δηλαδή, να είναι συνοπτική, διαφανής, κατανοητή και εύκολα προσβάσιμη. Εάν η



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αλλαγή στις πληροφορίες υποδεικνύει θεμελιώδη αλλαγή στη φύση της επεξεργασίας (π.χ., διεύρυνση των κατηγοριών αποδεκτών ή προσθήκη της δυνατότητας διαβιβάσεων σε τρίτη χώρα) οι πληροφορίες θα πρέπει να παρέχονται στο υποκείμενο των δεδομένων αρκετό χρόνο πριν από την πραγματοποίηση της αλλαγής.

☞ Καθώς πολλά υποκείμενα των δεδομένων δεν θυμούνται τις πληροφορίες που τους παρασχέθηκαν κατά τη συλλογή, το ΕΣΠΔ συνιστά να υπάρχει συνεχής και εύκολη πρόσβαση στις πληροφορίες.

### 6.3.4 Πληροφορίες σχετικά με περαιτέρω επεξεργασία

Σε περίπτωση που ένας υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί (περαιτέρω) τα δεδομένα προσωπικού χαρακτήρα για σκοπό διαφορετικό από εκείνον για τον οποίο τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά, οφείλει να παρέχει στο υποκείμενο των δεδομένων, **πριν από την εν λόγω περαιτέρω επεξεργασία**, συγκεκριμένες πληροφορίες οι οποίες περιλαμβάνουν, ειδικά, τον νέο σκοπό και τις πληροφορίες που αναγράφονται στις παραγράφους 2 των άρθρων 13 και 14. Το ΕΣΠΔ μάλιστα συνιστά να τίθεται στη διάθεση των υποκειμένων των δεδομένων και μια επεξήγηση όσον αφορά τον τρόπο με τον οποίο η επεξεργασία για διαφορετικό σκοπό είναι συμβατή προς τον αρχικό σκοπό, ως τμήμα των υποχρεώσεων διαφάνειας. Οι παραπάνω πληροφορίες πρέπει να παρέχονται πριν την περαιτέρω επεξεργασία ενώ, κατά προτίμηση, θα πρέπει να μεσολαβεί εύλογο χρονικό διάστημα μεταξύ της νέας ενημέρωσης και της έναρξης της περαιτέρω επεξεργασίας.

### 6.3.5 Εξαιρέσεις από την υποχρέωση παροχής ενημέρωσης

Η μόνη εξαίρεση από τις υποχρεώσεις ενός υπευθύνου επεξεργασίας για την παροχή των πληροφοριών που προβλέπονται στο άρθρο 13 όταν έχει συλλέξει δεδομένα προσωπικού χαρακτήρα απευθείας από ένα υποκείμενο των δεδομένων είναι «*όταν και εφόσον το υποκείμενο των δεδομένων έχει ήδη τις πληροφορίες*». Η εξαίρεση αυτή ισχύει και με βάση το άρθρο 14.

Με βάση την αρχή της λογοδοσίας, για να χρησιμοποιήσουν αυτή την εξαίρεση, οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να αποδεικνύουν (και να καταγράφουν) τις πληροφορίες που έχει ήδη το υποκείμενο των δεδομένων, με ποιο τρόπο και πότε

τις έλαβε, καθώς και ότι δεν έχουν προκύψει αλλαγές έκτοτε σε αυτές τις πληροφορίες.

Στο άρθρο 14 υπάρχουν τρεις ακόμα εξαιρέσεις από την υποχρέωση παροχής ενημέρωσης:

1) Όταν η παροχή των πληροφοριών αποδεικνύεται **αδύνατη** ή θα συνεπαγόταν **δυσανάλογη προσπάθεια**, ιδίως όσον αφορά επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, ή εφόσον η υποχρέωση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου **είναι πιθανόν να καταστήσει αδύνατη ή να βλάψει** σε μεγάλο βαθμό **την επίτευξη των σκοπών της εν λόγω επεξεργασίας**.
    - Η ενημέρωση μπορεί να είναι αδύνατη όταν ο υπεύθυνος επεξεργασίας δεν διαθέτει τρόπο επικοινωνίας με το υποκείμενο των δεδομένων.
    - Η προϋπόθεση για δυσανάλογη προσπάθεια αφορά, ιδίως, τις περιπτώσεις αρχειοθέτησης, έρευνας και στατιστικής, όταν π.χ. ο προσδιορισμός του υποκειμένου των δεδομένων απαιτεί άρση της ψευδωνυμοποίησης.
    - Η τρίτη υποπερίπτωση μεταφέρει στον υπεύθυνο επεξεργασίας το βάρος της απόδειξης ότι η παροχή των πληροφοριών που ορίζονται στο άρθρο 14 παράγραφος 1 θα ακύρωνε τους στόχους της επεξεργασίας. Η επίκληση αυτής της εξαίρεσης προϋποθέτει ότι η επεξεργασία των δεδομένων είναι σύμφωνη με τις αρχές που προβλέπονται στο άρθρο 5.

    Σε κάθε περίπτωση που δεν παρέχεται πληροφόρηση (ατομικά) προς τα υποκείμενα των δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να λάβει κατάλληλα μέτρα, μεταξύ άλλων καθιστώντας τις πληροφορίες διαθέσιμες στο κοινό, π.χ. με δημόσια ανάρτηση στη ιστοσελίδα του ή και με ανακοίνωση.
2) Όταν η απόκτηση ή η κοινολόγηση των δεδομένων προβλέπεται ρητώς σε νόμο ο οποίος περιέχει κατάλληλα μέτρα για την προστασία των έννομων συμφερόντων του υποκειμένου των δεδομένων.

    Αυτή η εξαίρεση, η οποία αφορά και δημόσιες αρχές, εξαρτάται από το εάν το



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εν λόγω δίκαιο «παρέχει τα κατάλληλα μέτρα για την προστασία των έννομων συμφερόντων του υποκειμένου των δεδομένων». Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να είναι σε θέση να αποδείξει τον τρόπο με τον οποίο ο νόμος περιέχει τις κατάλληλες διασφαλίσεις ώστε να του δίνει τη δυνατότητα να επικαλεστεί την εν λόγω εξαίρεση.

**Παράδειγμα:** Δημόσια Αρχή κοινωνικής ασφάλισης, σύμφωνα με νόμο, λαμβάνει τα στοιχεία κρατήσεων των εργαζομένων από τους εργοδότες τους. Τα δεδομένα προσωπικού χαρακτήρα δεν λαμβάνονται από τα υποκείμενα των δεδομένων και, συνεπώς, η δημόσια Αρχή υπόκειται στις απαιτήσεις του άρθρου 14. Δεδομένου ότι η λήψη των δεδομένων προσωπικού χαρακτήρα από τους εργοδότες προβλέπεται ρητώς στο νόμο για τη λειτουργία της δημόσιας αρχής και ότι οι εργαζόμενοι πρέπει να ενημερώνονται, γενικά, για τις κρατήσεις της μισθοδοσίας τους, οι απαιτήσεις για παροχή πληροφοριών στο άρθρο 14 δεν ισχύουν για τη εν λόγω Αρχή στην προκειμένη περίπτωση.

3) Όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να παραμείνουν εμπιστευτικά λόγω υποχρέωσης επαγγελματικού απορρήτου που ρυθμίζεται με νόμο.

   Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας που θέλει να επικαλεστεί αυτή την εξαίρεση, πρέπει να είναι σε θέση να τεκμηριώσει την εφαρμογή της με αναφορά στις σχετικές διατάξεις.

☞ Με την αρχή της λογοδοσίας, όλες οι εξαιρέσεις από την παροχή ενημέρωσης πρέπει να τεκμηριώνονται.

## 6.4 Το δικαίωμα πρόσβασης

Το δικαίωμα πρόσβασης (άρθρο 15 του ΓΚΠΔ) αποτελεί βασικό μέρος του ευρωπαϊκού συστήματος προστασίας δεδομένων από την αρχή του, αλλά ο ΓΚΠΔ περιέχει περισσότερο συγκεκριμένους κανόνες.

### 6.4.1 Σκοπός του δικαιώματος πρόσβασης

Ο βασικός στόχος του δικαιώματος πρόσβασης είναι να παρέχει στα άτομα επαρκείς, διαφανείς και εύκολα προσβάσιμες πληροφορίες σχετικά με την επεξεργασία



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

δεδομένων προσωπικού χαρακτήρα, ώστε να έχουν **επίγνωση** και να μπορούν να επαληθεύουν τη νομιμότητα της επεξεργασίας και την ακρίβεια των δεδομένων τους. Διευκολύνει επίσης –αλλά δεν αποτελεί προϋπόθεση– το υποκείμενο των δεδομένων να ασκήσει άλλα δικαιώματα, όπως το δικαίωμα διαγραφής ή το δικαίωμα διόρθωσης.

Το υποκείμενο των δεδομένων δεν οφείλει να αιτιολογήσει για ποιο λόγο υποβάλει το αίτημα πρόσβασης. Ο υπεύθυνος επεξεργασίας δεν μπορεί να αναλύσει εάν το αίτημα θα βοηθήσει πράγματι το υποκείμενο των δεδομένων να επαληθεύσει τη νομιμότητα ή να ασκήσει άλλα δικαιώματα. Θα πρέπει να ικανοποιήσει το αίτημα εκτός εάν είναι σαφές ότι το αίτημα υποβάλλεται σύμφωνα με άλλους κανόνες εκτός από τους κανόνες προστασίας δεδομένων.

Το δικαίωμα πρόσβασης περιλαμβάνει τρία διαφορετικά στοιχεία:

- **Επιβεβαίωση** για το εάν προσωπικά δεδομένα του αιτούντος υποβάλλονται σε επεξεργασία ή όχι.
- **Πρόσβαση** σε αντίγραφο αυτών των δεδομένων.
- **Πρόσβαση σε πληροφορίες** σχετικά με την επεξεργασία, ανάλογες με αυτές που περιέχονται στις υποχρεώσεις ενημέρωσης (όπως οι σκοποί της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα κ.α.).

### 6.4.2 Αξιολόγηση του αιτήματος

Κατά την ανάλυση του περιεχομένου του αιτήματος, ο υπεύθυνος επεξεργασίας πρέπει να αξιολογήσει εάν το αίτημα αφορά προσωπικά δεδομένα του προσώπου που υποβάλλει το αίτημα, εάν το αίτημα εμπίπτει στο πεδίο εφαρμογής του άρθρου 15 και εάν υπάρχουν άλλες, πιο συγκεκριμένες, διατάξεις που ρυθμίζουν την πρόσβαση σε συγκεκριμένη κατηγορία δεδομένων. Πρέπει επίσης να αξιολογήσει εάν το αίτημα αναφέρεται σε όλα ή μόνο σε τμήματα των δεδομένων που υποβάλλονται σε επεξεργασία σχετικά με το υποκείμενο των δεδομένων.

Αν ο υπεύθυνος επεξεργασίας δεν είναι σε θέση να εντοπίσει δεδομένα που αναφέρονται στον αιτούντα, οφείλει να τον ενημερώσει σχετικά και να αρνηθεί να δώσει πρόσβαση, εκτός εάν το υποκείμενο των δεδομένων παράσχει πρόσθετες



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

πληροφορίες που επιτρέπουν την ταυτοποίησή του.

**Παράδειγμα:** Πολίτης ασκεί σε δημόσια υπηρεσία που διαθέτει σύστημα βιντεοεπιτήρησης δικαίωμα πρόσβασης. Η υπηρεσία μπορεί να αρνηθεί να δώσει πρόσβαση εκτός εάν το υποκείμενο των δεδομένων καθορίσει την ώρα και ημερομηνία κατά την οποία βρέθηκε στην εμβέλεια των καμερών. Σε κάθε όμως περίπτωση, η υπηρεσία οφείλει να απαντήσει, έστω αρνητικά.

Εάν ο υπεύθυνος επεξεργασίας έχει αμφιβολίες σχετικά με το εάν το υποκείμενο των δεδομένων είναι αυτό που ισχυρίζονται ότι είναι, ο υπεύθυνος επεξεργασίας μπορεί να ζητήσει πρόσθετες πληροφορίες για να επιβεβαιώσει την ταυτότητα του υποκειμένου των δεδομένων.

Δεν υπάρχουν συγκεκριμένες απαιτήσεις σχετικά με τη μορφή ενός αιτήματος. Είναι ορθή πρακτική για τον υπεύθυνο επεξεργασίας να παρέχει κατάλληλα και φιλικά προς το χρήστη κανάλια επικοινωνίας και ειδικές φόρμες για την υποβολή των αιτημάτων άσκησης δικαιώματος πρόσβασης. Ωστόσο, το υποκείμενο των δεδομένων δεν απαιτείται να χρησιμοποιήσει αυτά τα συγκεκριμένα κανάλια και μπορεί να στείλει το αίτημα σε οποιοδήποτε επίσημο σημείο επαφής. Ο υπεύθυνος θα πρέπει να είναι σε θέση να αξιολογήσει το αίτημα ως δικαίωμα πρόσβασης.

### 6.4.3 Πεδίο εφαρμογής του δικαιώματος πρόσβασης

Το εύρος του δικαιώματος πρόσβασης καθορίζεται από το εύρος της έννοιας των προσωπικών δεδομένων. Συνεπώς, ένα δικαίωμα πρόσβασης αναφέρεται σε όλα τα προσωπικά δεδομένα που αφορούν το άτομο που υποβάλλει το αίτημα και μπορεί να περιλαμβάνει δεδομένα που θα μπορούσαν επίσης να αφορούν άλλα άτομα, για παράδειγμα ιστορικό επικοινωνίας που περιλαμβάνει εισερχόμενα και εξερχόμενα μηνύματα (βλ. συναφώς την ενότητα 6.4.5 για περιορισμούς σε αυτήν την περίπτωση).

Εκτός από την παροχή πρόσβασης στα προσωπικά δεδομένα, ο υπεύθυνος επεξεργασίας πρέπει να παρέχει πρόσθετες πληροφορίες σχετικά με την επεξεργασία και τα δικαιώματα των υποκειμένων των δεδομένων. Οι πληροφορίες αυτές μπορούν



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

να βασίζονται στην πολιτική προστασίας δεδομένων του υπεύθυνου επεξεργασίας με βάση τα άρθρα 13 και 14, καθώς κατά βάση είναι παρόμοιες. Ωστόσο, οι πληροφορίες θα πρέπει να προσαρμόζονται ώστε να αντιστοιχούν στις δραστηριότητες επεξεργασίας τις οποίες αφορά το αίτημα.

### 6.4.4 Τρόπος παροχής πρόσβασης

Εκτός εάν αναφέρεται ρητά το αντίθετο, ένα αίτημα δικαιώματος πρόσβασης θα πρέπει να θεωρείται ότι αναφέρεται σε όλα τα προσωπικά δεδομένα που αφορούν το υποκείμενο των δεδομένων. Ο υπεύθυνος επεξεργασίας, εφόσον τηρεί μεγάλο όγκο δεδομένων, μπορεί να ζητήσει από το υποκείμενο των δεδομένων να προσδιορίσει το αίτημα.

Ο υπεύθυνος επεξεργασίας θα πρέπει να αναζητήσει προσωπικά δεδομένα σε όλα τα πληροφοριακά συστήματα ή άλλα συστήματα αρχειοθέτησης με βάση κριτήρια αναζήτησης που αντικατοπτρίζουν τον τρόπο με τον οποίο είναι δομημένες οι πληροφορίες, για παράδειγμα όνομα και αριθμός πελάτη. Αφού εντοπιστούν, τα δεδομένα και οι πληροφορίες πρέπει να παρασχεθούν σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, με χρήση σαφούς και απλής γλώσσας. Εάν τα δεδομένα αποτελούνται από κωδικούς ή άλλα «ακατέργαστα δεδομένα», αυτά μπορεί να πρέπει να εξηγηθούν προκειμένου να είναι κατανοητά από το υποκείμενο των δεδομένων.

Ο βασικός τρόπος ικανοποίησης του δικαιώματος πρόσβασης είναι να παρέχεται στο υποκείμενο των δεδομένων αντίγραφο των δεδομένων του. Μπορούν όμως να προβλεφθούν άλλοι εναλλακτικοί τρόποι (όπως προφορικές πληροφορίες και επιτόπια πρόσβαση) εάν το ζητήσει το υποκείμενο των δεδομένων. Τα δεδομένα μπορούν να παρέχονται με ηλεκτρονικό τρόπο (με κατάλληλα μέτρα ασφάλειας) ή με άλλους αυτόματους τρόπους, όμως για παράδειγμα με εργαλείο αυτόματης εξαγωγής δεδομένων.

Όταν ο όγκος των δεδομένων είναι πολύ μεγάλος και θα ήταν δύσκολο για το υποκείμενο των δεδομένων να κατανοήσει τις πληροφορίες, μπορεί να ακολουθείται πολυεπίπεδη προσέγγιση. Το αντίγραφο των δεδομένων και οι πρόσθετες πληροφορίες θα πρέπει να παρέχονται σε γραπτή μορφή, όπως σε γραπτό κείμενο ή σε ηλεκτρονική μορφή με γνωστό μορφότυπο αρχείου.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Η αξιολόγηση του αιτήματος πρέπει να αντικατοπτρίζει την κατάσταση τη στιγμή που το αίτημα ελήφθη από τον υπεύθυνο επεξεργασίας. Πρέπει να παρέχονται ακόμη και δεδομένα που ενδέχεται να είναι εσφαλμένα ή υποβάλλονται σε παράνομη επεξεργασία. Αν όμως τα δεδομένα έχουν ήδη διαγραφεί, για παράδειγμα επειδή έχει λήξει ο χρόνος τήρησης, δεν χρειάζεται να παρέχονται και ο υπεύθυνος επεξεργασίας οφείλει να απαντήσει αρνητικά.

### 6.4.5 Περιορισμός του δικαιώματος

Ο ΓΚΠΔ στο άρθρο 15 παρ. 4 επιτρέπει περιορισμό του δικαιώματος πρόσβασης. Συγκεκριμένα, το δικαίωμα λήψης αντιγράφου δεν επηρεάζει αρνητικά τα δικαιώματα και τις ελευθερίες άλλων. Για την εφαρμογή της εξαίρεσης αυτής, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι τα δικαιώματα ή οι ελευθερίες άλλων θα επηρεάζονταν αρνητικά στη συγκεκριμένη κατάσταση. Ακόμα κι έτσι, η εφαρμογή της εξαίρεσης, πρέπει να έχει ως αποτέλεσμα να παραλείπονται εκείνα τα τμήματα των δεδομένων που ενδέχεται να έχουν αρνητικές επιπτώσεις για τα δικαιώματα και τις ελευθερίες άλλων.

**Παράδειγμα:** Πολίτης υποβάλλει σε δημόσια υπηρεσία καταγγελία. Ο καταγγελλόμενος ασκεί στη δημόσια υπηρεσία δικαίωμα πρόσβασης ώστε να λάβει γνώση, μεταξύ άλλων, και για την πηγή των δεδομένων, ήτοι τα στοιχεία του καταγγέλλοντα. Ακόμα και αν η δημόσια υπηρεσία δεν διαθέτει ειδική διάταξη για την απόκρυψη των στοιχείων του καταγγέλλοντα, μπορεί να αξιολογήσει –και να καταγράψει- εάν από την αποκάλυψη των στοιχείων του καταγγέλλοντα ενδέχεται να επηρεαστούν δυσμενώς τα δικαιώματα και οι ελευθερίες του καταγγέλλοντα (για το εν λόγω ζήτημα, βλ. συναφώς και την Ενότητα 14).

## 6.5 Δικαίωμα διόρθωσης

Το δικαίωμα διόρθωσης (άρθρο 16 του ΓΚΠΔ) αφορά το δικαίωμα που έχει το υποκείμενο των δεδομένων να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών πληροφοριών που το αφορούν ή, ανάλογα και του σκοπού της επεξεργασίας, τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

άλλων μέσω συμπληρωματικής δήλωσης. Όπως και στις άλλες περιπτώσεις, ο υπεύθυνος επεξεργασίας οφείλει να ανταποκρίνεται χωρίς αδικαιολόγητη καθυστέρηση (σύμφωνα και με τα οριζόμενα στο άρθρο 12 του ΓΚΠΔ).

Τα δεδομένα χαρακτηρίζονται ως ελλιπή όταν, εκ της απουσίας τους σε συγκεκριμένο πλαίσιο επεξεργασίας, δύναται να προκύψει παραπλάνηση ή παρεξήγηση.

**Παράδειγμα:** Πολίτης ζητά ληξιαρχική πράξη γέννησης και διαπιστώνει ανακριβή στοιχεία – π.χ. στην πόλη γέννησης ή στην ημερομηνία γέννησης. Το αίτημά του για διόρθωση των εν λόγω στοιχείων συνιστά άσκηση του, κατά του άρθρο 16 του ΓΚΠΔ, δικαιώματος διόρθωσης, οπότε ο Δήμος, ως υπεύθυνος επεξεργασίας, θα πρέπει να προβεί χωρίς καθυστέρηση (και το αργότερο εντός 30 ημερών) στις απαραίτητες ενέργειες για την εξέταση του αιτήματος και, εφόσον πράγματι τα στοιχεία δεν ήταν ακριβή, στη διόρθωσή τους.

## 6.6 Δικαίωμα διαγραφής

Τα υποκείμενα των δεδομένων μπορούν να ζητούν τη διαγραφή των δεδομένων τους, σύμφωνα με το άρθρο 17 του ΓΚΠΔ. Η ικανοποίηση του εν λόγω δικαιώματος είναι υποχρεωτική υπό συγκεκριμένες προϋποθέσεις. Ειδικότερα, σύμφωνα με το άρθρο 17 παρ. 1, ο υπεύθυνος επεξεργασίας πρέπει να προχωρεί στη διαγραφή των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση στις εξής περιπτώσεις:

α) Τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

β) Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία, όταν αυτή βασίζεται στη συγκατάθεσή του και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

γ) Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παρ. 1 και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παρ. 2 (για τις προβλέψεις του άρθρου 21 παρ. 1 θα αναφερθούμε στην Ενότητα 6.9).

δ) Τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα.

ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.

στ) Τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών που αναφέρονται στο άρθρο 8 παρ. 1 του ΓΚΠΔ, δηλαδή σε σχέση με υπηρεσίες που απευθύνονται σε παιδιά (βλ. και Ενότητα 5.7).

**Παράδειγμα:** Ουσιαστικά, για περιπτώσεις επεξεργασιών που διενεργεί δημόσιος φορέας, οι πλέον τυπικές περιπτώσεις που έχει εφαρμογή το δικαίωμα διαγραφής είναι οι εξής:
α) Ανάκληση συγκατάθεσης, εφόσον είναι η μόνη νομική βάση για την επεξεργασία (π.χ. πολίτης έχει εγγραφεί, με την ηλεκτρονική του διεύθυνση, στην ιστοσελίδα φορέα προκειμένου να λαμβάνει ενημερωτικά δελτία (newsletters) και επιθυμεί να σταματήσει να λαμβάνει – οπότε και θα πρέπει να διαγραφεί η συγκεκριμένη διεύθυνση από τις λίστες παραληπτών των ενημερωτικών δελτίων).
β) Η επεξεργασία είναι παράνομη (π.χ. ανάρτηση δεδομένων υγείας στη ΔΙΑΥΓΕΙΑ, κατά παράβαση των όσων ορίζονται στις σχετικές διατάξεις για τη ΔΙΑΥΓΕΙΑ, οπότε και θα πρέπει να γίνει απανάρτησή τους ή υπάρχει νομική υποχρέωση για διαγραφή δεδομένων μετά την πάροδο συγκεκριμένου χρονικού διαστήματος και τα δεδομένα, αν και έχει παρέλθει το διάστημα, δεν έχουν διαγραφεί: για παράδειγμα, αναφορικά με τα δεδομένα υγείας που τηρεί νοσοκομείο, το χρονικό διάστημα τήρησης των



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

δεδομένων υγείας ρυθμίζεται από νόμο[18]).

Θα πρέπει να σημειωθεί ωστόσο ότι το δικαίωμα διαγραφής δεν είναι ένα «απόλυτο» δικαίωμα καθώς η περαιτέρω τήρηση των δεδομένων, παρά την άσκηση του δικαιώματος, μπορεί να είναι επιτρεπτή εφόσον συντρέχουν προϋποθέσεις. Ειδικότερα, το δικαίωμα διαγραφής δεν εφαρμόζεται εφόσον η επεξεργασία είναι απαραίτητη για (βλ. άρθρο 17 παρ. 3):

1. για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση,
2. για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας (σσ. ουσιαστικά, εδώ η ανάγκη τήρησης των δεδομένων τελικά προκύπτει από διάταξη νόμου),
3. για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας σύμφωνα με το άρθρο 9 παρ. 2 στοιχεία η) και θ), καθώς και το άρθρο 9 παρ. 3 (βλ. Ενότητα 5),
4. για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, εφόσον το δικαίωμα διαγραφής είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της εν λόγω επεξεργασίας (βλ. σχετικά Ενότητα 14), ή
5. για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

☞ Ουσιαστικά, για επεξεργασία προσωπικών δεδομένων που διενεργεί δημόσιος φορέας και η νομική βάση αυτής είναι είτε η έννομη υποχρέωση (άρθρο 6 παρ. 1 στοιχ. γ') είτε η εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας (δηλαδή, για τις τυπικές περιπτώσεις επεξεργασιών που διενεργεί δημόσιος φορέας), και

[18] Ειδικότερα, σύμφωνα με το ν. 3418/2005, τα εν λόγω δεδομένα τηρούνται για μια εικοσαετία από την τελευταία επαφή (επίσκεψη ή νοσηλεία) του προσώπου με το Νοσοκομείο



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εφόσον βέβαια η επεξεργασία γίνεται με σύννομο και θεμιτό τρόπο και τα δεδομένα τηρούνται για όσο χρόνο είναι απαραίτητο εν όψει των σκοπών αυτών, τότε το δικαίωμα διαγραφής δεν ικανοποιείται.

☞ Αντίστοιχες προβλέψεις για – υπό προϋποθέσεις - μη ικανοποίηση δικαιώματος υπάρχουν και περιπτώσεις επεξεργασίας για ερευνητικούς ή στατιστικούς σκοπούς (βλ. αναλυτικότερα την Ενότητα 14).

Το δικαίωμα διαγραφής είναι γνωστό και ως «δικαίωμα στη λήθη» (right to be forgotten). Πιθανώς ο λόγος που χρησιμοποιείται αυτός ο όρος είναι ότι το εν λόγω δικαίωμα είναι σαφώς «ενισχυμένο» σε σχέση με το αντίστοιχο δικαίωμα που προέβλεπε η προηγούμενη Οδηγία 95/46/ΕΚ. Γιατί «ενισχυμένο»; Διότι όταν ο υπεύθυνος επεξεργασίας οφείλει να το ικανοποιήσει σύμφωνα με τα οριζόμενα ανωτέρω, έχει επιπροσθέτως και μία άλλη υποχρέωση: εφόσον έχει δημοσιοποιήσει τα εν λόγω δεδομένα, τότε πρέπει να προβεί σε όλες τις απαραίτητες ενέργειες ώστε, όλοι οι λοιποί υπεύθυνοι επεξεργασίας που τα έχουν λάβει ή αναδημοσιεύσει, να ενημερωθούν σχετικά, ώστε να φροντίσουν να μην τα επεξεργάζονται. Ειδικότερα, η παρ. 2 του άρθρου 17 αναφέρει την εξής υποχρέωση:

«*Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και υποχρεούται σύμφωνα με την παράγραφο 1 να διαγράψει τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα*».

Το πνεύμα της εν λόγω διάταξης έγκειται στο ότι, λόγω των κινδύνων σε επιγραμμικά (online) περιβάλλοντα, όπου για παράδειγμα μία ανάρτηση στο Διαδίκτυο μπορεί μέσα σε πολύ λίγα λεπτά να αναπαραχθεί από άλλες ιστοσελίδες/ιστολόγια, χρειάζονται πρόσθετα μέτρα για την διασφάλιση των δικαιωμάτων και ελευθεριών



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

των προσώπων. Συνεπώς, ο ΓΚΠΔ αναθέτει αυτήν την νέα υποχρέωση στον υπεύθυνο επεξεργασίας. Μάλιστα, δεν χρειάζεται αυτό να ζητηθεί ειδικώς από το υποκείμενο των δεδομένων (δηλαδή δεν χρειάζεται το υποκείμενο των δεδομένων να ζητήσει ειδικώς από τον υπεύθυνο επεξεργασίας να προβεί στις δέουσες ενέργειες για να πάψει η αναπαραγωγή/επεξεργασία των δεδομένων του και από άλλους υπεύθυνους επεξεργασίας): η εν λόγω υποχρέωση για τον υπεύθυνο επεξεργασίας προκύπτει αυτομάτως σε κάθε άσκηση δικαιώματος διαγραφής του υποκειμένου των δεδομένων.

**Παράδειγμα:** Πανεπιστήμιο αναρτά αποτελέσματα κατατακτηρίων εξετάσεων, με τα στοιχεία επιτυχόντων. Εκ παραδρομής, δημοσιεύει και στοιχεία αποτυχόντων. Εφόσον ασκηθεί δικαίωμα διαγραφής από υποκείμενο των δεδομένων ως προς τους αποτυχόντες, το Πανεπιστήμιο δεν αρκεί, προς ικανοποίηση του δικαιώματος, απλά να διαγράψει (απαναρτήσει) τον εν λόγω κατάλογο: εφόσον γνωρίζει ότι γνωστά ιστολόγια στον εκπαιδευτικό χώρο έχουν ήδη αναπαράγει τη λίστα, οφείλει να λάβει κατάλληλα μέτρα για να τα ενημερώσει ότι πρέπει με τη σειρά τους να διαγράψουν τις εν λόγω αναρτήσεις.

- Η εν λόγω υποχρέωση «διάχυσης» της πληροφορίας ότι τα δεδομένα πρέπει να διαγραφούν από παντού δεν είναι «απόλυτη» - ο ΓΚΠΔ εξάλλου ρητά αναφέρει ότι οι σχετικές ενέργειες του υπευθύνου επεξεργασίας γίνονται *λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής*. Για παράδειγμα, μπορεί τα προς διαγραφή προσωπικά δεδομένα να έχουν αναπαραχθεί από τόσους πολλούς ιστότοπους που να μην είναι πρακτικά εφικτό να εντοπιστούν όλοι. Επίσης, δεν πρέπει να ξεχνάμε ότι ακόμα και αν ο υπεύθυνος επεξεργασίας ενημερώσει έναν άλλον υπεύθυνο επεξεργασίας ως προς το ότι πρέπει να διαγράψει δεδομένα, τυχόν άρνηση του τελευταίου – κατά παράβαση του ΓΚΠΔ – να το πράξει δεν είναι κάτι που βαρύνει ως ευθύνη τον αρχικό υπεύθυνο επεξεργασίας. Ανάλογα τις περιστάσεις, η υποχρέωση αυτή μπορεί να ερμηνεύεται διαφορετικά, όπως για παράδειγμα ως υποχρέωση επισήμανσης στην αρχική ιστοσελίδα του αρχικού λάθους και



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

της υποχρέωσης όσων χρησιμοποίησαν τα δεδομένα να τα διαγράψουν.

☞ Ωστόσο, ανακαλώντας και την αρχή της λογοδοσίας, ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να αποδεικνύει ότι προέβη σε όλες τις δέουσες ενέργειες για τη συμμόρφωσή του με την υποχρέωση αυτή, παρά το γεγονός δεν είναι «απόλυτη» υπό την έννοια που περιγράφηκε.

Προσοχή: Ο όρος «δικαίωμα στη λήθη» χρησιμοποιείται ευρέως για την περίπτωση όπου πολίτες επιθυμούν διαγραφή αποτελεσμάτων μηχανών αναζήτησης (search engines) που τους αφορούν. Ειδικότερα, ο όρος χρησιμοποιείται για την εξής περίπτωση: Έστω ότι για πολίτη Α εμφανίζονται στοιχεία του σε μία ιστοσελίδα Ι. Λόγω αυτού, οποιοσδήποτε χρήστης του διαδικτύου που αξιοποιεί μία μηχανή αναζήτησης Μ αναζητώντας πληροφορίες για τον Α, θα «ανακαλύπτει» την ιστοσελίδα Ι που θα «επιστρέφεται» ως αποτέλεσμα αναζήτησης για τον Α. Ο χρήστης Α μπορεί να ζητήσει από την μηχανή αναζήτησης Μ να μην εμφανίζεται, ως αποτέλεσμα αναζήτησης, η ιστοσελίδα Ι που τον αφορά – όποιος και αν κάνει την αναζήτηση. Η μηχανή αναζήτησης οφείλει να εξετάζει τέτοια αιτήματα και είτε να τα ικανοποιεί είτε να τεκμηριώνει τους λόγους που δεν μπορεί να τα ικανοποιήσει[19]. Το ΕΣΠΔ έχει εκδώσει ειδικώς προς τούτο Κατευθυντήριες Γραμμές (5/2019) σχετικά με τα κριτήρια που διέπουν το δικαίωμα στη λήθη, σύμφωνα με τον ΓΚΠΔ, στις περιπτώσεις μηχανών αναζήτησης. Η εν λόγω περίπτωση όμως αφορά μόνο μη εμφάνιση αποτελεσμάτων από μηχανή αναζήτησης και όχι διαγραφή των δεδομένων που βρίσκονται στις αρχικές ιστοσελίδες (μπορεί να εξακολουθούν να παραμένουν εκεί, ειδικά αν ο πολίτης επιλέξει να μην απευθυνθεί στην ιστοσελίδα αλλά στη μηχανή αναζήτησης, όπως έχει ευχέρεια να πράξει). Σε κάθε περίπτωση, οι εν λόγω Κατευθυντήριες Γραμμές (5/2019) του ΕΣΠΔ δεν αφορούν περιπτώσεις άσκησης δικαιώματος διαγραφής τις οποίες θα κληθεί να εξετάσει δημόσιος φορέας.

## 6.7 Δικαίωμα περιορισμού της επεξεργασίας

[19] Βλ. ΔΕΕ, Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos, Mario Costeja González, 14.5.2014



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Τα υποκείμενα των δεδομένων μπορούν επίσης να ζητούν τον περιορισμό («κλείδωμα») της επεξεργασίας, σύμφωνα με το άρθρο 18 του ΓΚΠΔ. Η άσκηση του δικαιώματος αυτού δεν θα πρέπει να συγχέεται με την άσκηση του δικαιώματος διαγραφής: δεν ζητείται διαγραφή των δεδομένων αλλά να σταματήσει η διενέργεια κάποιας συγκεκριμένης πτυχής της επεξεργασίας (αφού θα εξακολουθεί να πραγματοποιείται τήρηση των δεδομένων) – για παράδειγμα, σε ένα αυτοματοποιημένο σύστημα αρχειοθέτησης, το υποκείμενο των δεδομένων μπορεί να αιτηθεί τα δεδομένα του να μην υπόκεινται σε πράξη περαιτέρω επεξεργασίας (π.χ. σε προσβάσεις ή διαβιβάσεις) και να μην μπορούν να αλλάξουν (βλ. αιτιολογική σκέψη 67 του ΓΚΠΔ). Σημειώνεται ότι το άρθρο 4 στοιχ. 3 του ΓΚΠΔ ορίζει ως περιορισμό της επεξεργασίας *την επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον («κλείδωμα»).*

Το υποκείμενο των δεδομένων δικαιούται να διασφαλίζει τον περιορισμό της επεξεργασίας, όταν ισχύει ένα εκ των ακόλουθων:

α) η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα.

**Παράδειγμα:** Μαζί με την άσκηση δικαιώματος διόρθωσης λόγω ανακριβών στοιχείων, ο πολίτης μπορεί να ζητήσει – αναλόγως την περίπτωση – να μη ληφθούν καθόλου υπόψη τα ανακριβή του στοιχεία από έναν φορέα (π.χ. να μην εκδοθεί κάποια ατομική πράξη, η οποία εξαρτάται από τα στοιχεία αυτά) μέχρι να διορθωθούν τα στοιχεία του.

β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους

**Παράδειγμα:** Πολίτης ο οποίος έχει αντιληφθεί ότι φορέας έχει παράνομα τα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

στοιχεία του, μπορεί να ζητήσει περιορισμό της επεξεργασίας (να μη γίνει καμία περαιτέρω χρήση τους) αντί διαγραφής, επειδή π.χ. θέλει να υποβάλει καταγγελία για την παράνομη επεξεργασία και χρειάζεται να υπάρχουν διαθέσιμα τα στοιχεία του που υπέστησαν παράνομη τήρηση και περαιτέρω επεξεργασία για τη διερεύνηση της καταγγελίας αυτής.

γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

**Παράδειγμα:** Πολίτης θα χρειαστεί υλικό συστήματος βιντεοεπιτήρησης εγκατεστημένου σε φορέα (π.χ. βρέθηκε «χτυπημένο» το αυτοκίνητό του στο χώρο στάθμευσης του φορέα). Δεδομένου ότι ο φορέας οφείλει να διαγράφει τα δεδομένα συστήματος βιντεοεπιτήρησης εφόσον δεν τα χρειάζεται για τους δικούς του σκοπούς (βλ. Ενότητα 14), ο πολίτης μπορεί να ζητήσει να μη διαγραφούν επειδή θα τα χρειαστεί.

δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων (για τις προβλέψεις του άρθρου 21 παρ. 1 θα αναφερθούμε στην Ενότητα 6.9).

Σύμφωνα με το άρθρο 18 παρ. 2, όταν η επεξεργασία έχει περιοριστεί λόγω άσκησης σχετικού δικαιώματος περιορισμού, τότε τα εν λόγω δεδομένα προσωπικού χαρακτήρα, υφίστανται επεξεργασία - πέραν της τήρησής τους - μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

☞ Εφόσον πρόκειται να αρθεί περιορισμός επεξεργασίας, ο οποίος περιορισμός έλαβε χώρα κατόπιν άσκησης του σχετικού δικαιώματος, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει σχετικά το υποκείμενο των δεδομένων (άρ 18 παρ. 3 του ΓΚΠΔ).

## 6.8 Δικαίωμα στη φορητότητα των δεδομένων

Το δικαίωμα στη φορητότητα των δεδομένων που εισάγει ο ΓΚΠΔ στο άρθρο 20 είναι ένα τελείως νέο δικαίωμα, σε σχέση με το προηγούμενο νομικό πλαίσιο (95/46/ΕΚ). Είναι ένα δικαίωμα προσανατολισμένο στο να διευκολύνονται τα φυσικά πρόσωπα στο να μπορούν να λάβουν τα δεδομένα τους, εφόσον το επιθυμούν, με συγκεκριμένο και κατάλληλο μορφότυπο (format) προκειμένου να μπορούν να μεταφερθούν ευχερώς σε άλλον υπεύθυνο επεξεργασίας έτσι ώστε να είναι άμεσα διαχειρίσιμα από αυτόν (προς όφελος του υποκειμένου των δεδομένων) κατ' ανάλογο τρόπο. Ουσιαστικά, με το εν λόγω δικαίωμα τα υποκείμενα των δεδομένων αποκτούν μεγαλύτερο έλεγχο επ' αυτών.

Συγκεκριμένα, σύμφωνα με το άρθρο 20 παρ. 1 του ΓΚΠΔ, «*το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα (...)*». Ουσιαστικά, όπως αναφέρει και το ΕΣΠΔ στις σχετικές κατευθυντήριες γραμμές που υιοθέτησε από την Ομάδα Εργασίας του Άρθρου 29 [42] το δικαίωμα στη φορητότητα των δεδομένων έχει ως στόχο να προσφέρει περισσότερες δυνατότητες στους χρήστες σε σχέση με τα δεδομένα προσωπικού χαρακτήρα τους, καθώς διευκολύνει την ικανότητά τους να διακινούν, να αντιγράφουν ή να διαβιβάζουν εύκολα δεδομένα προσωπικού χαρακτήρα από ένα υπολογιστικό σύστημα σε άλλο (στα δικά τους συστήματα, σε συστήματα έμπιστων τρίτων ή στα συστήματα νέων υπευθύνων επεξεργασίας).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Μάλιστα, στην παράγραφο 2 του ιδίου άρθρου το δικαίωμα αυτό κατά μία έννοια ενισχύεται, αφού, όπως αναφέρεται εκεί, «*κατά την άσκηση του δικαιώματος στη φορητότητα των δεδομένων (...), το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό*». Άρα, το εν λόγω δικαίωμα ενέχει τόσο την έννοια της λήψης των δεδομένων από το υποκείμενο αυτών (οπότε και κατά μία έννοια συμπληρώνει το δικαίωμα πρόσβασης), όσο και την έννοια της διαβίβασης σε άλλον υπεύθυνο επεξεργασίας (η οποία διαβίβαση, εφόσον το επιθυμεί το υποκείμενο των δεδομένων, θα πρέπει να είναι εφικτό να γίνει απευθείας μεταξύ των δύο υπευθύνων επεξεργασίας, χωρίς να μεσολαβήσει το υποκείμενο των δεδομένων).

☞ Είναι κρίσιμο να αναφερθεί ότι το δικαίωμα φορητότητας υφίσταται για δεδομένα τα οποία τα έχει παράσχει το ίδιο το υποκείμενο αυτών. Αν ένας υπεύθυνος επεξεργασίας έχει δεδομένα που δεν τα παρείχε το ίδιο το υποκείμενο (π.χ. αν χρηματοπιστωτικό ίδρυμα έχει δημιουργήσει προφίλ πελάτη ως καλού ή κακού δανειολήπτη), τότε το δικαίωμα φορητότητας δεν υφίσταται για τα δεδομένα αυτά.

**Παράδειγμα (βασισμένο σε παράδειγμα από το** [42]): Ένας χρήστης υπηρεσίας μουσικής συνεχούς ροής (music streaming) μπορεί να ασκήσει το δικαίωμα προκειμένου να ανακτήσει τη λίστα των τραγουδιών (playlist) που άκουσε το τελευταίο διάστημα. Ενδεχομένως μάλιστα να θέλει αυτή η λίστα να διαβιβαστεί σε άλλη συναφή υπηρεσία, και να είναι εκεί αυτομάτως λειτουργική (δηλαδή, συνδεόμενος στη νέα υπηρεσία, να εμφανίζεται εκεί όπως εάν ήταν ήδη χρήσης που είχε ήδη ακούσει τα τραγούδια). Περαιτέρω, στη δεύτερη αυτή περίπτωση, η πρώτη υπηρεσία (αρχικός υπεύθυνος επεξεργασίας) πρέπει να είναι σε θέση, εάν το ζητήσει ο χρήστης, να τα διαβιβάσει απευθείας στη δεύτερη υπηρεσία (νέος υπεύθυνος



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επεξεργασίας), σε κατάλληλο μορφότυπο για να μπορεί η δεύτερη να τα διαχειριστεί κατάλληλα, με βάση την επιθυμία του χρήστη.

Το ανωτέρω παράδειγμα σαφώς εκφεύγει των εφαρμογών του Δημοσίου Τομέα. Υπάρχουν περιπτώσεις που το δικαίωμα φορητότητας έχει εφαρμογή στο Δημόσιο Τομέα; Εδώ πρέπει να επισημάνουμε ότι το δικαίωμα φορητότητας υφίσταται, σύμφωνα πάντα με την παρ. 1 του άρθρου 20, μόνο όταν ισχύει ένα από τα εξής:
α) η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παρ. 1 στοιχ. α' ή το άρθρο 9 παρ. 2 στοιχ. α' ή σε σύμβαση σύμφωνα με το άρθρο 6 παρ. 1 στοιχείο β' και
β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

Συνεπώς, το δικαίωμα φορητότητας μπορεί να ισχύει μόνο εφόσον, πέραν του ότι η επεξεργασία πρέπει να είναι αυτοματοποιημένη, η νομική βάση αυτής είναι η συγκατάθεση είτε η εκτέλεση σύμβασης. Όπως είδαμε και στην Ενότητα 5, οι εν λόγω νομικές βάσεις δεν είναι από τις συνήθεις που συναντώνται σε επεξεργασίες που διενεργεί Δημόσιος φορέας. Μάλιστα, ρητώς αναφέρεται στην παρ. 3 του ιδίου άρθρου ότι το εν λόγω δικαίωμα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Ως εκ τούτου, μάλλον σπανίως αναμένεται να έχει εφαρμογή το εν λόγω δικαίωμα σε δημόσιο φορέα.

☞ Όπως επισημαίνεται στο [42], το άρθρο 20 παρ. 3 αλλά και η Αιτιολογική Σκέψη 68 ορίζουν ότι η φορητότητα των δεδομένων δεν ισχύει όταν η επεξεργασία των δεδομένων είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, ή κατά την άσκηση των δημόσιων καθηκόντων ή τη συμμόρφωση με νομική υποχρέωση του υπευθύνου επεξεργασίας. Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας δεν υποχρεούνται να παρέχουν φορητότητα σε αυτές τις περιπτώσεις. Ωστόσο, αποτελεί ορθή πρακτική η ανάπτυξη διαδικασιών για αυτόματη (αρνητική) απάντηση σε αιτήματα φορητότητας,



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σύμφωνα με τις αρχές που διέπουν το δικαίωμα στη φορητότητα των δεδομένων, ενώ κατάλληλη ενημέρωση πρέπει να παρέχεται και με βάση τα άρθρα 13 και 14, ώστε να γνωρίζουν τα υποκείμενα των δεδομένων ότι δεν εφαρμόζεται το εν λόγω δικαίωμα.

## 6.9 Δικαίωμα εναντίωσης

Όταν δεδομένα προσωπικού χαρακτήρα μπορούν να υποβληθούν νόμιμα σε επεξεργασία επειδή η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας ή για λόγους έννομων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου μέρους, κάθε υποκείμενο των δεδομένων θα πρέπει να δικαιούται παρ' όλα αυτά να αντιταχθεί στην επεξεργασία τυχόν δεδομένων προσωπικού χαρακτήρα που αφορούν την ιδιαίτερη κατάστασή του (Αιτιολογική Σκέψη 69 του ΓΚΠΔ). Το εν λόγω δικαίωμα συνιστά το λεγόμενο δικαίωμα εναντίωσης που προβλέπεται στο άρθρο 21 του ΓΚΠΔ, το οποίο με το παλαιότερο θεσμικό πλαίσιο (ν. 2472/1997) ήταν επίσης γνωστό ως δικαίωμα αντίρρησης ή αντίταξης, ορολογία που απαντάνται στο ν. 3471/2006. Ειδικότερα, σύμφωνα με το άρθρο 21 παρ. 1:

«*Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο ε) ή στ), περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων*».

☞ Το δικαίωμα εναντίωσης για επεξεργασία που διενεργεί δημόσιος φορέας ως υπεύθυνος επεξεργασίας υφίσταται – κατά την έννοια που περιγράφηκε ανωτέρω



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- μόνο στην περίπτωση κατά την οποία η νομική βάση για την επεξεργασία είναι η εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (άρθρο 6, παρ. 1, στοιχ. ε΄).

Άρα, όταν ασκείται δικαίωμα εναντίωσης ο υπεύθυνος επεξεργασίας θα πρέπει να σταματά την επεξεργασία, εκτός εάν μπορεί να αποδείξει ότι υπάρχουν επιτακτικοί και νόμιμοι λόγοι που επιβάλλουν τη συνέχισή της και οι οποίοι υπερισχύουν των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων. Η ιδιαίτερη κατάσταση ενός ατόμου μπορεί να σχετίζεται π.χ. με οικογενειακές καταστάσεις ανάγκης, με νομικές ανάγκες κ.α.

Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει ρητώς για την ύπαρξη του εν λόγω δικαιώματος, το οποίο και πρέπει να περιγράφεται με σαφήνεια και χωριστά από οποιαδήποτε άλλη πληροφορία. Η ενημέρωση αυτή πρέπει να γίνεται το αργότερο κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων (άρ. 21 παρ. 4 του ΓΚΠΔ). Ειδικές προβλέψεις υπάρχουν επίσης στην εν λόγω διάταξη για την περίπτωση επεξεργασίας για σκοπούς εμπορικής προώθησης (βλ. παρ. 2 και 3 του άρθρου 21) – όπου, ουσιαστικά, για τους σκοπούς αυτούς, το δικαίωμα πρέπει να ικανοποιείται πάντα[20].

Τέλος, ειδική πρόβλεψη για το δικαίωμα εναντίωσης υπάρχει στην παρ. 6 του εν λόγω άρθρου, για την περίπτωση επεξεργασίας για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς. Ουσιαστικά, για τους εν λόγω σκοπούς το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί, για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν, με εξαίρεση την περίπτωση κατά την οποία η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος. Περισσότερες πληροφορίες για την επεξεργασία προσωπικών δεδομένων για αυτούς τους σκοπούς υπάρχουν στην Ενότητα 14 (όπου,

[20] Αυτό ισχύει για περίπτωση, π.χ., προωθητικών ενεργειών μέσω συμβατικού ταχυδρομείου. Για άλλες περιπτώσεις ωστόσο προωθητικών ενεργειών υπάρχει ειδικότερη νομοθεσία που, ως ειδικότερη, κατισχύει (lex specialis), αν και η λογική της είναι παρόμοια – βλ. Ενότητα 13 στη συνέχεια.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

όπως θα δούμε, για τους εν λόγω σκοπούς δύναται να υπάρχουν περιορισμοί στα δικαιώματα, συμπεριλαμβανομένου και του δικαιώματος εναντίωσης).

## 6.10 Αυτοματοποιημένη ατομική λήψη αποφάσεων - κατάρτιση προφίλ

Η τεχνολογική πρόοδος, πέρα από τα προφανή και αδιαμφισβήτητα οφέλη της σε διάφορους κρίσιμους τομείς (υγεία, έρευνα, επικοινωνίες κτλ.), έχει ταυτόχρονα αυξήσει και τους κινδύνους από τη σκοπιά της ιδιωτικότητας. Για παράδειγμα, υπάρχουν πλέον εργαλεία και τεχνικές που μπορούν να αξιοποιήσουν αποτελεσματικά την πληθώρα προσωπικών πληροφοριών που είναι πια ευχερώς (και απλόχερα) διαθέσιμες, προκειμένου να γίνουν επεξεργασίες «ερήμην» των χρηστών για διάφορους σκοπούς: ίσως ένα από τα πιο χαρακτηριστικά «διάσημα» παραδείγματα είναι η περίπτωση της εταιρείας ανάλυσης δεδομένων Cambridge Analytica, η οποία συγκεντρώνοντας πληροφορίες χρηστών του Facebook ερήμην τους, δημιούργησε προφίλ τους βάσει των οποίων, ακολούθως, φέρεται να υπήρξε πολιτική χειραγώγησή τους [43].

Ειδικότερα, τεχνολογίες όπως μηχανικής μάθησης (machine learning), ανάλυσης μαζικών δεδομένων (big data analysis) και ευρύτερες τεχνολογίες τεχνητής νοημοσύνης[21] (artificial intelligence) επιτρέπουν πλέον όχι μόνο τη δημιουργία προφίλ ατόμων με ακρίβεια, αλλά και τη λήψη αυτοματοποιημένων (δηλαδή χωρίς παρέμβαση ανθρώπινου παράγοντα) αποφάσεων. Όπως επισημαίνεται και στις σχετικές κατευθυντήριες γραμμές της Ομάδας Εργασίας του Άρθρου 29 που έχει εγκρίνει το ΕΣΠΔ [44], *η κατάρτιση προφίλ και η αυτοματοποιημένη ατομική λήψη αποφάσεων χρησιμοποιούνται σε αυξανόμενο αριθμό τομέων, ιδιωτικών και δημόσιων. Ο τραπεζικός και χρηματοπιστωτικός τομέας, ο τομέας υγείας, η φορολογία, οι ασφαλίσεις, η εμπορική προώθηση και η διαφήμιση είναι μερικά μόνο παραδείγματα.* Για παράδειγμα, η πιστοληπτική ικανότητα ενός ατόμου μπορεί να αξιολογηθεί αυτοματοποιημένα από λογισμικό, αξιοποιώντας και αξιολογώντας πληθώρα πληροφοριών για το άτομο. Μία ενδιαφέρουσα πηγή αναφορικά με τους διάφορους

[21] Η τεχνητή νοημοσύνη αναφέρεται στην ικανότητα μιας μηχανής να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι η μάθηση, ο σχεδιασμός και η δημιουργικότητα.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τομείς που μπορούν να χρησιμοποιηθούν οι εν λόγω αλγόριθμοι, και ειδικότερα για τομείς άπτονται του εμπορικού δικαίου, του οικογενειακού, στεγαστικού και πτωχευτικού, σε συνδυασμό με τους συναφείς κινδύνους για υποκείμενα των δεδομένων, είναι η [45].

Πράγματι, οι κίνδυνοι για τα υποκείμενα των δεδομένων από αυτοματοποιημένες, βάσει αλγορίθμων, αποφάσεις που λαμβάνονται για αυτά είναι μεγάλοι. Σύμφωνα με το [44], οι εν λόγω επεξεργασίες κατ' αρχάς μπορεί να γίνονται ερήμην των προσώπων που αφορούν, τα οποία να μη γνωρίζουν απολύτως τίποτα ως προς το ότι καταρτίζεται συγκεκριμένο προφίλ για αυτά ή να μην γνωρίζουν με τι είδους δεδομένα τους καταρτίζεται το προφίλ, όπως και με ποια λογική ο υποκείμενος αλγόριθμος λαμβάνει αποφάσεις για αυτά (π.χ. κατάταξή τους σε συγκεκριμένη κατηγορία). Η κατάταξη ενός ατόμου σε συγκεκριμένη κατηγορία μπορεί να συνιστά περιορισμό στις ελευθερίες του – ενώ δεν αποκλείεται η κατάταξή του αυτή να είναι λανθασμένη. Σε κάθε περίπτωση, η κατάρτιση προφίλ μπορεί να έχει ως αποτέλεσμα τη διαιώνιση υφιστάμενων στερεοτύπων και του κοινωνικού διαχωρισμού [44].

Λόγω των ανωτέρω υπαρκτών κινδύνων, ο ΓΚΠΔ αναγνωρίζει στο άρθρο 22 ένα συναφές δικαίωμα σχετικά με την αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ. Κατ' αρχάς, στο άρθρο 4 στοιχ. 4 ορίζεται η κατάρτιση προφίλ ως *οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου*. Το κρίσιμο στοιχείο εδώ είναι η έννοια της αυτοματοποιημένης επεξεργασίας: ωστόσο, από τον ορισμό δεν προκύπτει ότι αποκλείεται τελείως η παρουσία ανθρώπινου παράγοντα για τη δημιουργία προφίλ.

Το δικαίωμα που αναγνωρίζει ο ΓΚΠΔ στο άρθρο 22 παρ. 1 είναι το εξής: «*το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο*». Συνεπώς, το εν λόγω δικαίωμα αφορά την περίπτωση αποκλειστικά αυτοματοποιημένης επεξεργασίας (και, άρα, όχι κάθε κατάρτιση προφίλ[22]), εφόσον από την απόφαση που λαμβάνεται προκύπτουν έννομα αποτελέσματα για το άτομο ή αυτό επηρεάζεται σημαντικά.

- Μπορεί να υπάρξει αυτοματοποιημένη λήψη απόφασης χωρίς δημιουργία προφίλ (π.χ. επιβολή προστίμου λόγω παραβίασης ορίου ταχύτητας, βάσει «έξυπνου» συστήματος καμερών παρακολούθησης για παράβαση του Κ.Ο.Κ), όπως βέβαια και δημιουργία προφίλ χωρίς αυτοματοποιημένες αποφάσεις. Ωστόσο, οι δύο έννοιες δεν είναι ασύμβατες και σαφώς μπορούν να συνυπάρξουν (π.χ. το ύψος προστίμου στην ανωτέρω περίπτωση να προσδιορίζεται από τυχόν προηγούμενες παραβάσεις, βάσει προφίλ που έχει δημιουργηθεί) [44]

**Παράδειγμα (βασισμένο σε παράδειγμα από το** [44]**):** Αποφάσεις από αυτοματοποιημένη επεξεργασία που παράγουν έννομα αποτελέσματα για το υποκείμενο των δεδομένων μπορεί να είναι, ενδεικτικώς, σχετικές με την απόκτηση δικαιώματος ή τον αποκλεισμό από συγκεκριμένη κοινωνική παροχή η οποία χορηγείται βάσει του νόμου, όπως επίδομα τέκνων ή στεγαστικό επίδομα, ή την άρνηση εισδοχής σε μια χώρα και την άρνηση παροχής ιθαγένειας. Αποφάσεις που επιφέρουν σημαντικές συνέπειες για το υποκείμενο των δεδομένων μπορεί να είναι, ενδεικτικώς, σχετικές με αποκλεισμό του από μια ευκαιρία απασχόλησης ή που επηρεάζουν την πρόσβασή του στην εκπαίδευση (π.χ. την εισαγωγή στο πανεπιστήμιο).

Κρίσιμο σημείο είναι το εξής: Ο όρος «δικαίωμα» στη εν λόγω διάταξη δεν σημαίνει

[22] Βέβαια, για περίπτωση κατάρτισης προφίλ χωρίς πλήρως αυτοματοποιημένη επεξεργασία, ενδεχομένως, ανά περίπτωση, να έχουν εφαρμογή άλλα δικαιώματα που ήδη έχουμε δει, όπως, π.χ. το δικαίωμα εναντίωσης του άρθρου 21.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ότι εφαρμόζεται μόνο όταν ασκείται από το υποκείμενο των δεδομένων. Στο άρθρο 22 παρ. 1 θεσπίζεται ουσιαστικά γενική απαγόρευση της λήψης αποφάσεων (με έννομα αποτελέσματα ή με σημαντικές συνέπειες) με βάση αποκλειστικά αυτοματοποιημένη επεξεργασία [44]. Πρέπει επίσης να επισημανθεί ότι ο υπεύθυνος επεξεργασίας δεν μπορεί να «κατασκευάζει» ανθρώπινη παρέμβαση προκειμένου να αποφύγει την απαγόρευση που θέτει η εν λόγω διάταξη (π.χ. δεν μπορεί να επικαλείται ότι υπάρχει ανθρώπινη παρέμβαση επειδή άνθρωπος κάνει ενέργειες απλά προς εφαρμογή του αποτελέσματος που παρήγαγε ο αλγόριθμος λήψης αυτοματοποιημένων αποφάσεων).

Υπάρχουν ωστόσο περιπτώσεις όπου μία τέτοια λήψη απόφασης είναι επιτρεπτή (βλ. παρ. 2 του άρθρου 22). Ειδικότερα, το ως άνω δικαίωμα δεν εφαρμόζεται όταν:

i. Η εν λόγω επεξεργασία προβλέπεται ρητά από το δίκαιο της Ένωσης ή το εθνικό δίκαιο. Π.χ. μπορεί να υπάρχει ειδική νομική πρόβλεψη για πραγματοποίηση μίας τέτοιας επεξεργασίας για σκοπούς παρακολούθησης και πρόληψης της απάτης και της φοροδιαφυγής. Η σχετική νομοθεσία πρέπει να θεσπίζει κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.
ii. Το υποκείμενο των δεδομένων έχει δώσει τη ρητή συγκατάθεσή του – χαρακτηριστικό παράδειγμα, το οποίο μπορεί να έχει εφαρμογή στο Δημόσιο Τομέα είναι η διενέργεια μίας τέτοιας επεξεργασίας στο πλαίσιο ερευνητικού προγράμματος που εκπονεί Πανεπιστήμιο (οπότε και, εφόσον οι συμμετέχοντες σε αυτό δώσουν τη ρητή συγκατάθεσή τους κατόπιν πλήρους ενημέρωσής τους, η επεξεργασία είναι επιτρεπτή). Και σε αυτήν την περίπτωση βέβαια ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.
iii. Η επεξεργασία είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ υποκειμένου των δεδομένων και υπευθύνου επεξεργασίας (περίπτωση που μάλλον δύσκολα θα έχει εφαρμογή στο Δημόσιο Τομέα).

Σε κάθε περίπτωση, μία τέτοια επεξεργασία πρέπει να είναι απόλυτα διαφανής προς τα υποκείμενα των δεδομένων, όπου η σχετική ενημέρωση που θα παρέχεται προς



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αυτά, είτε τα δεδομένα συλλέγονται από τα ίδια τα υποκείμενα (άρθρο 13 του ΓΚΠΔ) είτε όχι (άρθρο 14 του ΓΚΠΔ), θα πρέπει να περιέχει πληροφορίες και σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων. Πρόσθετα μέτρα που μπορεί να λάβει ο υπεύθυνος επεξεργασίας για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων είναι να δίνεται το δικαίωμα διατύπωσης της άποψής του, το δικαίωμα να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω επεξεργασίας αλλά και το δικαίωμα αμφισβήτησης της απόφασης (βλ. παρ. 3 του ιδίου άρθρου). Εξάλλου, όπως θα δούμε μετέπειτα στην Ενότητα 10, για κάθε τέτοια επεξεργασία είναι υποχρεωτική η εκτίμηση αντικτύπου ως προς την προστασία δεδομένων.

- Σύμφωνα με την αιτιολογική σκέψη 71 του ΓΚΠΔ, προκειμένου να διασφαλισθεί δίκαιη και διαφανής επεξεργασία σε σχέση με το υποκείμενο των δεδομένων, λαμβανομένων υπόψη των ειδικών συνθηκών και του πλαισίου εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες σε δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος.

Η αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ που βασίζονται σε



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο υπό ειδικές προϋποθέσεις. Ειδικότερα, σύμφωνα και με την παρ. 4 του άρθρου 22, μία τέτοια επεξεργασία επιτρέπεται μόνο εφόσον σωρευτικά πληρούνται τα εξής:

- υπάρχει μία εφαρμοστέα εξαίρεση από το άρθρο 22 παράγραφος 2, και
- εφαρμόζεται το στοιχείο α΄ ή ζ΄ του άρθρου 9 παράγραφος 2 (όπου η πρώτη περίπτωση είναι αυτή όπου υπάρχει ρητή συγκατάθεση του υποκειμένου των δεδομένων και η δεύτερη είναι αυτή όπου η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων).

Φυσικά, και στην περίπτωση των δεδομένων ειδικών κατηγοριών, ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων των υποκειμένων των δεδομένων.

## 6.11 Περιορισμοί των δικαιωμάτων

Τα δικαιώματα των υποκειμένων των δεδομένων δύνανται να υπόκεινται σε περιορισμούς: αυτό προβλέπεται στο άρθρο 23 του ΓΚΠΔ. Ωστόσο, σύμφωνα πάντα με το ίδιο άρθρο, για να υπάρχουν περιορισμοί στα δικαιώματα πρέπει:

a. Να υπάρχει ειδική προς τούτο νομοθετική πρόβλεψη.
b. Ο περιορισμός να σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και να συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση:

   α) της ασφάλειας του κράτους,

   β) της εθνικής άμυνας,

   γ) της δημόσιας ασφάλειας,

   δ) της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της πρόληψης



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αυτών,

ε) άλλων σημαντικών στόχων γενικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους, ιδίως σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος της Ένωσης ή κράτους μέλους, συμπεριλαμβανομένων των νομισματικών, δημοσιονομικών και φορολογικών θεμάτων, της δημόσιας υγείας και της κοινωνικής ασφάλισης,

στ) της προστασίας της ανεξαρτησίας της δικαιοσύνης και των δικαστικών διαδικασιών,

ζ) της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης παραβάσεων δεοντολογίας σε νομοθετικά κατοχυρωμένα επαγγέλματα,

η) της παρακολούθησης, της επιθεώρησης ή της κανονιστικής λειτουργίας που συνδέεται, έστω περιστασιακά, με την άσκηση δημόσιας εξουσίας στις περιπτώσεις που αναφέρονται στα στοιχεία α) έως ε) και ζ),

θ) της προστασίας του υποκειμένου των δεδομένων ή των δικαιωμάτων και των ελευθεριών τρίτων,

ι) της εκτέλεσης αστικών αξιώσεων.

☞ Για να υπάρξει περιορισμός στα δικαιώματα, πρέπει υποχρεωτικά για τον περιορισμό αυτόν να υπάρχει ρητή νομοθετική πρόβλεψη[23]. Η νομική βάση ή το νομοθετικό μέτρο θα πρέπει να είναι διατυπωμένο με σαφήνεια και ακρίβεια και η εφαρμογή του να είναι προβλέψιμη για τα πρόσωπα που υπόκεινται σε αυτό (βλ. και Αιτιολογική Σκέψη 41 του ΓΚΠΔ).

Είναι κρίσιμο να σημειωθεί ότι οι περιορισμοί στα δικαιώματα αποτελούν την εξαίρεση και όχι τον κανόνα: ως εκ τούτου, δεν μπορούν να ερμηνεύονται με ευρεία

[23] Σύμφωνα με την Αιτιολογική Σκέψη 41, οποτεδήποτε ο ΓΚΠΔ αναφέρεται σε νομική βάση ή νομοθετικό μέτρο, αυτό δεν προϋποθέτει απαραιτήτως νομοθετική πράξη εγκεκριμένη από ένα κοινοβούλιο. Ωστόσο, αυτή η νομική βάση ή το νομοθετικό μέτρο θα πρέπει να είναι διατυπωμένο με σαφήνεια και ακρίβεια και η εφαρμογή του να είναι προβλέψιμη για πρόσωπα που υπόκεινται σε αυτό, σύμφωνα με τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης και του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου. Εξάλλου, σύμφωνα και με το άρθρο 52 παρ. 1 του Χάρτη Ανθρωπίνων Δικαιωμάτων, Κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον Χάρτη πρέπει να προβλέπεται από το νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

έννοια. Ο υπεύθυνος επεξεργασίας, σύμφωνα και με την αρχή της λογοδοσίας, θα πρέπει να μπορεί να αποδείξει, εφόσον περιορίζει κάποιο δικαίωμα, ότι πράγματι ο περιορισμός είναι κατ' εξαίρεση επιτρεπτός: αυτό θα πρέπει να προκύπτει με σαφήνεια από τη σχετική νομοθετική πρόβλεψη, χωρίς να γίνεται καμία διασταλτική ερμηνεία αυτής, και βεβαίως ο σκοπός του περιορισμού του δικαιώματος θα πρέπει να εμπίπτει σε αυτούς της περίπτωσης 2 ανωτέρω. Στις σχετικές Κατευθυντήριες Γραμμές 10/2020 του ΕΣΠΔ [46] αναλύονται περαιτέρω οι προϋποθέσεις υπό τις οποίες η σχετική νομική πρόβλεψη σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών.

**Παράδειγμα:** Πολίτης ασκεί δικαίωμα πρόσβασης σε φορέα Α. Ο φορέας Α κρίνει ότι δέον είναι, κατ' εξαίρεση, να μην ικανοποιήσει το δικαίωμα, γιατί στη συγκεκριμένη περίπτωση η ικανοποίησή του επηρεάζει υπέρμετρα τα έννομα συμφέροντά του, σε σχέση με την έκταση του περιορισμού των δικαιωμάτων και ελευθεριών που θα επέλθει από τη μη ικανοποίησή του. Ωστόσο, για τη συγκεκριμένη περίπτωση, δεν υπάρχει καμία νομική πρόβλεψη που να επιτρέπει τον περιορισμό του δικαιώματος. Συνεπώς, δεν υφίσταται κανένας περιορισμός και το δικαίωμα πρέπει να ικανοποιηθεί.

Η παράγραφος 2 του άρθρου 23 του ΓΚΠΔ παρουσιάζει το τι θα πρέπει να καλύπτει, ως πληροφορία, μία τέτοια διάταξη αναφορικά με περιορισμό δικαιωμάτων. Ειδικότερα, κάθε τέτοιο νομοθετικό μέτρο, το οποίο όπως προαναφέρθηκε (βλ. παρ. 1 του άρθρου 23) θα πρέπει να σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και να συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία, θα πρέπει να έχει διατάξεις που να αφορούν, κατά περίπτωση, τουλάχιστον τα εξής:

- τους σκοπούς της επεξεργασίας ή τις κατηγορίες επεξεργασίας,
- τις κατηγορίες δεδομένων προσωπικού χαρακτήρα,
- το πεδίο εφαρμογής των περιορισμών που επιβλήθηκαν (π.χ. περιορισμοί μόνο σε κάποια δικαιώματα),
- εγγυήσεις για την πρόληψη καταχρήσεων ή παράνομης πρόσβασης ή



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

διαβίβασης (οι οποίες μπορεί να περιλαμβάνουν οργανωτικά και τεχνικά μέτρα – βλ. και Ενότητα 10),

- ειδική περιγραφή του υπευθύνου επεξεργασίας ή των κατηγοριών των υπευθύνων επεξεργασίας,
- περιόδους αποθήκευσης και ισχύουσες εγγυήσεις,
- κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (οι οποίοι μπορούν να προκύψουν και μέσω εκτίμησης αντικτύπου για τα προσωπικά δεδομένα, όπως θα συζητήσουμε στην Ενότητα 10 και θα μπορούσαν ενδεχομένως να αποτυπώνονται και στην αιτιολογική έκθεση του νόμου) και
- το δικαίωμα των υποκειμένων των δεδομένων να ενημερώνονται σχετικά με τον περιορισμό, εκτός εάν αυτό μπορεί να αποβεί επιζήμιο για τους σκοπούς του περιορισμού.

Το ΕΣΠΔ, στις Κατευθυντήριες Γραμμές 10/2020 [46] προτείνει την ενεργή συμμετοχή του Υπευθύνου Προστασίας Δεδομένων κάθε φορά που περιορίζεται δικαίωμα (ήτοι να ενημερώνεται σχετικά και να λαμβάνει γνώση την τεκμηρίωση του περιορισμού). Ο Υπεύθυνος Προστασίας Δεδομένων είναι ένας πολύ σημαντικός ρόλος εντός του οργανισμού, υποχρεωτικός για κάθε Δημόσιο φορέα, και αναλύεται στην Ενότητα 9.

Ο ν. 4624/2019, στα άρθρα 31-35, προβλέπει περιορισμούς σε δικαιώματα. Ωστόσο, για τους εν λόγω περιορισμούς, η Αρχή με τη Γνωμοδότηση 1/2020 έχει εκφράσει επιφυλάξεις ως προς το αν οι περιορισμοί αυτοί είναι σύμφωνοι με τον ΓΚΠΔ αλλά και με τις επιταγές που απορρέουν από τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και την ΕΣΔΑ. Ειδικότερα, όπως αναφέρεται στην εν λόγω Γνωμοδότηση, «*με τα άρθρα 31 έως 35 του νόμου προβλέπονται εκτεταμένοι περιορισμοί των δικαιωμάτων των υποκειμένων χωρίς να ορίζονται συγκεκριμένες ρυθμίσεις ανάλογα με την περίπτωση για τα θέματα που αναφέρονται στην παράγραφο 2 του άρθρου 23 ΓΚΠΔ*». Ως εκ τούτου, και καθώς η Αρχή επιφυλάσσεται να κρίνει ανά περίπτωση τους εν λόγω περιορισμούς, δεν θα αναλυθούν περαιτέρω στο παρόν.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

☞ Δημόσιοι φορείς που επιθυμούν να περιορίσουν κάποιο δικαίωμα του ΓΚΠΔ, οφείλουν να εξετάσουν αν στην δική τους νομοθεσία προβλέπεται τέτοιος περιορισμός, με τα χαρακτηριστικά του άρθρου 23 παρ. 2. Η επίκληση των άρθρων 31-35 του ν. 4624/2019 δεν επαρκεί.

Τέλος, άξιο αναφοράς είναι ότι, με αφορμή και την πανδημία του COVID-19, το ΕΣΠΔ εξέδωσε δήλωση[24] σχετικά με τα δικαιώματα του υποκειμένου των δεδομένων στο πλαίσιο της κατάστασης έκτακτης ανάγκης στα κράτη μέλη. Όπως επισημαίνει, μεταξύ άλλων, το ΕΣΠΔ, ο ΓΚΠΔ εξακολουθεί να εφαρμόζεται και επιτρέπει μια αποτελεσματική απόκριση στην πανδημία, προστατεύοντας ταυτόχρονα τα θεμελιώδη δικαιώματα και τις ελευθερίες. Επίσης, στην ίδια δήλωση, αναφέρεται ότι *τα δικαιώματα του υποκειμένου των δεδομένων αποτελούν τον πυρήνα του θεμελιώδους δικαιώματος της προστασίας των δεδομένων, το δε άρθρο 23 του ΓΚΠΔ πρέπει να ερμηνεύεται με γνώμονα την αρχή ότι η άσκηση των εν λόγω δικαιωμάτων πρέπει να αποτελεί τον γενικό κανόνα. Καθώς οι περιορισμοί αποτελούν εξαιρέσεις στον γενικό κανόνα, η εφαρμογή τους πρέπει να επιτρέπεται μόνο σε συγκεκριμένες περιπτώσεις (...) Η απλή ύπαρξη πανδημίας ή οποιασδήποτε άλλης κατάστασης έκτακτης ανάγκης δεν δικαιολογεί επαρκώς την εφαρμογή οποιουδήποτε περιοριστικού μέτρου σε βάρος των δικαιωμάτων των υποκειμένων των δεδομένων (...)Περιορισμοί που θεσπίζονται στο πλαίσιο μιας κατάστασης έκτακτης ανάγκης αναστέλλοντας ή αναβάλλοντας την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων και την τήρηση των σχετικών υποχρεώσεων των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία χωρίς σαφές χρονικό όριο ισοδυναμούν με εν τοις πράγμασι γενική αναστολή των εν λόγω δικαιωμάτων και δεν είναι συμβατοί με την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών.*

## 6.12 Εφαρμογή δικαιωμάτων ανά νομική βάση

Τα δικαιώματα που παρέχονται στα υποκείμενα των δεδομένων βάσει του ΓΚΠΔ δεν εφαρμόζονται όλα σε κάθε περίπτωση. Ορισμένα από τα δικαιώματα εφαρμόζονται

[24] Βλ. **https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_el**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μόνο όταν η επεξεργασία βασίζεται σε συγκεκριμένες νομικές βάσεις. Ο παρακάτω πίνακας, βασισμένος στο [38], παρουσιάζει συνοπτικά τα δικαιώματα που θα μπορούσαν να εφαρμοστούν όταν τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία βάσει των διαφορετικών νομικών βάσεων.

| | **Δικαίωμα Πρόσβασης** | **Δικαίωμα Διόρθωσης** | **Δικαίωμα Διαγραφής** | **Δικαίωμα Περιορισμού** | **Δικαίωμα Φορητότητας** | **Δικαίωμα Εναντίωσης** |
|---|---|---|---|---|---|---|
| **Συγκατάθεση** | ✔ | ✔ | ✔ | ✔ | ✔ | ~ Ανάκληση |
| **Σύμβαση** | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ |
| **Έννομη υποχρέωση** | ✔ | ✔ | ✘ | ✔ | ✘ | ✘ |
| **Ζωτικό Συμφέρον** | ✔ | ✔ | ✔ | ✔ | ✘ | ✘ |
| **Δημόσιο καθήκον** | ✔ | ✔ | ✘ | ✔ | ✘ | ✔ |
| **Υπέρτερο έννομο συμφέρον** | ✔ | ✔ | ✔ | ✔ | ✘ | ✔ |

Ωστόσο, ενδέχεται να υπάρχουν και άλλες απαιτήσεις ή περιορισμοί σχετικά με κάποια από τα δικαιώματα του υποκειμένου των δεδομένων που παρουσιάζονται παραπάνω. Ο πίνακας παρατίθεται ως ένα πρώτο εργαλείο, ώστε οι υπεύθυνοι επεξεργασίας να εξετάζουν ποια δικαιώματα μπορεί, κατ' αρχήν, να εφαρμόζονται κατά την αξιολόγηση των υποχρεώσεών τους.

## 6.13 Βιβλιογραφία για περισσότερη μελέτη

- Ομάδα Εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του Κανονισμού 2016/679». [41]
- Ομάδα Εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων». [42]
- Ομάδα Εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τη λήψη αυτοματοποιημένων αποφάσεων και τη δημιουργία προφίλ». [44]



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, «Κατευθυντήριες γραμμές 10/2020 σχετικά με τους περιορισμούς του άρθρου 23 του ΓΚΠΔ». [46]




Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 7. Ο ρόλος υπευθύνου και εκτελούντα

Όπως ήδη αναλύθηκε παραπάνω, στο άρθρο 5 παρ. 2 του ΓΚΠΔ εισάγεται η αρχή της λογοδοσίας σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας:

- είναι υπεύθυνος για τη συμμόρφωση με τις αρχές του άρθρου 5 παρ. 1 και
- πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τις αρχές αυτές.

Η αρχή της λογοδοσίας απευθύνεται κυρίως στον υπεύθυνο επεξεργασίας και αναπτύσσεται περαιτέρω στο άρθρο 24 του Κανονισμού. Ωστόσο, κάποιοι από τους κανόνες για τη λογοδοσία απευθύνονται τόσο στους υπεύθυνους επεξεργασίας όσο και στους εκτελούντες την επεξεργασία. Αυτή η αλλαγή, που είναι μια από τις ουσιαστικές του ΓΚΠΔ, έχει μάλιστα μεταφέρει και ένα επίπεδο «κινδύνων» από κυρώσεις και στους εκτελούντες την επεξεργασία. Οι εκτελούντες πρέπει πάντα να ενεργούν υπό τις οδηγίες του υπεύθυνου επεξεργασίας, αλλά πλέον, ο Κανονισμός κατανέμει την ευθύνη στους διαφόρους ρόλους που ενδέχεται να εμπλέκονται σε μια επεξεργασία.

## 7.1 Η ευθύνη του υπεύθυνου επεξεργασίας

Στο άρθρο 24 του ΓΚΠΔ, το οποίο προσδιορίζει τις ευθύνες του υπεύθυνου επεξεργασίας, αναφέρονται τα εξής:

«*1. Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο.*

*2. Όταν δικαιολογείται σε σχέση με τις δραστηριότητες επεξεργασίας, τα μέτρα που αναφέρονται στην παράγραφο 1 περιλαμβάνουν την εφαρμογή κατάλληλων πολιτικών για την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας.*

*3. Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας.*»

Η διάταξη αυτή αποτελεί την εισαγωγή στο Κεφάλαιο IV και προσδιορίζει το πλαίσιο των υποχρεώσεων λογοδοσίας, διευκρινίζοντας την αρχή της λογοδοσίας του άρθρου 5 παρ. 2. Πως πρέπει λοιπόν, να ενεργεί ένας υπεύθυνος επεξεργασίας για να διασφαλίζει και να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με ΓΚΠΔ;

Ο υπεύθυνος επεξεργασίας οφείλει να:

- Εφαρμόζει **κατάλληλα τεχνικά και οργανωτικά μέτρα**, τα οποία προσδιορίζονται με βάση:
    - Τα **ιδιαίτερα χαρακτηριστικά της επεξεργασίας** (φύση, πεδίο εφαρμογής, πλαίσιο, σκοπούς)
    - τους **κινδύνους** για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, για τους οποίους πρέπει να λαμβάνεται υπόψη ότι έχουν διαφορετική πιθανότητα να επέλθουν
- **Επανεξετάζει και να επικαιροποιεί** τα παραπάνω μέτρα.

Ο Κανονισμός αναφέρει ότι τα μέτρα αυτά όταν «*δικαιολογείται σε σχέση με τις δραστηριότητες επεξεργασίας*» δηλαδή για δραστηριότητες οι οποίες φαίνεται να έχουν κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας **οφείλει να διαθέτει κατάλληλες «πολιτικές**[25]**»** τις οποίες να εφαρμόζει. Η απαίτηση για την καταγραφή των διαδικασιών που ακολουθούνται σε σχέση με τα προσωπικά δεδομένα σε κείμενα πολιτικών δεν είναι απόλυτη, αλλά συνδέεται με τα χαρακτηριστικά της επεξεργασίας. Συνεπώς, σε έναν υπεύθυνο επεξεργασίας μικρού μεγέθους, ο οποίος τηρεί τα τυπικά και προβλεπόμενα από το νόμο αρχεία πελατών και εργαζομένων, η απαίτηση αυτή μπορεί να μην εφαρμόζεται. Αλλά σε μεγαλύτερους υπευθύνους επεξεργασίας, ειδικά όταν οι δραστηριότητες επεξεργασίας είναι δραστηριότητες ιδιαίτερης «έντασης» ως προς την επεξεργασία προσωπικών δεδομένων, είναι εξαιρετικά πιθανό οι εποπτικές αρχές να απαιτούν την ύπαρξη εγγράφων πολιτικών. Το άρθρο 24 παρ. 3 καταδεικνύει την προτίμηση του Κανονισμού σε εργαλεία έγγραφης απόδειξης της νομιμότητας, όπως οι κώδικες δεοντολογίας και οι εγκεκριμένοι μηχανισμοί πιστοποίησης, τα οποία εμπεριέχουν

[25] Υπενθυμίζουμε την αναφορά σε κατάλληλα εσωτερικά έγγραφα τα οποία χρησιμοποιούνται για την απόδειξη της συμμόρφωσης.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

και μια έννοια προληπτικού ελέγχου των εποπτικών αρχών, κατά την έγκρισή τους, αν και όχι κατά την εφαρμογή τους από τον εκάστοτε υπεύθυνο επεξεργασίας.

Στο άρθρο 24 είναι σαφής η **κινδυνοστραφής «risk-based» προσέγγιση** του Κανονισμού (όπως αναλύεται και περαιτέρω, τόσο στην Ενότητα 10 όσο και στην Ενότητα 15). Τα «κατάλληλα» μέτρα δεν είναι απόλυτα, δεν μπορεί να βασίζονται σε συνταγές. Ο Κανονισμός δεν περιέχει κατάλογο μέτρων, ούτε παραπέμπει σε έκδοση κανονιστικής πράξης ή απόφασης για τον προσδιορισμό των μέτρων αυτών. Άρα, ένας υπεύθυνος επεξεργασίας οφείλει, σε κάθε ξεχωριστή επεξεργασία, να προσδιορίζει τα κατάλληλα μέτρα, με βάση τους κινδύνους για την επεξεργασία.

Γίνεται επίσης λόγος για τη γενικότερη ευθύνη του υπεύθυνου επεξεργασίας «*να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό*» δηλαδή να εξασφαλίζει και να αποδεικνύει **το σύνολο της νομιμότητας μιας επεξεργασίας**. Επομένως, τα τεχνικά και οργανωτικά μέτρα που οφείλει να λαμβάνει ένας υπεύθυνος επεξεργασίας δεν πρέπει να περιορίζονται σε μέτρα ασφάλειας, αλλά να επεκτείνονται σε μέτρα για το σύνολο της νομιμότητας και άρα για τη διασφάλιση των αρχών των Κανονισμού.

Η αναφορά σε μέτρα που επανεξετάζονται και επικαιροποιούνται εισάγει έννοια παρόμοια με αυτή των Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών (π.χ. ISO27001) αλλά με την ουσιώδη διαφορά ότι απαιτεί Σύστημα Διαχείρισης Νομιμότητας Προσωπικών Δεδομένων.

Συμπερασματικά, ο ΓΚΠΔ φαίνεται, αρχικά, να παρουσιάζει «ανασφάλεια δικαίου», ιδίως σε σχέση με το τι μπορεί να απαιτήσει μια εποπτική αρχή από ένα φορέα. Οι υπεύθυνοι επεξεργασίας, (και σε κάποιες περιπτώσεις και οι εκτελούντες την επεξεργασία), έχουν το δύσκολο έργο να αποδεικνύουν τη νομιμότητα των δραστηριοτήτων τους γραπτά. Ακόμα και μια κατά τα άλλα νόμιμη δραστηριότητα επεξεργασίας μπορεί να θεωρηθεί μη συμβατή με το σύνολο των προϋποθέσεων νομιμότητας του ΓΚΠΔ, αν ο υπεύθυνος επεξεργασίας δεν χρησιμοποιεί «προληπτικά» «εργαλεία λογοδοσίας» για την τεκμηρίωση της νομιμότητας (βλ. σχετικά και τις Ενότητες 8-10).

Για την διασφάλιση των υπεύθυνων επεξεργασίας αλλά και την, σε ένα βαθμό άρση της ανασφάλειας δικαίου, ο ΓΚΠΔ παρέχει μια σειρά από «εργαλεία λογοδοσίας στα άρθρα 24 – 43. Όμως, η επιλογή του/των κατάλληλου/ων εργαλείου/ων είναι



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αποκλειστική ευθύνη του υπεύθυνου επεξεργασίας (και σε λίγες περιπτώσεις του εκτελούντος). Λίγα από τα «εργαλεία» είναι υποχρεωτικά για όλους (π.χ. συμβάσεις υπευθύνων - εκτελούντων), ενώ τα πιο πολλά είναι προαιρετικά ή υποχρεωτικά μόνο σε συγκεκριμένες περιπτώσεις (οι οποίες όμως δεν είναι λίγες). Στη συνέχεια του παρόντος θα εστιάσουμε σε πολλά από αυτά τα εργαλεία.

## 7.2 Από κοινού υπεύθυνοι επεξεργασίας

Το άρθρο 4 παρ. 7 του ΓΚΠΔ αναγνωρίζει ότι οι «*σκοποί και ο τρόπος*» της επεξεργασίας μπορεί να καθοριστούν από περισσότερες οντότητες. Υπεύθυνος επεξεργασίας, όπως είδαμε νωρίτερα, είναι η οντότητα που *μόνη ή από κοινού με άλλες*, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Αυτό σημαίνει ότι πολλές διαφορετικές οντότητες μπορεί να ενεργούν ως υπεύθυνοι για την ίδια επεξεργασία, με καθέναν από αυτούς να υπόκειται στις ισχύουσες διατάξεις προστασίας προσωπικών δεδομένων. Μια οντότητα μπορεί να είναι υπεύθυνος επεξεργασίας ακόμα κι αν δεν λαμβάνει όλες τις αποφάσεις ως προς τους σκοπούς και τα μέσα της επεξεργασίας. Τα κριτήρια για τον «κοινό έλεγχο» και ο βαθμός στον οποίο δύο ή περισσότερες οντότητες ασκούν από κοινού έλεγχο μπορεί να έχουν διαφορετικές μορφές.

### 7.2.1 Πότε έχουμε από κοινού υπεύθυνους επεξεργασίας;

Κοινός έλεγχος μπορεί να υπάρχει σε σχέση με μια συγκεκριμένη δραστηριότητα επεξεργασίας, όταν δύο ή παραπάνω οντότητες καθορίζουν «από κοινού» τον σκοπό και τα μέσα αυτής της δραστηριότητας. Το «από κοινού» πρέπει να ερμηνεύεται ως «μαζί» ή «όχι μόνες», σε διαφορετικές μορφές και συνδυασμούς, όπως εξηγείται παρακάτω. Όπως και για τον καθορισμό του υπεύθυνου επεξεργασίας, απαιτείται και εδώ μια πραγματολογική και όχι τυπική προσέγγιση. Το βασικό κριτήριο για την ύπαρξη κοινού ελέγχου είναι η κοινή συμμετοχή δύο ή περισσότερων φορέων στον προσδιορισμό των σκοπών ή/και των μέσων μιας επεξεργασίας. Αν είτε ο σκοπός είτε τα ουσιώδη μέσα της επεξεργασίας αποφασίζονται από παραπάνω από μια οντότητες, τότε υπάρχει περίπτωση «κοινού ελέγχου».

☞ Ένα βασικό κριτήριο για να αντιληφθούμε αν υπάρχει κοινός έλεγχος είναι το



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κατά πόσον η επεξεργασία θα ήταν εφικτή χωρίς τη συμμετοχή των οντοτήτων αυτών στον καθορισμό των σκοπών και των μέσων.

Επισημαίνουμε ότι δεν είναι όλες οι μορφές συνεργασίας οντοτήτων «κοινός έλεγχος». Απαιτείται μελέτη κάθε χωριστής περίπτωσης. Τυπικότερο παράδειγμα είναι η ανταλλαγή πληροφοριών μεταξύ δημοσίων φορέων.

**Παράδειγμα:** Κάθε δημόσιος φορέας αποτελεί υπεύθυνο επεξεργασίας για τα δεδομένα μισθοδοσίας των υπαλλήλων του. Η μισθοδοσία όμως εκτελείται μέσω της Ενιαίας Αρχής Πληρωμών, η οποία επιπλέον, έχει αρμοδιότητα οικονομικής επίβλεψης. Η ΕΑΠ και ο δημόσιος φορέας, δεν αποτελούν από κοινού υπευθύνους για την οικονομική επίβλεψη, παρότι επεξεργάζονται το ίδιο σύνολο δεδομένων. Κάθε φορέας επιτελεί τη δική του αρμοδιότητα. Η ΕΑΠ, ως προς την πληρωμή και μόνο, αποτελεί εκτελούντα την επεξεργασία για τους λοιπούς φορείς.

### 7.2.2 Επιμερισμός της ευθύνης

Ο Κανονισμός καθορίζει ότι οι από κοινού υπεύθυνοι επεξεργασίας οφείλουν να καθορίζουν με διαφανή τρόπο τις αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις του ΓΚΠΔ, μέσω συμφωνίας μεταξύ τους, εκτός κι αν ο κοινός έλεγχος προκύπτει μέσω νόμου, αλλά δεν ορίζει τη μορφή της συμφωνίας. Στην περίπτωση δημόσιων φορέων και καθώς η πλειονότητα των δραστηριοτήτων τους συνδέεται με τις αρμοδιότητές τους ή με υποχρεώσεις που τους αποδίδει ο νόμος, η συνηθέστερη περίπτωση είναι ο από κοινού έλεγχος να προκύπτει από νόμο. Με βάση όμως το άρθρο 26 απαιτείται να είναι καθορισμένο με διαφανή τρόπο το ποια οντότητα έχει ευθύνη για συμμόρφωση προς συγκεκριμένες υποχρεώσεις του ΓΚΠΔ, ιδίως όσον αφορά την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και τις υποχρεώσεις παροχής ενημέρωσης με βάση τα άρθρα 13 και 14. Συνεπώς, λαμβάνοντας υπόψη και την αρχή της λογοδοσίας, πρέπει να υπάρχει έγγραφο από το οποίο να προκύπτει, αδιαμφισβήτητα ο καταμερισμός της ευθύνης.

Επιπλέον, η κατανομή των αρμοδιοτήτων θα πρέπει να καλύπτει και άλλες υποχρεώσεις –που αναλύονται στη συνέχεια του παρόντος - όπως τα μέτρα ασφαλείας, την υποχρέωση κοινοποίησης παραβίασης δεδομένων, τις εκτιμήσεις επιπτώσεων στην προστασία δεδομένων, τη χρήση εκτελούντων την επεξεργασία,



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

διαβιβάσεις σε τρίτες χώρες και επικοινωνία με τα υποκείμενα των δεδομένων ή και τις εποπτικές αρχές. Ανεξάρτητα από τους όρους της συμφωνίας, τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματά τους προς οποιονδήποτε από τους από κοινού υπευθύνους επεξεργασίας. Τέλος, οι εποπτικές αρχές δεν δεσμεύονται από τους όρους της συμφωνίας ούτε για το χαρακτηρισμό των μερών ως από κοινού υπευθύνους ούτε σε σχέση με το καθορισμένο σημείο επαφής.

**Παράδειγμα:** Δημόσιο νοσοκομείο και δημόσιο πανεπιστήμιο αποφασίζουν να ξεκινήσουν μαζί κλινική δοκιμή με τον ίδιο ερευνητικό στόχο. Τα δύο ιδρύματα συνεργάζονται για τη σύνταξη του πρωτοκόλλου της δοκιμής. Μπορούν να θεωρηθούν ως από κοινού υπεύθυνοι επεξεργασίας, για αυτή την κλινική δοκιμή, καθώς καθορίζουν και συμφωνούν μαζί τον σκοπό και τα ουσιαστικά μέσα της επεξεργασίας. Η συλλογή προσωπικών δεδομένων από τον ιατρικό φάκελο του ασθενούς με σκοπό την έρευνα, πρέπει να διακρίνεται από την επεξεργασία των ίδιων δεδομένων για σκοπούς περίθαλψης, για την οποία το Νοσοκομείο παραμένει ο υπεύθυνος επεξεργασίας.

Σε περίπτωση όπως που το Νοσοκομείο δεν συμμετέχει στη σύνταξη του ερευνητικού πρωτοκόλλου (απλώς δέχεται το πρωτόκολλο που έχει ήδη εκπονηθεί από το Πανεπιστήμιο), το Πανεπιστήμιο θα πρέπει να θεωρείται ως υπεύθυνος επεξεργασίας και το Νοσοκομείο ως ο εκτελών την επεξεργασία για την κλινική δοκιμή.

**Παράδειγμα:** Στην υπόθεση Fashion ID C-40/17, το ΔΕΕ έκρινε ότι διαχειριστής ιστοσελίδας ο οποίος ενσωματώνει στην εν λόγω ιστοσελίδα πρόσθετο μέσου κοινωνικής δικτύωσης («like» button) το οποίο μέσω του φυλλομετρητή του επισκέπτη της ιστοσελίδας αντλεί περιεχόμενο από τον πάροχο του εν λόγω μέσου κοινωνικής δικτύωσης και διαβιβάζει στον εν λόγω πάροχο δεδομένα προσωπικού χαρακτήρα του επισκέπτη. Ο διαχειριστής της ιστοσελίδας πρέπει να θεωρηθεί από κοινού υπεύθυνος της επεξεργασίας, με τον πάροχο του μέσου κοινωνικής δικτύωσης. Η ευθύνη του διαχειριστή της ιστοσελίδας περιορίζεται μόνο στη συλλογή και την ανακοίνωση (με διαβίβαση στον πάροχο) των επίμαχων δεδομένων.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 7.3 Εκπρόσωποι υπευθύνων ή εκτελούντων επεξεργασίας

Σύμφωνα με το άρθρο 27 του ΓΚΠΔ, όταν ένας υπεύθυνος επεξεργασίας δεν έχει εγκατάσταση στην Ε.Ε., οφείλει να ορίσει γραπτώς εκπρόσωπο στην Ένωση ο οποίος να είναι εγκατεστημένος σε ένα από τα κράτη μέλη όπου βρίσκονται τα υποκείμενα των δεδομένων, των οποίων τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία, εφόσον η δραστηριότητα εμπίπτει εντός του πεδίου εφαρμογής του ΓΚΠΔ. Οι εποπτικές αρχές και τα υποκείμενα των δεδομένων μπορούν να απευθύνονται σε εκείνον, επιπρόσθετα ή αντί του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, για όλα τα θέματα που σχετίζονται με την επεξεργασία. Ο εκπρόσωπος αποτελεί ένα έγκυρο μέσο επικοινωνίας με τον υπεύθυνο ή τον εκτελούντα την επεξεργασία, αλλά δεν τον υποκαθιστά. Για παράδειγμα, καταγγελίες εξετάζονται πάντα σε σχέση με τον υπεύθυνο ή τον εκτελούντα και δεν μπορούν να επιβληθούν κυρώσεις κατά του εκπροσώπου του.

Προφανώς, η διάταξη αυτή δεν έχει εφαρμογή για δημόσιους φορείς του εξωτερικού. Επίσης, εκ των πραγμάτων, επηρεάζει ελάχιστα τους δημόσιους φορείς. Δημόσιος φορέας της Ε.Ε. οφείλει να είναι προσεχτικός όταν συμβάλλεται ή συνεργάζεται στο πλαίσιο μιας δραστηριότητας επεξεργασίας δεδομένων με εταιρεία χωρίς εγκατάσταση εντός Ε.Ε.. Η εν λόγω εταιρεία οφείλει (μεταξύ άλλων) να έχει ορίσει εκπρόσωπο εντός Ε.Ε. και ο δημόσιος φορέας οφείλει να το εξασφαλίσει. Φυσικά, ο ΓΚΠΔ καθιστά αρκετά δύσκολη τη συνεργασία δημόσιου φορέα με εταιρεία που δεν έχει εγκατάσταση εντός Ε.Ε, ιδίως αν ληφθεί υπόψη το κεφάλαιο V του κανονισμού για τις διαβιβάσεις δεδομένων σε τρίτες χώρες.

## 7.4 Εκτελούντες την επεξεργασία

Είδαμε νωρίτερα την έννοια του εκτελούντος την επεξεργασία και τι αυτό σημαίνει για τη νομοθεσία των προσωπικών δεδομένων. Η σχέση εκτελούντος την επεξεργασία με τον υπεύθυνο της επεξεργασίας είναι αναβαθμισμένη στο ΓΚΠΔ, σε σχέση με την οδηγία 95/46/ΕΚ. Αναφέραμε ήδη ότι οι εκτελούντες μπορεί να έχουν και αυτοί πλέον συγκεκριμένες υποχρεώσεις και, εκ τούτου ευθύνες σε περίπτωση μη συμμόρφωσής τους με συγκεκριμένες προβλέψεις της νομοθεσίας. Στο σύγχρονο κόσμο των μεγάλων επιχειρήσεων διαδικτύου, που οι εκτελούντες την επεξεργασία μπορεί να είναι πολυεθνικές εταιρείες με τεράστιους προϋπολογισμούς που παρέχουν



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

υπηρεσίες σε πλειάδα φορέων του δημόσιου και ιδιωτικού τομέα, είναι κρίσιμο να μπορεί να αποδοθεί η ευθύνη για μια παράβαση στην οντότητα η οποία έχει πραγματικά τον έλεγχο. Σε κάθε όμως περίπτωση, το βασικό χαρακτηριστικό του εκτελούντος την επεξεργασία είναι ότι **επεξεργάζεται δεδομένα για λογαριασμό και κατ' εντολή του υπεύθυνου επεξεργασίας**.

Ένα συγκεκριμένο άρθρο του ΓΚΠΔ, το άρθρο 28, ρυθμίζει τον τρόπο συνεργασίας υπευθύνου της επεξεργασίας και εκτελούντος. Βασικό χαρακτηριστικό είναι η ρητή απαίτηση για απόλυτα καθορισμένη σχέση μεταξύ υπεύθυνου και (κάθε) εκτελούντος την επεξεργασία.

☞ Η σχέση υπεύθυνου επεξεργασίας και εκτελούντος την επεξεργασία πρέπει υποχρεωτικά να διέπεται από σύμβαση ή άλλη νομική πράξη, η οποία να προβλέπεται σε νόμο (εθνικό η ευρωπαϊκό).

Η σύμβαση αυτή πρέπει να δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και να έχει συγκεκριμένο τύπο. Στο δημόσιο τομέα, αντί σύμβασης μεταξύ δημοσίων φορέων, μπορεί να υπάρχει διάταξη νόμου, η οποία καθορίζει το πλαίσιο συνεργασίας του εκτελούντος την επεξεργασίας με τον υπεύθυνο επεξεργασίας.

Στόχος της σύμβασης ή συμφωνίας είναι να παρέχονται επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, ώστε η επεξεργασία να:

1) Εξασφαλίζει τις απαιτήσεις του Κανονισμού, άρα το σύνολο της νομιμότητας, και
2) Να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.

Συνεπώς, με τη γραπτή αυτή ανάθεση της επεξεργασίας, επιδιώκεται να εξασφαλιστεί το σύνολο των δραστηριοτήτων (και η λογοδοσία) με έμφαση στην ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων.

☞ Δεν επιτρέπεται η εκτέλεση τμήματος επεξεργασίας από τρίτο φορέα χωρίς



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

έγγραφη σύμβαση ή νομική πράξη.

### 7.4.1 Ανάθεση επεξεργασίας από εκτελούντα σε νέο εκτελούντα την επεξεργασία.

Ο Κανονισμός δεν αποκλείει την περίπτωση να μπορεί ένας εκτελών την επεξεργασία να χρησιμοποιήσει επίσης άλλον εκτελούντα την επεξεργασία. Στα σύγχρονα μοντέλα επιχειρήσεων δεν είναι ασύνηθες μια εταιρεία να προσλαμβάνει έναν υπεργολάβο (ως εκτελούντα την επεξεργασία) ο οποίος με τη σειρά του, προκειμένου να φέρει εις πέρας τη σύμβαση που έχει αναλάβει, να προσλαμβάνει κι αυτός υπό-υπεργολάβο. Στο άρθρο 28 παρ. 2 του Κανονισμού καθορίζονται μέτρα και για αυτή την περίπτωση: «*Ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας. Σε περίπτωση γενικής γραπτής άδειας, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για τυχόν σκοπούμενες αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση των άλλων εκτελούντων την επεξεργασία, παρέχοντας με τον τρόπο αυτό τη δυνατότητα στον υπεύθυνο επεξεργασίας να αντιταχθεί σε αυτές τις αλλαγές.*».

☞ Για να προσλάβει ο εκτελών την επεξεργασία άλλον (υπο)εκτελούντα απαιτείται **προηγούμενη** ειδική ή γενική **γραπτή άδεια** από τον υπεύθυνο επεξεργασίας.

Η διάταξη διακρίνει δύο περιπτώσεις:

- Γενικής άδειας: όταν ο υπεύθυνος και ο εκτελών την επεξεργασία έχουν προνοήσει και στη σύμβαση συνεργασίας τους έχει προβλεφθεί ότι ο εκτελών μπορεί να προσλάβει νέο εκτελούντα την επεξεργασία. Η πρόβλεψη αυτή αποτελεί γενική άδεια. Στην περίπτωση αυτή, ο εκτελών την επεξεργασία, όταν επιθυμεί να προσθέσει ή να αντικαταστήσει έναν υποεκτελούντα, οφείλει να ενημερώσει τον υπεύθυνο επεξεργασίας για τις αλλαγές. Ο υπεύθυνος επεξεργασίας έχει πάντα τον τελευταίο λόγο, καθώς μπορεί να αντιταχθεί στη χρήση του νέου υποεκτελούντα την επεξεργασία.
- Ειδικής άδειας: όταν ο εκτελών την επεξεργασία ζητάει σε κάθε ξεχωριστή



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

περίπτωση ξεχωριστή, γραπτή άδεια, του υπευθύνου για τη χρήση ενός υποεκτελούντα την επεξεργασία.

Επομένως, σε κάθε περίπτωση, όλες οι αλλαγές και προσθήκες εκτελούντων την επεξεργασία, βρίσκονται υπό τον απόλυτο έλεγχο του υπεύθυνου της επεξεργασίας. Μάλιστα, ο ΓΚΠΔ δεν αποκλείει την πολλαπλών επιπέδων ανάθεση επεξεργασίας σε εκτελούντες, αρκεί για όλους τους εκτελούντες, όλων των επιπέδων, να υπάρχει τελικά, συμβατική δέσμευση και έλεγχος του υπευθύνου επεξεργασίας. Οι ίδιες υποχρεώσεις που βαρύνουν τον αρχικό εκτελούντα επιβάλλονται και σε κάθε άλλον εκτελούντα μέσω σύμβασης ή άλλης νομικής πράξης. Ο αρχικός εκτελών την επεξεργασία είναι πλήρως υπόλογος έναντι του υπευθύνου επεξεργασίας, όταν ο υποεκτελών δεν μπορεί να ανταποκριθεί στις υποχρεώσεις του.

### 7.4.2 Χαρακτηριστικά της πράξης ανάθεσης επεξεργασίας

Η πράξη ανάθεσης επεξεργασίας πρέπει, υποχρεωτικά με βάση την παρ. 3 του άρθρου 28, να έχει συγκεκριμένα χαρακτηριστικά. Δεν αρκεί μια τυπική σύμβαση συνεργασίας, αλλά πρέπει να περιέχει συγκεκριμένους όρους. Συνοπτικά, η σύμβαση πρέπει να καθορίζει:

- Το αντικείμενο της επεξεργασίας.
- Τη διάρκεια της επεξεργασίας.
- Τη φύση και **τον σκοπό** της επεξεργασίας.
- Το είδος των δεδομένων προσωπικού χαρακτήρα τα οποία θα επεξεργαστεί ο εκτελών.
- Τις κατηγορίες των υποκειμένων των δεδομένων τις οποίες αφορούν τα παραπάνω δεδομένα.
- Τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας, ιδίως όπως απορρέουν από το ΓΚΠΔ.

Ενώ η σύμβαση πρέπει, υποχρεωτικά, να περιέχει όρους για τα παρακάτω:

- Να ορίσει ότι ο εκτελών επεξεργάζεται προσωπικά δεδομένα μόνο βάσει **καταγεγραμμένων εντολών** του υπευθύνου επεξεργασίας,
    - Αυτό ισχύει πολύ περισσότερο για τη διαβίβαση δεδομένων σε τρίτη χώρα, εκτός εάν η διαβίβαση προβλέπεται σε νόμο, όταν και ο



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εκτελών την επεξεργασία οφείλει να ενημερώσει τον υπεύθυνο επεξεργασίας για την εν νομική απαίτηση

- Να διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα καλύπτονται από δέσμευση τήρησης εμπιστευτικότητας
- Για τη λήψη κατάλληλων (και συγκεκριμένων) μέτρων ασφάλειας.
- Για την πρόσληψη άλλου εκτελούντος την επεξεργασία, σύμφωνα με τις προβλέψεις του ΓΚΠΔ
- Για το ότι ο εκτελών οφείλει να επικουρεί τον υπεύθυνο επεξεργασίας για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας να απαντά σε αιτήματα άσκησης δικαιωμάτων του υποκειμένου των δεδομένων.
- Για το ότι ο εκτελών οφείλει να συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις λήψης μέτρων ασφάλειας, γνωστοποίησης και ανακοίνωσης περιστατικών παραβίασης, διενέργειας εκτίμησης αντικτύπου και αν χρειαστεί διαβούλευση με την εποπτική αρχή.
- Για το ότι ο εκτελών οφείλει να διαγράψει ή να επιστρέψει (ανάλογα με την επιλογή του υπευθύνου) όλα τα προσωπικά δεδομένα στον υπεύθυνο επεξεργασίας μετά την ολοκλήρωση της επεξεργασίας. Ο εκτελών οφείλει να διαγράψει κάθε αντίγραφο, εκτός εάν από νόμο απαιτείται η αποθήκευση των δεδομένων.
- Για το ότι ο εκτελών οφείλει να θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης του προς τις υποχρεώσεις του με βάση το άρθρο 28, οφείλει να επιτρέπει και να διευκολύνει τους ελέγχους από τον υπεύθυνο επεξεργασίας.

Επομένως, διαπιστώνουμε ότι ο υπεύθυνος επεξεργασίας έχει μεγάλη δυνατότητα ελέγχου πάνω στις δραστηριότητες του εκτελούντος, ο οποίος οφείλει να ακολουθεί τις οδηγίες και εντολές του. Μάλιστα, αν ο εκτελών την επεξεργασία κρίνει ότι κάποια εντολή παραβιάζει το ΓΚΠΔ ή άλλες διατάξεις νόμου, ο Κανονισμός δεν ορίζει ότι δεν πρέπει να υπακούσει, αλλά ότι οφείλει να ενημερώσει αμέσως τον υπεύθυνο επεξεργασίας.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ο εκτελών οφείλει να περιορίζεται μόνο στην εκτέλεση της επεξεργασίας η οποία εγγράφως του έχει ανατεθεί. Ο ρόλος του δεν περιλαμβάνει το καθορισμό των σκοπών ή των ουσιωδών μέσων της επεξεργασίας. Ο σκοπός πρέπει να καθορίζεται πλήρως από τον υπεύθυνο επεξεργασίας, ενώ ο εκτελών μπορεί να έχει ευθύνη καθορισμού των μη ουσιωδών μέσων της επεξεργασίας.

**Παράδειγμα:** Δημόσια υπηρεσία Α αναθέτει σε συνεργαζόμενη εταιρεία Β την εκτύπωση προσωποποιημένων επιστολών προς μεγάλο αριθμό πολιτών, με δικά τους οικονομικά δεδομένα. Η δημόσια υπηρεσία, λαμβάνοντας υπόψη τη νομοθεσία για τις δημόσιες συμβάσεις και το άρθρο 28 του ΓΚΠΔ, καταρτίζει σύμβαση, στην οποία προβλέπει, μεταξύ άλλων και την εφαρμογή συγκεκριμένων μέτρων ασφάλειας για τη αποφυγή της διαρροής των δεδομένων. Η εταιρεία Β, έχει πλήρως καθορισμένο σκοπό από την Α, και έχει καθορισμένο πλαίσιο λήψης μέτρων ασφάλειας. Η εταιρεία Β μπορεί όμως να καθορίσει μη ουσιώδη μέσα της επεξεργασίας, όπως το λογισμικό εκτύπωσης ή με ποιο τρόπο θα εφαρμόσει τα μέτρα ασφάλειας σε σχέση με το προσωπικό της.

Συνεπώς, για τα ζητήματα νομιμότητας (του άρθρου 6 του ΓΚΠΔ), η ευθύνη έγκειται στον υπεύθυνο επεξεργασίας, ενώ ο εκτελών την επεξεργασία ευθύνεται για την λήψη και την εφαρμογή των κατάλληλων μέτρων ασφάλειας (με βάση το αρ. 32 του ΓΚΠΔ, όπως αναλύεται στη συνέχεια[26]) και για να ακολουθεί, τόσο αυτός, όσο και το προσωπικό του, τις οδηγίες του υπεύθυνου επεξεργασίας. Η μη τήρηση, από την πλευρά του εκτελούντος την επεξεργασία, των οδηγιών του υπευθύνου επεξεργασίας, μπορεί να αποτελεί αυτοτελή παράβαση του άρθρου 29 του ΓΚΠΔ, όπου ρητά αναφέρεται η υποχρέωση αυτή.

Υπάρχουν όμως, περιπτώσεις που ο εκτελών την επεξεργασία μπορεί να θεωρηθεί ότι καθορίζει ο ίδιος νέο σκοπό (και μέσα) για μια επεξεργασία. Τότε, ο εκτελών την

[26] Προσοχή: όπως θα δούμε, οι υποχρεώσεις του άρθρου 32 του ΓΚΠΔ βαρύνουν γενικά τόσο υπευθύνους επεξεργασίας όσο και εκτελούντες την επεξεργασία. Εφόσον όμως μία επεξεργασία διενεργείται αποκλειστικά από τον εκτελούντα, για λογαριασμό του υπευθύνου επεξεργασίας, ο τελευταίος μπορεί μέχρι ένα σημείο μόνο να εξασφαλίσει την ασφάλεια της επεξεργασίας (όπως να επιλέξει εκτελούντα με κατάλληλα εχέγγυα, να θέσει συγκεκριμένες απαιτήσεις για την ασφάλεια, να ελέγχει με κάποιον τρόπο ότι οι απαιτήσεις ασφάλειας πληρούνται κτλ.). Η υλοποίηση των κατάλληλων μέτρων ασφάλειας, για την επίτευξη των στόχων που έχουν τεθεί από τον υπεύθυνο επεξεργασίας, είναι ευθύνη - σε ένα τέτοιο σενάριο - του εκτελούντος του επεξεργασία.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επεξεργασία θεωρείται υπεύθυνος επεξεργασίας για τη συγκεκριμένη επεξεργασία και ελέγχεται ως προς τούτο όχι μόνο για παράβαση των οδηγιών του υπευθύνου αλλά και για παραβάσεις νομιμότητας του ΓΚΠΔ.

**Παράδειγμα:** Δημόσια υπηρεσία Α αναθέτει, με κατάλληλη σύμβαση, σε συνεργαζόμενη εταιρεία Β την αποστολή μαζικών ενημερωτικών email για τη διεξαγωγή δημόσιας έρευνας. Η εταιρεία Β θεωρεί ότι μπορεί να χρησιμοποιήσει τα εν λόγω email για να προσεγγίσει νέους πελάτες, και στέλνει μηνύματα προς τούτο. Στην περίπτωση αυτή, η εταιρεία Β έχει καθορίσει το νέο σκοπό κατά παράβαση του ΓΚΠΔ, εκτός του πλαισίου της σύμβασης, συνεπώς θα αντιμετωπιστεί από την εποπτική αρχή ως ένας υπεύθυνος επεξεργασίας που παραβιάζει τις διατάξεις του ΓΚΠΔ.

### 7.4.3 Εργαλεία διευκόλυνσης της πράξης ανάθεσης επεξεργασίας

Όπως ήδη είδαμε, οι συμβάσεις υπευθύνου – εκτελούντος πρέπει να περιλαμβάνουν συγκεκριμένα στοιχεία και δημιουργούν πολλές υποχρεώσεις τόσο στον εκτελούντα, όσο και στον υπεύθυνο επεξεργασίας. Για τη διευκόλυνση των υπευθύνων και εκτελούντων ο Κανονισμός παρέχει τα εξής εργαλεία:

- Η τήρηση εκ μέρους του εκτελούντος την επεξεργασία **εγκεκριμένου κώδικα δεοντολογίας** σύμφωνα με το άρθρο 40 ή **εγκεκριμένου μηχανισμού πιστοποίησης** σύμφωνα με το άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για να αποδειχθεί ότι ο εκτελών παρέχει επαρκείς διαβεβαιώσεις. Στην πράξη, οι εκτελούντες την επεξεργασία οι οποίοι θα δεσμεύονται μέσω κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης, θα αποκτούν ένα σημαντικό ανταγωνιστικό πλεονέκτημα. Για τις εν λόγω έννοιες, παραπέμπουμε σχετικά στην Ενότητα 10.
- Η Ευρωπαϊκή Επιτροπή άσκησε τη δυνατότητα που της έχει δώσει ο Κανονισμός να θεσπίσει τυποποιημένες συμβατικές ρήτρες [47] μετά από κοινή γνώμη του ΕΣΠΔ και του Ευρωπαίου Επόπτη Προστασίας Δεδομένων [48]. Χρησιμοποιώντας τις πρότυπες αυτές συμβάσεις για τη μεταξύ τους σχέση, οι υπεύθυνοι και εκτελούντες την επεξεργασία έχουν τη νομική



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ασφάλεια ότι οι συμβάσεις τους είναι τυπικά πλήρεις. Απομένει, φυσικά, ο ουσιαστικός έλεγχος των μέτρων που περιγράφονται στα παραρτήματα της σύμβασης, τα οποία πρέπει να καταρτίζονται για το αντικείμενο της συγκεκριμένης ανάθεσης επεξεργασίας.

- Τυποποιημένες συμβατικές ρήτρες μπορεί να θεσπίσει και μια εποπτική αρχή. Αυτό έχει ιδιαίτερη αξία για συνεργασίες που διέπονται από το δίκαιο ενός συγκεκριμένου Κ-Μ. Έως τη στιγμή που γράφονται οι σημειώσεις αυτές, έχουν εκδοθεί και εγκριθεί από το ΕΣΠΔ τυποποιημένες συμβατικές ρήτρες από την εποπτική αρχή της Δανίας [49], ενώ έχουν εκδοθεί γνώμες για ρήτρες των αρχών της Σλοβενίας και της Λιθουανίας.

## 7.5 Βιβλιογραφία για περισσότερη μελέτη

ΕΣΠΔ - Guidelines 07/2020 on the concepts of controller and processor in the GDPR [23]



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 8. Λοιπές γενικές υποχρεώσεις

Στην παρούσα ενότητα θα εστιάσουμε σε κάποιες γενικές υποχρεώσεις τις οποίες εισήγαγε ο ΓΚΠΔ για τους υπευθύνους επεξεργασίας και οι οποίες εντάσσονται στη λεγόμενη κατηγορία «εργαλεία λογοδοσίας». Αυτές οι υποχρεώσεις είναι οι: α) Προστασία των δεδομένων ήδη από το σχεδιασμό, β) Προστασία των δεδομένων εξ ορισμού, γ) Αρχεία δραστηριοτήτων επεξεργασίας (η υποχρέωση αυτή αφορά και εκτελούντες την επεξεργασία, όπως θα εξηγηθεί).

## 8.1 Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Στην παρούσα υπο-ενότητα περιγράφονται κατά σειρά δύο υποχρεώσεις συναφείς μεταξύ τους: η προστασία των δεδομένων ήδη από το σχεδιασμό και η προστασία δεδομένων εξ ορισμού.

### 8.1.2 Προστασία των δεδομένων ήδη από το σχεδιασμό

Ανέκαθεν οι εποπτικές αρχές, και με το προηγούμενο νομικό πλαίσιο, υποστήριζαν ότι κατά το σχεδιασμό και ανάπτυξη/υλοποίηση μίας επεξεργασίας δεδομένων προσωπικού χαρακτήρα, οι απαιτήσεις για προστασία προσωπικών δεδομένων πρέπει να λαμβάνονται ουσιωδώς υπόψη εξ αρχής: διαφορετικά, η επεξεργασία μπορεί να υλοποιηθεί λανθασμένα, να μην είναι εφικτό, εκ των υστέρων, να γίνουν οι κατάλληλες τροποποιήσεις/αλλαγές και να απαιτείται εκ βάθρων επανασχεδίαση. Αυτή η απαίτηση, αν και δεν υπήρχε σαφώς διατυπωμένη σε νομικό κείμενο, είχε παγιωθεί με τον όρο «*ιδιωτικότητα εκ σχεδιασμού*» (*privacy by design*).

Ο ΓΚΠΔ εισάγει πλέον την ως άνω αρχή ως υποχρέωση για τους υπευθύνους επεξεργασίας, για κάθε είδος επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Πρόκειται για την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό (data



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

protection by design[27]), η οποία προβλέπεται στο άρθρο 25 παρ. 1 του ΓΚΠΔ:

«*Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.*»

Ουσιαστικά, η εν λόγω αρχή υποδηλώνει ότι σε κάθε στάδιο του κύκλου ζωής μίας επεξεργασίας δεδομένων (ανάλυση απαιτήσεων – σχεδίαση – υλοποίηση – παρακολούθηση), οι αρχές της προστασίας δεδομένων (κατά το άρθρο 5 του ΓΚΠΔ) πρέπει να «ενσωματώνονται» αποτελεσματικά, ως σχεδιαστικές παράμετροι και απαιτήσεις, μέσω κατάλληλων τεχνολογικών επιλογών αλλά και οργανωτικών μέτρων. Με άλλα λόγια, ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα σχεδιασμένα για την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις και να προστατεύονται τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων.

Σύμφωνα με τις Κατευθυντήριες Γραμμές 4/2019 του ΕΣΠΔ [47], ένα τεχνικό ή οργανωτικό μέτρο μπορεί να περιλαμβάνει πληθώρα ενεργειών, από τη χρήση προηγμένων τεχνικών λύσεων έως τη βασική εκπαίδευση του προσωπικού. Παραδείγματα που μπορεί να είναι κατάλληλα, αναλόγως του πλαισίου και των κινδύνων που συνδέονται με την εκάστοτε επεξεργασία, είναι: η ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα, η αποθήκευση διαθέσιμων δεδομένων

[27] Ο Ευρωπαίος νομοθέτης εισάγει τον όρο «data protection by design», ο οποίος ουσιαστικά αντανακλά την έννοια που οι περισσότεροι έδιναν στον προηγούμενο, καθιερωμένο στην πράξη, όρο «privacy by design». Ο νέος όρος βέβαια ενσωματώνει όλες τις αρχές προστασίας προσωπικών δεδομένων, συμπεριλαμβανομένων των απαιτήσεων για ικανοποίηση δικαιωμάτων κτλ.

προσωπικού χαρακτήρα σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, η παροχή δυνατότητας των υποκειμένων των δεδομένων να παρεμβαίνουν στην επεξεργασία, η πρόβλεψη συστημάτων ανίχνευσης κακόβουλου λογισμικού, η καθιέρωση συστημάτων διαχείρισης απορρήτου και ασφάλειας των πληροφοριών κλπ.

Πρέπει να σημειωθεί ότι η εκπλήρωση της εν λόγω υποχρέωσης δεν απαιτεί την εφαρμογή συγκεκριμένων τεχνικών και οργανωτικών μέτρων τα οποία να αφορούν, οριζόντια, κάθε επεξεργασία: η φύση της εκάστοτε επεξεργασίας, το πλαίσιο στο οποίο εντάσσεται, οι σχετικοί κίνδυνοι αλλά και το κόστος εφαρμογής των αντίστοιχων λύσεων σε σχέση με τους αντίστοιχους κινδύνους, λαμβάνοντας πάντα υπόψη τις πλέον πρόσφατες εξελίξεις στην τεχνολογία, πρέπει να συνυπολογίζονται – και ο υπεύθυνος επεξεργασίας οφείλει να μπορεί να αποδείξει ότι τα εξέτασε προσηκόντως και ότι σχεδίασε και υλοποίησε την επεξεργασία καταλλήλως, με βάση την αποτίμηση που πραγματοποίησε, έτσι ώστε να υπάρχει αποτελεσματική[28] υλοποίηση των αρχών προστασίας δεδομένων.

**Παράδειγμα[29]:** Ένας οργανισμός δημόσιων μεταφορών επιθυμεί να συγκεντρώσει στατιστικά στοιχεία με βάση τις διαδρομές των επιβατών, προκειμένου, από μία τέτοια πληροφορία, να ληφθούν αποφάσεις προς βελτίωση των παρεχόμενων υπηρεσιών (π.χ τροποποιήσεις δρομολογίων των μέσων μεταφοράς). Οι επιβάτες πρέπει να «περάσουν» το εισιτήριό τους μέσω ενός αναγνώστη (reader) κάθε φορά που εισέρχονται ή εξέρχονται από ένα μέσο μεταφοράς, το οποίο εισιτήριο έχει έναν μοναδικό αριθμό. Τα στατιστικά στοιχεία εξάγονται μέσω αυτού του αριθμού. Οι κάτοχοι εισιτηρίων ειδικού τύπου με έκπτωση (π.χ. φοιτητές, άνεργοι κτλ.), κατά την παραλαβή του εισιτηρίου έχουν παράσχει και τα προσωπικά τους στοιχεία προκειμένου αυτά να «αποτυπωθούν» στην όψη του εισιτηρίου (αφού πρέπει να

[28] Σύμφωνα με το [47], ο υπεύθυνος επεξεργασίας μπορεί να καθορίζει τους κατάλληλους δείκτες επιδόσεων για την απόδειξη της αποτελεσματικότητας. Ένας δείκτης επίδοσης συνιστά μετρήσιμη τιμή που επιλέγεται από τον υπεύθυνο επεξεργασίας, η οποία καταδεικνύει το πόσο αποτελεσματικά επιτυγχάνει ο υπεύθυνος επεξεργασίας τον στόχο του σε ό,τι αφορά την προστασία των δεδομένων. Οι δείκτες επιδόσεων μπορούν να είναι ποσοτικοί, όπως η μείωση των καταγγελιών, η μείωση του χρόνου απάντησης όταν τα υποκείμενα των δεδομένων ασκούν τα δικαιώματά τους κ.α., ή να είναι ποιοτικοί, όπως αξιολογήσεις επιδόσεων, χρήση κλιμάκων βαθμολόγησης ή αξιολόγηση από εμπειρογνώμονες.

[29] Βασισμένο στις Κατευθυντήριες Γραμμές 4/2019 του ΕΣΠΔ [47], αλλά και στη Γνωμοδότηση 1/2017 της Αρχής [102].

γίνεται χρήση τους αποκλειστικά και μόνο από τον κάτοχό τους) και τα οποία αποθηκεύονται από τον οργανισμό (με κατάλληλα οργανωτικά μέτρα ασφάλειας).

Εάν το πληροφοριακό σύστημα που αφορά την εν λόγω επεξεργασία υλοποιηθεί κατά τα ανωτέρω, τότε από την τήρηση των προσωπικών στοιχείων – για συγκεκριμένες έστω περιπτώσεις – αλλά και την επεξεργασία του μοναδικού αριθμού του εισιτηρίου για την εξαγωγή των ως άνω στατιστικών, ελλοχεύει ο κίνδυνος να εντοπίζονται ευχερώς συγκεκριμένοι επιβάτες και οι ακριβείς διαδρομές που πραγματοποιούν συνολικά: αυτό ισχύει σαφώς για όσους έχουν εισάγει τα προσωπικά τους στοιχεία και τα οποία έχουν καταχωρηθεί στο πληροφοριακό σύστημα, αλλά εν τούτοις ο εντοπισμός είναι πιθανός και μόνο από τον αριθμό εισιτηρίου και για κάποιες άλλες ειδικές περιπτώσεις – όπως, π.χ., για επιβάτες οι οποίοι ζουν ή εργάζονται σε αραιοκατοικημένες περιοχές (για παράδειγμα, αν υπάρχει η γνώση ότι συγκεκριμένο άτομο στην εν λόγω περιοχή είναι και το μόνο που πραγματοποιεί σε καθημερινή βάση ένα συγκεκριμένο δρομολόγιο, οπότε «αποκαλύπτεται» ο αριθμός του εισιτηρίου του).

Επομένως, δεδομένου ότι μία τέτοια πληροφορία δεν είναι απαραίτητη για τον σκοπό της βελτιστοποίησης των παρεχόμενων υπηρεσιών (και άρα, θα παραβίαζε την αρχή της *ελαχιστοποίησης* των δεδομένων), το σύστημα θα έπρεπε εξ αρχής να σχεδιαστεί, λαμβάνοντας εγκαίρως υπόψη τους ως άνω κινδύνους, έτσι ώστε: α) να μην τηρούνται σε κεντρική βάση τα προσωπικά στοιχεία των κατόχων των εισιτηρίων ειδικού τύπου, β) να μην αποθηκεύεται το αναγνωριστικό του εισιτηρίου, για το σκοπό της εξαγωγής στατιστικών – αφού πράγματι, μετά το τέλος του ταξιδιού, ο υπεύθυνος επεξεργασίας μπορεί να αποθηκεύει μόνο τις μεμονωμένες ταξιδιωτικές διαδρομές ώστε να μην είναι σε θέση να εντοπίσει ταξίδια που συνδέονται με ένα ενιαίο εισιτήριο, αλλά διατηρεί μόνο πληροφορίες για ξεχωριστές ταξιδιωτικές διαδρομές.

**Παράδειγμα:** Αρχή επιφορτισμένη για τη Δημόσια Υγεία οφείλει να συλλέγει, βάσει διάταξης, στοιχεία νοσηλευόμενων από νοσοκομεία προκειμένου να κάνει αντίστοιχες παρεμβάσεις, βάσει της ανάλυσης των πληροφοριών, υπέρ της Δημόσιας



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Υγείας. Η Αρχή για τη Δημόσια Υγεία κρίνει ότι για κάνει τις στοχευμένες παρεμβάσεις χρειάζονται στοιχεία όπως η ημερομηνία εισαγωγής/εξιτηρίου ασθενούς, διάγνωση, θεραπεία, αποτέλεσμα θεραπείας, φύλο ασθενούς, ημερομηνία γέννησης, πόλη/χωριό κατοικίας. Η εν λόγω διάταξη αναφέρεται σε «κωδικοποιημένα δεδομένα, που δεν επιτρέπουν την αναγνώριση του ασθενούς».

Για να υλοποιηθεί η απαίτηση της διάταξης, που άλλωστε είναι απόρροια της αρχής της ελαχιστοποίησης, πρέπει η επεξεργασία συνολικά να σχεδιαστεί εξ αρχής και υλοποιηθεί κατά τρόπο τέτοιο ώστε από τα συλλεγόμενα δεδομένα να μην είναι εφικτή, από την αρμόδια Αρχή για τη Δημόσια Υγεία, η αναγνώριση ασθενών (μία τέτοια αναγνώριση δεν είναι απαραίτητη για την επίτευξη του επιδιωκόμενου σκοπού). Ως εκ τούτου, πιθανά ενδεδειγμένα μέτρα είναι: ι) η αποστολή ψευδωνυμοποιημένης[30] πληροφορίας από το κάθε νοσοκομείο, όπου από το κάθε ψευδώνυμο από μόνο του δεν θα πρέπει να είναι εφικτή η ταυτοποίηση του προσώπου (π.χ. από το ψευδώνυμο δεν πρέπει να είναι δυνατή η ανάκτηση του ΑΜΚΑ του ασθενούς, ακόμα και αν ο ΑΜΚΑ αξιοποιείται για την παραγωγή μοναδικού ψευδωνύμου ανά ασθενή), β) Λήψη μέτρων ως προς το ακριβές είδος της πληροφορίας που θα διαβιβάζεται από τα νοσοκομεία, έτσι ώστε να είναι εφικτή η επίτευξη του επιδιωκόμενου σκοπού μειώνοντας στο ελάχιστο δυνατό τους κινδύνους αναγνώρισης για τα υποκείμενα των δεδομένων. Τέτοια μέτρα[31] μπορεί να είναι η αποστολή του έτους γέννησης αντί της ακριβούς ημερομηνίας γέννησης, η αποστολή ευρύτερης γεωγραφικής περιοχής διαμονής του ασθενούς αντί της επωνυμίας της πόλης/χωριού κτλ.

**Παράδειγμα (βασισμένο** στο [47], **με τροποποιήσεις):** Ένα νοσοκομείο συλλέγει δεδομένα σχετικά με τους ασθενείς του μέσω νοσοκομειακού πληροφοριακού συστήματος (ηλεκτρονικό μητρώο υγείας). Το προσωπικό του νοσοκομείου χρειάζεται πρόσβαση σε φακέλους ασθενών αναφορικά με την περίθαλψη και τη θεραπεία των ασθενών, καθώς και για την τεκμηρίωση όλων των μέτρων διάγνωσης, περίθαλψης και θεραπείας που λαμβάνονται. Η πρόσβαση πρέπει να παρέχεται μόνο

[30] Για τεχνικές ψευδωνυμοποίησης, θα γίνει ειδικότερη αναφορά στην Ενότητα 15
[31] Ουσιαστικά, τα μέτρα αυτά εντάσσονται σε τεχνικές ανωνυμοποίησης – βλ. Ενότητα 15



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σε εκείνα τα μέλη του ιατρικού προσωπικού που αναλαμβάνουν τη θεραπεία του αντίστοιχου ασθενούς στο τμήμα της ειδικότητας όπου αυτός υπάγεται. Η ομάδα ατόμων που έχουν πρόσβαση στον φάκελο ενός ασθενούς διευρύνεται μόνο εφόσον στη θεραπεία του συμμετέχουν και άλλα τμήματα ή διαγνωστικές μονάδες.

Η συνολική σχεδίαση του πληροφοριακού συστήματος πρέπει εξ αρχής να υλοποιεί κατάλληλο σύστημα προσβάσεων/εξουσιοδοτήσεων. Για παράδειγμα, υπάλληλοι λογιστηρίου δεν χρειάζεται να έχουν πρόσβαση στο περιεχόμενο ιατρικού φακέλου, αφού αυτή η πληροφορία δεν χρειάζεται για την τιμολόγηση.

**Ερώτηση δραστηριότητας**: Υπουργείο αναφέρει στην ιστοσελίδα του, σε σχέση με την παροχή πληροφόρησης προς τους πολίτες για τις επεξεργασίες που επιτελεί με νομική βάση τη συμμόρφωση με έννομη υποχρέωση (άρ. 6 παρ. 1 στοιχ. γ' του ΓΚΠΔ), όλους τους σχετικούς νόμους με υπερσυνδέσμους στα .pdf αρχεία αυτών. Ειδικότερα, η ενημέρωση για τις συγκεκριμένες επεξεργασίες είναι η εξής:

*«Συλλέγουμε και επεξεργαζόμαστε δεδομένα σας βάσει των ν. XXXX/2018 [link], YYYY/2019 [link] και ZZZZ/2020 [link]. Δεν επεξεργαζόμαστε άλλα δεδομένα σας παρά μόνο όσα προβλέπονται στις εν λόγω διατάξεις. Η νομική μας βάσει, σύμφωνα με το ΓΚΠΔ, είναι η εκπλήρωση έννομης υποχρέωσής μας (άρ. 6 παρ. 1 στοιχ. γ' του ΓΚΠΔ)».*

Πιστεύετε ότι ανακύπτει, από το ανωτέρω και μόνο κείμενο ενημέρωσης, παραβίαση του άρθρου 25 παρ.1 του ΓΚΠΔ για την προστασία των δεδομένων ήδη από το σχεδιασμό; Αν ναι, για ποια αρχή προστασίας δεδομένων δεν έχουν εφαρμοστεί αποτελεσματικά κατάλληλα τεχνικά και οργανωτικά μέτρα; Εξηγείστε συνοπτικά το συλλογισμό σας.

### 8.1.2 Προστασία των δεδομένων εξ ορισμού

Μία συναφής με την ανωτέρω υποχρέωση των υπευθύνων επεξεργασίας είναι η προστασία των δεδομένων εξ ορισμού (data protection by default), η οποία



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προβλέπεται στο άρθρο 25 παρ. 2 του ΓΚΠΔ. Σύμφωνα με αυτή:

*«Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων».*

Ουσιαστικά, ο ΓΚΠΔ αναγνωρίζει τη σημασία που έχουν οι προκαθορισμένες (default) επιλογές/ρυθμίσεις σε μία επεξεργασία, οι οποίες θα πρέπει να είναι οι πιο φιλικές προς την ιδιωτικότητα. Η υποχρέωση αυτή γίνεται πιο εύκολα κατανοητή αν την αναλογιστούμε στο πλαίσιο επεξεργασιών δεδομένων οι οποίες πραγματοποιούνται μέσω κάποιου λογισμικού ή κάποιας διαδικτυακής υπηρεσίας (όπου και στις δύο περιπτώσεις κάποιες ρυθμίσεις που αφορούν επεξεργασία προσωπικών δεδομένων μπορεί να είναι προεπιλεγμένες). Για παράδειγμα, μία υπηρεσία κοινωνικού δικτύου μπορεί να παρέχει τη δυνατότητα σε εγγεγραμμένους χρήστες να έχουν το προφίλ τους είτε δημόσια προσβάσιμο είτε «κλειστό» σε συγκεκριμένο κύκλο ατόμων (π.χ. στους «φίλους»): η προεπιλεγμένη ρύθμιση στην εν λόγω περίπτωση πρέπει να είναι η δεύτερη έτσι ώστε, αν ο χρήστης δεν το ζητήσει ρητώς, το προφίλ του να μην είναι «ανοικτό» προς όλους.

**Παράδειγμα:** Δήμος αναπτύσσει «έξυπνη» εφαρμογή (smart app) που μπορούν να εγκαταστήσουν οι δημότες προκειμένου να λαμβάνουν, μέσω ειδοποιήσεων της εφαρμογής, νέα που αφορούν το Δήμο. Επίσης, η εφαρμογή δίνει τη δυνατότητα να εντοπίζει ο χρήστης σημεία ενδιαφέροντος στη περιοχή που βρίσκεται (όπως πρατήρια υγρών καυσίμων, εστιατόρια κτλ.). Για τον εντοπισμό σημείων ενδιαφέροντος, ο χρήστης πρέπει να ενεργοποιήσει την λειτουργία GPS, επιτρέποντας στην εφαρμογή να εντοπίζει πού ακριβώς βρίσκεται.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Δεδομένου ότι ένας χρήστης μπορεί να μην επιθυμεί να ενεργοποιήσει αυτή τη δυνατότητα εντοπισμού σημείων ενδιαφέροντος, η εφαρμογή πρέπει να υλοποιηθεί κατά τρόπο τέτοιο ώστε να μην ζητά εξ ορισμού πρόσβαση σε δεδομένα τοποθεσίας: η πρόσβαση πρέπει να αποκτάται όταν ο χρήστης την επιτρέπει στο πλαίσιο αξιοποίησης της υπηρεσίας εντοπισμού σημείων ενδιαφέροντος και μόνο.

Γενικότερα, η εύρεση των βέλτιστων προκαθορισμένων ρυθμίσεων προς την ιδιωτικότητα δεν είναι πάντα προφανής: μία καλή πηγή αποτελεί η σχετική αναφορά του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA) [48].

### 8.1.3 Αφορούν μόνο υπευθύνους επεξεργασίας;

Οι προαναφερθείσες υποχρεώσεις του άρθρου 25 αφορούν υπευθύνους επεξεργασίας, καθώς και κάθε πράξη επεξεργασίας. Στην αιτιολογική σκέψη 78 του ΓΚΠΔ παρέχεται μεγαλύτερη επεξήγηση/ανάλυση:

*«Η προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα απαιτεί τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε να διασφαλίζεται ότι τηρούνται οι απαιτήσεις του παρόντος κανονισμού. Προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται ειδικότερα στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Τέτοια μέτρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα το συντομότερο δυνατόν, τη διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφάλειας».*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ωστόσο, αν και δεν αποτελούν υποχρεώσεις για εκτελούντες την επεξεργασία, καθίσταται σαφές ότι κάθε εκτελών θα πρέπει να λαμβάνει υπόψη του τις άνω αρχές, ιδίως αν παρέχει υπηρεσίες/πλατφόρμες σε υπευθύνους επεξεργασίας. Ακόμα περισσότερο, το ίδιο ισχύει και για όσους αναπτύσσουν εφαρμογές/προϊόντα τα οποία θα διατεθούν σε υπευθύνους επεξεργασίας: αν και τα εν λόγω πρόσωπα (π.χ. εταιρείες ανάπτυξης λογισμικού) δεν αποτελούν ούτε υπευθύνους επεξεργασίας ούτε εκτελούντες, οπότε δεν υπόκεινται στο ΓΚΠΔ, εν τούτοις ο ρόλος τους είναι κρίσιμος. Αυτό αναγνωρίζεται επίσης στην εισαγωγική σκέψη 78 του ΓΚΠΔ, που επιπροσθέτως στα προηγούμενα αναφέρει τα εξής:

*«Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των τελευταίων εξελίξεων, να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων».*

☞ Άξιο αναφοράς επίσης είναι ότι στη Γνώμη 5/2018 του Ευρωπαίου Επόπτη Προστασίας Δεδομένων [49] γίνεται ειδική αναφορά στη σημασία της εκπλήρωσης της υποχρέωσης της προστασίας δεδομένων ήδη από το σχεδιασμό και εξ ορισμού ειδικά για δημόσιους φορείς. Συγκεκριμένα, αναφέρεται το εξής: **"***Article 25 applies to all types of organisations acting as controllers, including public administrations, which, considering their role to serve the public good, should give the example in protecting individuals' fundamental rights and freedoms***"**. Συναφώς, στην Εισαγωγική Σκέψη 78 του ΓΚΠΔ, γίνεται ρητή αναφορά ως προς το ότι ***οι αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού θα πρέπει επίσης να λαμβάνονται υπόψη στο πλαίσιο των δημόσιων διαγωνισμών***.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 8.2 Αρχείο δραστηριοτήτων επεξεργασίας

Στο άρθρο 30 του ΓΚΠΔ προβλέπεται η υποχρέωση καταγραφής όλων των ειδών των επεξεργασιών προσωπικών δεδομένων που πραγματοποιεί ένας υπεύθυνος επεξεργασίας. Η ίδια υποχρέωση ισχύει και για εκτελούντες την επεξεργασία. Τα σχετικά αρχεία που οφείλουν να τηρούν εγγράφως, μεταξύ άλλων σε ηλεκτρονική μορφή, οι εκάστοτε φορείς (υπεύθυνοι επεξεργασίας / εκτελούντες την επεξεργασία) ονομάζονται *αρχεία δραστηριοτήτων επεξεργασίας*.

**Ποιους αφορά;**

Σύμφωνα με το άρθρο 30 παρ. 5, αφορά κάθε υπεύθυνο επεξεργασίας και κάθε εκτελούντα την επεξεργασία που απασχολεί περισσότερους από 250 υπαλλήλους. Ωστόσο, και για περιπτώσεις με μικρότερους από 250 υπαλλήλους υφίσταται ως υποχρέωση, εφόσον:

- Η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, ή
- Η επεξεργασία δεν είναι περιστασιακή (π.χ. μισθοδοσία υπαλλήλων) ή
- Η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων κατά το άρθρο 9 παράγραφος 1 ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

Άρα, ουσιαστικά, στη συντριπτική πλειοψηφία των οργανισμών, η τήρηση αρχείων δραστηριοτήτων επεξεργασίας είναι υποχρεωτική, αφού κατά κανόνα συντρέχει πάντα μία εκ των ανωτέρω εξαιρέσεων - ακόμα και για οργανισμούς με ολιγάριθμο προσωπικό (βλ. [50]).

☞ Πρακτικά, όλοι οι Δημόσιοι Φορείς εμπίπτουν στην υποχρέωση τήρησης αρχείων δραστηριοτήτων.

**Τι περιλαμβάνει;**

Ένα αρχείο δραστηριοτήτων για **υπεύθυνο επεξεργασίας** περιλαμβάνει τα εξής, σύμφωνα με το άρθρο 30 παρ. 1:

α) Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων (βλ. συνέχεια),

β) τους σκοπούς της επεξεργασίας,

γ) περιγραφή των κατηγοριών των υποκειμένων των δεδομένων και των κατηγοριών των δεδομένων προσωπικού χαρακτήρα,

δ) τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,

ε) όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων κατά παρέκκλιση (με βάση το άρθρο 49 παράγραφος 1 δεύτερο εδάφιο), της τεκμηρίωσης των κατάλληλων εγγυήσεων,

στ) όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων,

ζ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος 1 του ΓΚΠΔ.

Ένα αρχείο δραστηριοτήτων για **εκτελούντα την επεξεργασία** περιλαμβάνει τα εξής, σύμφωνα με το άρθρο 30 παρ. 2:

α) το όνομα και τα στοιχεία επικοινωνίας του εκτελούντος ή των εκτελούντων την επεξεργασία και των υπευθύνων επεξεργασίας εκ μέρους των οποίων ενεργεί ο εκτελών και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, καθώς και του υπευθύνου προστασίας δεδομένων,

β) τις κατηγορίες επεξεργασιών που διεξάγονται εκ μέρους κάθε υπευθύνου επεξεργασίας,

γ) όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, με τον ίδιο τρόπο όπως και για τον υπεύθυνο επεξεργασίας,

δ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος 1 του ΓΚΠΔ.

**Πώς δημιουργείται (μορφότυπο κτλ.);**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ένα αρχείο δραστηριοτήτων δεν απαιτείται να ακολουθεί κάποιο συγκεκριμένο μορφότυπο. Η ιστοσελίδα της Αρχής παρέχει κάποια ενδεικτικά πρότυπα (templates) σε μορφή λογιστικού φύλλου. Αυτά περιγράφονται στην Εικόνα 1 (όσον αφορά τα εισαγωγικά στοιχεία) και στην Εικόνα 2 (όσον αφορά την καταγραφή των δραστηριοτήτων επεξεργασίας): τα εν λόγω πρότυπα στις δύο Εικόνες αφορούν στην περίπτωση υπευθύνου επεξεργασίας, αλλά αντίστοιχα πρότυπα διατίθενται στην ιστοσελίδα της Αρχής και για εκτελούντες την επεξεργασία. Αξίζει να ανατρέξει κανείς στην ιστοσελίδα της Αρχής για τα πρότυπα αυτά και για τις δύο περιπτώσεις, διότι η Αρχή «προτείνει» και πρόσθετες πληροφορίες που θα μπορούσαν να ενταχθούν σε ένα αρχείο δραστηριοτήτων, οι οποίες – αν και δεν επιβάλλονται από το ΓΚΠΔ – βοηθούν σημαντικά στην αποτελεσματική καταγραφή των διαφόρων πτυχών της επεξεργασίας.

**Παράδειγμα:** Σε ένα Δημόσιο φορέα, οι τυπικές περιπτώσεις (σκοποί) επεξεργασιών που αναμένεται, κατ' ελάχιστο, να καταγραφούν σε ένα αρχείο δραστηριοτήτων επεξεργασίας είναι: α) Μισθοδοσία προσωπικού, β) Εκπαίδευση προσωπικού, γ) Αξιολόγηση προσωπικού, δ) Ασφάλιση προσωπικού, ε) Διαχείριση δεδομένων υποψηφίων εργαζομένων, στ) Διαχείριση προμηθευτών, ζ) Αιτήσεις πολιτών. Από εκεί και ύστερα, άλλοι πιθανοί σκοποί είναι: η) Προστασία προσώπων και αγαθών (περίπτωση χρήσης καμερών για ασφάλεια), θ) αποστολή ενημερωτικών δελτίων (newsletters), ι) Ασφάλεια ιστοσελίδας.

Για κάθε έναν εκ των ανωτέρω σκοπών, εφόσον πράγματι εμπίπτουν στις επεξεργασίες δεδομένων που πραγματοποιεί ο φορέας, θα πρέπει να καταγραφούν οι κατηγορίες των υποκειμένων των δεδομένων που αφορά η επεξεργασία (π.χ. εργαζόμενοι, εισερχόμενοι στο χώρο, επισκέπτες ιστοσελίδας κτλ.), το είδος των δεδομένων (π.χ. Αριθμός Αστυνομικής ταυτότητας, ονοματεπώνυμο, ταχυδρομική διεύθυνση, ηλεκτρονική διεύθυνση, Αριθμός Φορολογικού Μητρώου, δεδομένα εικόνας από κάμερα, διεύθυνση δικτύου (IP) συσκευής χρήστη κ.α.), εάν γίνονται διαβιβάσεις σε χώρα ή οργανισμό εκτός ΕΕ, ο χρόνος τήρησης των δεδομένων, καθώς και μία γενική περιγραφή των μέτρων ασφάλειας.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

| | A | B |
|---|---|---|
| 1 | | |
| 2 | **1. Όνομα και στοιχεία επικοινωνίας Υπεύθυνου Επεξεργασίας** | |
| 3 | Επωνυμία/Ονοματεπώνυμο | |
| 4 | Αριθμός ΓΕΜΗ (αν υπάρχει) | |
| 5 | ΑΦΜ | |
| 6 | Ηλεκτρονική Διεύθυνση | |
| 7 | Τηλέφωνο | |
| 8 | Ταχυδρομική Διεύθυνση | |
| 9 | | |
| 10 | **2. Όνομα και στοιχεία επικοινωνίας Εκπροσώπου του Υπευθύνου Επεξεργασίας** | |
| 11 | Επωνυμία/Ονοματεπώνυμο | |
| 12 | ΑΦΜ | |
| 13 | Ηλεκτρονική Διεύθυνση | |
| 14 | Τηλέφωνο | |
| 15 | Ταχυδρομική Διεύθυνση | |
| 16 | | |
| 17 | **3. Όνομα και στοιχεία επικοινωνίας Υπευθύνου Προστασίας Δεδομένων** | |
| 18 | Ονοματεπώνυμο | |
| 19 | Ηλεκτρονική Διεύθυνση | |
| 20 | Τηλέφωνο | |
| 21 | Ταχυδρομική Διεύθυνση | |
| 22 | | |
| 23 | **4. Όνομα και στοιχεία επικοινωνίας από κοινού Υπευθύνου Επεξεργασίας** | |
| 24 | Από κοινού Δραστηριότητες επεξεργασίας | |
| 25 | Επωνυμία/Ονοματεπώνυμο | |
| 26 | Αριθμός ΓΕΜΗ (αν υπάρχει) | |
| 27 | ΑΦΜ | |
| 28 | Ηλεκτρονική Διεύθυνση | |
| 29 | Τηλέφωνο | |
| 30 | Ταχυδρομική Διεύθυνση | |

**Εικόνα 1 - Πρότυπο (template) για τα εισαγωγικά στοιχεία ενός αρχείου δραστηριοτήτων επεξεργασίας**

| | A | C | E | F | H | I | L | N | P |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Αρχείο Δραστηριοτήτων Επεξεργασίας (Άρ. 30 του Κανονισμού (ΕΕ) 679/2016) | | | | | | | | |
| 2 | | Βασικά χαρακτηριστικά της επεξεργασίας | | | | | Διαβιβάσεις σε χώρες/οργανισμούς εκτός Ε.Ε. | | Τεχνικά και οργανωτικά χαρακτηριστικά |
| 3 | Α/Α | Σκοπός επεξεργασίας | Κατηγορίες υποκειμένων των δεδομένων | Κατηγορίες δεδομένων προσωπικού χαρακτήρα | Κατηγορίες αποδεκτών | Προβλεπόμενες προθεσμίες διαγραφής (όπου είναι δυνατό) | Τρίτες χώρες ή διεθνείς οργανισμοί στους οποίους θα διαβιβαστούν τα δεδομένα (εφόσον υπάρχουν) | Τεκμηρίωση εγγυήσεων για τις διαβιβάσεις σε τρίτες χώρες ή διεθνείς οργανισμούς (εφόσον πραγματοποιείται διαβίβαση σύμφωνα με το άρ. 49 παρ. 1 β' εδαφ. του Κανονισμού) | Γενική περιγραφή οργανωτικών και τεχνικών μέτρων ασφάλειας (όπου είναι δυνατό) |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | | | | | | | | | |
| 7 | | | | | | | | | |
| 8 | | | | | | | | | |

**Εικόνα 2 – Πρότυπο (template) για την καταγραφή επεξεργασιών προσωπικών δεδομένων σε ένα αρχείο δραστηριοτήτων επεξεργασίας**

**Ερώτηση δραστηριότητας**: Ένα αρχείο δραστηριοτήτων επεξεργασίας ενός υπευθύνου επεξεργασίας ή ενός εκτελούντος την επεξεργασία περιέχει δεδομένα προσωπικού χαρακτήρα; Αν ναι, τι είδους;

## 8.3 Βιβλιογραφία για περισσότερη μελέτη


1. ENISA, “Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default”, Jan. 2019. Διαθέσιμο στο **https://www.enisa.europa.eu/publications/recommendations-**




Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**on-shaping-technology-according-to-gdpr-provisions-part-2**

2. European Data Protection Board, “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”. Διαθέσιμο στο **https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_el** (και στα ελληνικά)
3. European Data Protection Supervisor, “Opinion 5/2018 on privacy by design”. Διαθέσιμο στο **https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 9. Υποχρεώσεις: Υπεύθυνος Προστασίας Δεδομένων

Μία εκ των νέων υποχρεώσεων, τόσο για υπευθύνους επεξεργασίας, όσο και για εκτελούντες την επεξεργασία, που εισάγει ο ΓΚΠΔ (στο άρθρο 37) και εντάσσεται σε αυτές που αποκαλούνται «εργαλεία λογοδοσίας» είναι ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ) – για τον οποίο είθισται να χρησιμοποιείται στην καθομιλουμένη και ο πρωτότυπος από το αρχικό κείμενο όρος «Data Protection Officer» ή «DPO». Ο ΥΠΔ είναι ένα πρόσωπο[32], είτε μέλος του προσωπικού του φορέα είτε εξωτερικός βάσει σύμβασης παροχής υπηρεσιών, ο οποίος μεταξύ άλλων έχει τα εξής καθήκοντα (βλ. άρθρο 39 του ΓΚΠΔ):

α) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται προσωπικά δεδομένα, σχετικά με τις υποχρεώσεις τους που απορρέουν από το ΓΚΠΔ αλλά και από άλλες διατάξεις σχετικά με την προστασία δεδομένων,

β) παρακολουθεί τη συμμόρφωση με το ΓΚΠΔ και με άλλες διατάξεις, εθνικές ή ευρωπαϊκές, σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,

γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της (βλ. σχετικώς την Ενότητα 10) ,

δ) συνεργάζεται με την εποπτική Αρχή,

ε) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης (βλ. σχετικώς την Ενότητα 10), και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Ο ρόλος του ΥΠΔ είναι πολύ σημαντικός και ουσιαστικός, γιατί - όπως προκύπτει

[32] Μπορεί να συνεπικουρείται και από ομάδα ατόμων, όπως περιγράφεται στη συνέχεια



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

και από τα ανωτέρω - είναι αυτός που, μεταξύ άλλων, θα προτείνει κατευθύνσεις και τυχόν διορθωτικά μέτρα εντός του οργανισμού, αναφορικά με ζητήματα προστασίας προσωπικών δεδομένων και συμμόρφωσης με τις συναφείς υποχρεώσεις (και ως εκ τούτου πρέπει να διαθέτει τα κατάλληλα προσόντα, όπως αναλύονται στη συνέχεια). Ωστόσο, **ο ρόλος του είναι αμιγώς συμβουλευτικός και όχι αποφασιστικός**: η ευθύνη της συμμόρφωσης με το δίκαιο περί προστασίας των δεδομένων έγκειται αποκλειστικά, αναλόγως την περίπτωση, στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία. Για την ακριβή θέση του ΥΠΔ εντός του οργανισμού, καθώς σε τι αυτό μεταφράζεται αναφορικά με τις ενέργειες που οφείλει να κάνει ο εκάστοτε φορέας για τη ορθή αξιοποίηση του ΥΠΔ, περισσότερα στοιχεία δίνονται στη συνέχεια.

## 9.1 Ποιος υποχρεούται να θεσπίσει ΥΠΔ

Σύμφωνα με το άρθρο 37 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία οφείλουν να ορίσουν ΥΠΔ εφόσον συντρέχει μία εκ των ακόλουθων προϋποθέσεων:

α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας, ή

β) οι βασικές δραστηριότητες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή

γ) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

☞ Όλοι οι Δημόσιοι Φορείς εμπίπτουν στην υποχρέωση ορισμού ΥΠΔ. Για πολλές δημόσιες αρχές ή δημόσιους φορείς, μπορεί να ορίζεται ένας μόνο ΥΠΔ, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους (βλ. άρθρο



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

37 παρ. 3).

## 9.2 Προσόντα του ΥΠΔ

Ένας ΥΠΔ θα πρέπει να ορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, σε συνάρτηση και με τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας (βλ. άρθρο 37 παρ. 5 του ΓΚΠΔ, σε συνδυασμό με το άρθρο 39 παρ. 2). Για παράδειγμα, όταν μια δραστηριότητα επεξεργασίας δεδομένων είναι ιδιαίτερα πολύπλοκη, ή όταν εμπλέκεται μεγάλος όγκος ευαίσθητων δεδομένων, ο ΥΠΔ είναι πιθανό να χρειάζεται υψηλότερο επίπεδο εμπειρογνωμοσύνης και υποστήριξης [51].

Σε κάθε περίπτωση, ο ΥΠΔ πρέπει να διαθέτει, μεταξύ άλλων, τις ακόλουθες δεξιότητες και εμπειρογνωμοσύνη:

- εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, καθώς και άριστη γνώση του ΓΚΠΔ,
- γνώση των πράξεων επεξεργασίας που διενεργούνται,
- γνώση του τομέα των τεχνολογιών πληροφοριών και της ασφάλειας δεδομένων,
- γνώση του τομέα δραστηριότητας και του οργανισμού,
- ικανότητα ανάπτυξης νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού [51].

☞ Ο ΓΚΠΔ δεν θέτει κάποια απαίτηση πιστοποίησης ΥΠΔ.

Ειδικά για το Δημόσιο Τομέα, σκόπιμο είναι ο ΥΠΔ να διαθέτει καλή γνώση των διοικητικών κανόνων και διαδικασιών του φορέα.

☞ Ο ΥΠΔ μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις (π.χ. ένας



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

υπάλληλος μπορεί να συνεχίσει να ασκεί τα προηγούμενα καθήκοντά του και να αναλάβει να είναι ΥΠΔ). Ωστόσο, σε κάθε περίπτωση (όπως αναλύεται στη συνέχεια) ο φορέας πρέπει να διασφαλίζει ότι ο ΥΠΔ έχει τους κατάλληλος πόρους για την εκτέλεση των καθηκόντων του (συμπεριλαμβανομένων των χρονικών πόρων), ενώ επίσης τα λοιπά καθήκοντά του δεν πρέπει να συνεπάγονται σύγκρουση συμφερόντων.

## 9.3 Θέση του ΥΠΔ – Συναφείς υποχρεώσεις του φορέα

Ο ΥΠΔ πρέπει να μπορεί απρόσκοπτα να επιτελεί το έργο του, με ανεξάρτητο τρόπο. Σύμφωνα με το άρθρο 38 παρ. 3 του ΓΚΠΔ, ο φορέας του ΥΠΔ (είτε υπεύθυνος επεξεργασίας είτε εκτελών την επεξεργασία) οφείλει να διασφαλίζει τα εξής:
α) Ο ΥΠΔ δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του
β) Ο ΥΠΔ δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.
γ) Ο ΥΠΔ λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του φορέα.

Τα ανωτέρω είναι στενά συνυφασμένα με την ανεξαρτησία του ΥΠΔ. Πράγματι, για να είναι ουσιαστικός ο ρόλος του, οι ανωτέρω προϋποθέσεις πρέπει να τηρούνται στο ακέραιο (αν για παράδειγμα, ο ΥΠΔ εντοπίσει εντός του οργανισμού ότι μία επεξεργασία δεν συντελείται κατά τον ορθό τρόπο από τη σκοπιά της προστασίας προσωπικών δεδομένων, θα πρέπει να το επισημάνει ελεύθερα και να ληφθεί δεόντως υπόψη η επισήμανσή του). Με άλλα λόγια, κατά την επιτέλεση των καθηκόντων τους οι Υπεύθυνοι Προστασίας Δεδομένων απολαύουν αυτοτέλειας και ανεξαρτησίας.

☞ Η αυτοτέλεια και ανεξαρτησία των ΥΠΔ δεν είναι συμβατή με την υποστήριξη της νομιμότητας πράξεων επεξεργασίας προσωπικών δεδομένων από μέρους του υπευθύνου επεξεργασίας. Ως εκ τούτου, οι ΥΠΔ δεν μπορούν να εκπροσωπούν υπευθύνους επεξεργασίας σε ακροάσεις τους ενώπιον της Αρχής (βλ. σχετικά το



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

από 23/1/2020 δελτίο τύπου της Αρχής[33])

Από την πλευρά του φορέα (υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία), πρέπει να λαμβάνεται μέριμνα για την όσο το δυνατόν έγκαιρη συμμετοχή του ΥΠΔ σε όλα τα ζητήματα που σχετίζονται με την προστασία των δεδομένων και είναι καίριας σημασίας. Ως εκ τούτου, είναι σημαντικό ο ΥΠΔ να αντιμετωπίζεται ως συνομιλητής στους κόλπους του οργανισμού και να συμμετέχει στις ομάδες εργασίας που ασχολούνται με δραστηριότητες επεξεργασίας δεδομένων εντός του οργανισμού. Ενδεικτικά παραδείγματα ως προς το τι θα πρέπει να πράττει σχετικώς ο οργανισμός, σύμφωνα και με τα όσα προσδιορίζονται στο [51], είναι η τακτική κλήση του ΥΠΔ για συμμετοχή του στις συσκέψεις των ανώτερων και μεσαίων στελεχών της διοίκησης, να είναι παρών όταν λαμβάνονται αποφάσεις που έχουν επιπτώσεις στην προστασία δεδομένων και να του δίνονται εγκαίρως οι πληροφορίες που χρειάζεται προκειμένου να παράσχει κατάλληλες συμβουλές, καθώς επίσης και να δίνεται βαρύτητα στη γνώμη του: αυτό δεν σημαίνει ότι η γνώμη του δεσμεύει τη Διοίκηση, αλλά σε περίπτωση διαφωνίας, ως ορθή πρακτική συνιστάται να καταγράφονται οι λόγοι για τους οποίους δεν ακολουθήθηκαν οι συμβουλές του.

Κρίσιμο σημείο, που συνιστά υποχρέωση για τον οργανισμό, είναι να δίνονται οι απαραίτητοι πόροι στον ΥΠΔ. Ειδικότερα, σύμφωνα με το άρθρο 38 παρ. 2 του ΓΚΠΔ, ο οργανισμός στηρίζει τον Υπεύθυνο Προστασίας Δεδομένων «*παρέχοντας απαραίτητους πόρους για την άσκηση των καθηκόντων [του] και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του*». Στη χορήγηση των απαραίτητων πόρων θα πρέπει να συνυπολογίζονται και οι χρονικοί πόροι, το οποίο έχει ιδιαίτερη σημασία ιδίως όταν ο ΥΠΔ επιτελεί παράλληλα και άλλα καθήκοντα (π.χ. αν είναι υπάλληλος που διατηρεί και τις προηγούμενες αρμοδιότητες και υποχρεώσεις του από την υπαλληλική του σχέση). Όπως αναφέρεται στο [51], συνιστά ορθή πρακτική να ορίζεται συγκεκριμένο ποσοστό χρόνου ενασχόλησης με

[33] Διαθέσιμο στο **https://www.dpa.gr/el/enimerwtiko/deltia/deltio-typoy-shetika-me-tin-ekprosopisi-ton-ypeythynon-epexergasias-enopion-tis**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τα καθήκοντα του ΥΠΔ όταν δεν επιτελούνται υπό καθεστώς πλήρους απασχόλησης. Πέραν των χρονικών πόρων ωστόσο, ο οργανισμός οφείλει να στηρίζει τον ΥΠΔ και από πλευράς υποδομών, καθώς επίσης και να ανακοινωθεί ο ορισμός του σε όλο το προσωπικό, μαζί με τα καθήκοντά του, με τη συναφή υποχρέωση του λοιπού προσωπικού να συνδράμουν (όπως επιτρέποντας πρόσβαση, παρέχοντας πληροφόρηση κτλ.). Βεβαίως, ο οργανισμός θα πρέπει επίσης, να διευκολύνει τη συνεχή κατάρτιση του ΥΠΔ (π.χ. ενθάρρυνση για συμμετοχή σε σεμινάρια κατάρτισης).

☞ Αναλόγως του μεγέθους και της δομής του οργανισμού, μπορεί ενδεχομένως να απαιτείται η σύσταση ομάδας υπευθύνου προστασίας δεδομένων (να υπάρχει δηλαδή υπεύθυνος προστασίας δεδομένων ο οποίος να διοικεί δικό του προσωπικό). Σε τέτοιες περιπτώσεις, θα πρέπει να καθορίζεται με σαφήνεια η εσωτερική δομή της ομάδας, καθώς και τα καθήκοντα και οι αρμοδιότητες των επιμέρους μελών της [51].

## 9.4 Το ενδεχόμενο σύγκρουσης συμφερόντων

Στενά συνυφασμένη με την ανεξαρτησία του ΥΠΔ είναι η απαίτηση που θέτει το άρθρο 38 παρ. 6 του ΓΚΠΔ, σύμφωνα με την οποία, εφόσον ο ΥΠΔ επιτελεί ταυτόχρονα και άλλα καθήκοντα εντός του φορέα, «*ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζουν ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων*». Αυτό σημαίνει ιδίως, ότι ο ΥΠΔ δεν μπορεί να έχει, εκ των λοιπών αρμοδιοτήτων του, κάποια θέση εντός του οργανισμού η οποία του επιτρέπει να λαμβάνει αποφάσεις αναφορικά με επεξεργασία δεδομένων.

Όπως έχει επισημάνει και η Ο.Ε. του Άρθρου 29 [51], θέσεις στις οποίες εντοπίζονται συνήθως συγκρούσεις συμφερόντων στους κόλπους ενός οργανισμού είναι, μεταξύ άλλων, οι θέσεις της ανώτερης διοίκησης (όπως, διευθύνων σύμβουλος, διοικητικός γενικός διευθυντής, οικονομικός διευθυντής, αρχίατρος, προϊστάμενος τμήματος



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μάρκετινγκ, προϊστάμενος ανθρωπίνων πόρων ή προϊστάμενος τμήματος πληροφορικής), αλλά και άλλες θέσεις κατώτερων βαθμίδων της οργανωτικής δομής, εφόσον από τις θέσεις αυτές είναι δυνατός ο καθορισμός των σκοπών και των μέσων της επεξεργασίας. Ως εκ τούτου, αν ένας υπεύθυνος επεξεργασίας ορίσει ΥΠΔ ο οποίος κατέχει μία εκ των ανωτέρω θέσεων, δεν προκύπτει, κατ' αρχήν, εκπλήρωση της υποχρέωσης του άρθρου 38 του ΓΚΠΔ. Βέβαια, επειδή κάθε οργανισμός έχει διαφορετική οργανωτική δομή, το συγκεκριμένο ζήτημα θα πρέπει να εξετάζεται ανά περίπτωση.

**Παράδειγμα:** Ένας Δημόσιος φορέας διαθέτει ειδικό Τμήμα Ασφάλειας Δικτύων. Ο Προϊστάμενος αυτού είναι υπεύθυνος, διά του τμήματός του, για ζητήματα ασφάλειας δικτύου (διαχείριση κινδύνων ασφαλείας, ανίχνευση/αντιμετώπιση επιθέσεων ασφαλείας, έγκαιρη εισήγηση για προμήθεια εξοπλισμού για θέματα ασφάλειας κτλ.). Ο Προϊστάμενος, λόγω του ρόλου του, μπορεί αν χρειαστεί να έχει πρόσβαση σε οποιοδήποτε αρχείο καταγραφής (log file), προκειμένου να διερευνήσει ένα εικαζόμενο, βάσει ενδείξεων, περιστατικό.

Από τα ανωτέρω συνάδεται ότι ο εν λόγω Προϊστάμενος δεν θα πρέπει να αναλάβει ρόλο ΥΠΔ εντός του οργανισμού, λόγω σύγκρουσης συμφερόντων.

## 9.5 Δημοσιοποίηση στοιχείων ΥΠΔ

Τα στοιχεία του ΥΠΔ γνωστοποιούνται στην εποπτική Αρχή (άρθρο 37 παρ. 7 του ΓΚΠΔ). Επίσης, τα στοιχεία του αποτελούν τμήμα της ενημέρωσης που οφείλει να παρέχει ο υπεύθυνος επεξεργασίας προς τα υποκείμενα των δεδομένων, σύμφωνα με τα όσα ήδη είδαμε στην Ενότητα 6: όπως ρητά αναφέρει η ανωτέρω διάταξη, τα στοιχεία του πρέπει να δημοσιεύονται. Εξάλλου, όπως προβλέπεται και στο άρθρο 38 παρ. 4, «*τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους (…)*».

Τα στοιχεία επικοινωνίας του ΥΠΔ τα οποία δημοσιεύονται θα πρέπει να είναι τέτοια ώστε να διευκολύνεται η επικοινωνία των υποκειμένων των δεδομένων μαζί του



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

(ταχυδρομική διεύθυνση ή/και συγκεκριμένος τηλεφωνικός αριθμός ή/και συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου – τα οποία πρέπει να είναι λειτουργικά). Επισημαίνεται ότι, σύμφωνα με το άρθρο 37 παρ. 7 του ΓΚΠΔ, δεν απαιτείται η δημοσιοποίηση του ονόματος του ΥΠΔ (χωρίς βεβαίως να αποκλείεται, εφόσον ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κρίνει ανάλογα). **Βέβαια, η ανακοίνωση του ονόματος του ΥΠΔ στην εποπτική Αρχή είναι υποχρεωτική.**

☞ Πρέπει να αποσαφηνιστεί ότι η ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων είναι, όπως αναφέρθηκε και στην Ενότητα 6, υποχρέωση του υπεύθυνου επεξεργασίας και, ως εκ τούτου, δεν συνιστά υποχρέωση του ΥΠΔ. Ο ΥΠΔ μπορεί να διευκολύνει τα υποκείμενα των δεδομένων ως προς το να τους δώσει σχετικές πληροφορίες (π.χ. αν υπάρχουν απορίες, παρά την ενημέρωση που (οφείλει να) παρέχει ο οργανισμός, ως προς το πώς να ασκηθεί ένα δικαίωμα).

Επίσης, καλή πρακτική κατά την Ο.Ε του Άρθρου 29, είναι να γνωστοποιεί ο οργανισμός το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ στους υπαλλήλους του, δημοσιεύοντάς τα, για παράδειγμα, στο ενδοδίκτυό του, στον εσωτερικό τηλεφωνικό κατάλογο και στα οργανογράμματά του [51].

**Ερώτηση δραστηριότητας**: Με βάση την οργανωτική δομή του φορέα σας, κατονομάστε τρεις θέσεις για τις οποίες οι κάτοχοί τους δεν θα πρέπει να οριστούν ως ΥΠΔ.

**Ερώτηση δραστηριότητας**: Ένας δημόσιος οργανισμός καλείται να υπερασπιστεί τον εαυτό του ενώπιον δικαστηρίου αναφορικά με ζήτημα που άπτεται πιθανής παράνομης επεξεργασίας προσωπικών δεδομένων. Η Διοίκηση του οργανισμού αποφασίζει να αναλάβει την εκπροσώπησή του, ενώπιον του δικαστηρίου, ο ΥΠΔ (εσωτερικός του φορέα) που γνωρίζει πλήρως το νομικό πλαίσιο και είναι σε θέση να πείσει ότι ο οργανισμός ενήργησε όπως πρέπει.

α) Σχολιάστε σχετικά την ως άνω απόφαση του οργανισμού για την εκπροσώπησή



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

του.

β) Αν ο ΥΠΔ δεν είναι εσωτερικός αλλά εξωτερικός, θα άλλαζε κάτι στο ως άνω σχόλιό σας για την περίπτωση α);

**Ερώτηση δραστηριότητας**: Στην ιστοσελίδα δημόσιου φορέα, στο κείμενο ενημέρωσης προς τα υποκείμενα των δεδομένων αναφέρεται, ως προς τον ΥΠΔ, το εξής:

*Μπορείτε να επικοινωνείτε με τον Υπεύθυνο Προστασίας Δεδομένων του οργανισμού για κάθε ζήτημα σχετικό με την επεξεργασία των προσωπικών σας δεδομένων, στην ηλεκτρονική διεύθυνση* ***dpo@foreasA.gr***

Είναι συμβατή η εν λόγω ενημέρωση με τις σχετικές υποχρεώσεις του φορέα για δημοσιοποίηση των στοιχείων επικοινωνίας του ΥΠΔ;

## 9.6 Βιβλιογραφία για περισσότερη μελέτη


1. Working Party 29, "Guidelines on Data Protection Officer", 2017. Διαθέσιμο στο **https://ec.europa.eu/newsroom/article29/items/612048/en** (και στα ελληνικά)
2. T4DATA, «The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation", 2019. Διαθέσιμο στο **https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf** (περιέχει χρήσιμο υλικό και για άλλες ενότητες)




Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 10. Υποχρεώσεις τεχνικού και οργανωτικού χαρακτήρα

Το άρθρο 24 του ΓΚΠΔ περιγράφει το γενικό πλαίσιο για τις υποχρεώσεις τεχνικού και οργανωτικού χαρακτήρα για τον υπεύθυνο επεξεργασίας. Ειδικότερα, σύμφωνα με την παρ. 1 αυτού:

*«Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο».*

Οι κίνδυνοι προσδιορίζονται ιδίως με βάση τη σοβαρότητα των συνεπειών που θα ανακύψουν για τα θιγόμενα πρόσωπα αλλά και την πιθανότητα επέλευσής τους: τόσο η σοβαρότητα όσο και η πιθανότητα επέλευσης προσδιορίζονται με τη σειρά τους σε συνάρτηση με τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας. Τέτοιοι κίνδυνοι για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων ανακύπτουν όταν (βλ. και αιτιολογική σκέψη 75 του ΓΚΠΔ):

i) υπάρχει ενδεχόμενο σωματικής, υλικής ή μη υλικής βλάβης για τα υποκείμενα των δεδομένων, ιδίως όταν η επεξεργασία μπορεί να οδηγήσει σε διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, βλάβη φήμης, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο, παράνομη άρση της ψευδωνυμοποίησης, ή οποιαδήποτε άλλη σημαντική οικονομική ή κοινωνική ζημιά

ii) τα υποκείμενα των δεδομένων θα μπορούσαν να στερηθούν των δικαιωμάτων και ελευθεριών τους ή να εμποδίζονται από την άσκηση ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα

iii) υπόκεινται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα και γίνεται επεξεργασία γενετικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα,
iv) αξιολογούνται προσωπικές πτυχές, ιδίως όταν επιχειρείται ανάλυση ή πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή μετακινήσεις, προκειμένου να δημιουργηθούν ή να χρησιμοποιηθούν προσωπικά προφίλ,
v) υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα ευάλωτων φυσικών προσώπων, ιδίως παιδιών,
vi) η επεξεργασία περιλαμβάνει μεγάλη ποσότητα δεδομένων προσωπικού χαρακτήρα και επηρεάζει μεγάλο αριθμό υποκειμένων των δεδομένων.

Στο ίδιο άρθρο αναφέρεται ότι τα ως άνω αναφερόμενα οργανωτικά και τεχνικά μέτρα μπορούν να περιλαμβάνουν, όταν δικαιολογείται σε σχέση με τις δραστηριότητες επεξεργασίας, την εφαρμογή κατάλληλων πολιτικών για την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας.

Επί της ουσίας, ο ΓΚΠΔ θέτει ως γενική υποχρέωση στον υπεύθυνο επεξεργασίας, να υλοποιεί μία συστηματική προσέγγιση προκειμένου να διασφαλίζει τη νόμιμη επεξεργασία προσωπικών δεδομένων, υπό το φως των πιθανών κινδύνων που ανακύπτουν για κάθε περίπτωση οι οποίοι πρέπει να εντοπίζονται και να αξιολογούνται, έτσι ώστε να λαμβάνονται τεκμηριωμένα τα κατάλληλα μέτρα αντιμετώπισής τους.
Στο υπόλοιπο μέρος της Ενότητας αυτής αναλύονται επιμέρους υποχρεώσεις προς εκπλήρωση της ως άνω αναφερόμενης γενικότερης υποχρέωσης του άρθρου 24. Όπως θα περιγραφεί στη συνέχεια, κάποιες εκ των ειδικών αυτών υποχρεώσεων αφορούν και εκτελούντες την επεξεργασία.

## 10.1 Οργανωτικά και τεχνικά μέτρα ασφάλειας

Η έννοια της ασφάλειας των προσωπικών δεδομένων είναι ιδιαίτερα σημαντική, όπως



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ήδη είδαμε αρχικά και στην Ενότητα 4 όπου η εμπιστευτικότητα και η ακεραιότητα των δεδομένων αποτελούν μία εκ των θεμελιωδών προϋποθέσεων για τη νόμιμη επεξεργασία τους.

Η σχετική υποχρέωση του υπευθύνου επεξεργασίας, αλλά και του εκτελούντος την επεξεργασία, προσδιορίζεται στο άρθρο 32 του ΓΚΠΔ, όπου στην παρ. 1 αυτού αναφέρεται ότι:

*«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:*

*α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,*

*β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,*

*γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,*

*δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.»*

Ουσιαστικά, ο ΓΚΠΔ θέτει ως υποχρέωση στον υπεύθυνο επεξεργασίας, αλλά και στον εκτελούντα την επεξεργασία, να πραγματοποιεί μία ανάλυση και διαχείριση κινδύνων αναφορικά με την ασφάλεια της επεξεργασίας, προκειμένου να λάβει τεκμηριωμένα τις κατάλληλες αποφάσεις για το ποια οργανωτικά και τεχνικά μέτρα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ασφάλειας θα πρέπει να υλοποιηθούν[34]. Οι κίνδυνοι ασφάλειας, οι οποίοι πρέπει να αξιολογούνται στο πλαίσιο της διαχείρισης κινδύνων, απορρέουν ιδίως από το ενδεχόμενο τυχαίας ή παράνομης καταστροφής, απώλειας, αλλοίωσης, άνευ αδείας κοινολόγησης ή προσπέλασης δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Και στην περίπτωση των κινδύνων ασφάλειας, αυτοί προσδιορίζονται ιδίως με βάση τη σοβαρότητα των συνεπειών που θα ανακύψουν για τα θιγόμενα πρόσωπα αλλά και την πιθανότητα επέλευσής τους: για παράδειγμα, μεγαλύτερος κίνδυνος υπάρχει για τη διαρροή δεδομένων υγείας Δημοτών από ό,τι από τη διαρροή διευθύνσεων ηλεκτρονικού ταχυδρομείου Δημοτών (η σοβαρότητα είναι σαφώς υψηλότερη στην πρώτη περίπτωση), ενώ αντίστοιχα μεγαλύτεροι κίνδυνοι υπάρχουν για μία επεξεργασία επί μίας βάσης δεδομένων η οποία είναι προσπελάσιμη μέσω Διαδικτύου από ό,τι επί μίας βάσης δεδομένων η οποία δεν είναι προσπελάσιμη μέσω Διαδικτύου (η πιθανότητα κακόβουλης πρόσβασης στην βάση είναι σαφώς υψηλότερη στην πρώτη περίπτωση).

Τα οργανωτικά και τεχνικά μέτρα ασφάλειας των προσωπικών δεδομένων αποσκοπούν στην επίτευξη των κάτωθι στόχων[35]:

1) **Εμπιστευτικότητα** (Confidentiality): Τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
2) **Ακεραιότητα** (Integrity): Τα δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
3) **Διαθεσιμότητα** (Availability): Τα δεδομένα πρέπει να είναι διαθέσιμα όποτε απαιτείται η χρήση τους.

**Παράδειγμα** (βασισμένο σε παράδειγμα από το [52], αλλά εμπλουτισμένο**):** Ένα παράδειγμα παραβίασης της εμπιστευτικότητας δεδομένων προσωπικού χαρακτήρα μπορεί να περιλαμβάνει την περίπτωση απώλειας ή κλοπής μιας συσκευής η οποία

[34] Ανάλυση οργανωτικών και τεχνικών μέτρων ασφάλειας δίνεται στην Ενότητα 15.
[35] Οι εν λόγω στόχοι αφορούν γενικότερα την ασφάλεια οποιουδήποτε είδους πληροφορίας – όχι μόνο προσωπικών δεδομένων. Ο ΓΚΠΔ βέβαια εστιάζει αποκλειστικά στα προσωπικά δεδομένα.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

περιέχει ένα αντίγραφο βάσης δεδομένων του υπευθύνου επεξεργασίας, η οποία περιέχει προσωπικά δεδομένα (π.χ. δεδομένα πολιτών που επεξεργάζεται ένα Υπουργείο). Ακόμα και αν δεν υπάρξει απώλεια ή κλοπή της βάσης, αλλά κάποιος μη εξουσιοδοτημένος χρήστης καταφέρει να αποκτήσει πρόσβαση και να λάβει αντίγραφο - είτε μερικό είτε πλήρες - αυτής, τότε πάλι υπάρχει απώλεια εμπιστευτικότητας (για παράδειγμα, μία τέτοια πρόσβαση μπορεί να αποκτηθεί μέσω διαδικτυακής επίθεσης, η οποία εκμεταλλεύτηκε κάποιο κενό ασφάλειας).

Ένα παράδειγμα παραβίασης ακεραιότητας μπορεί να περιλαμβάνει την περίπτωση όπου σε μία βάση δεδομένων με προσωπικά δεδομένα, κάποιος κακόβουλος χρήστης αλλοιώνει το περιεχόμενο κάποιων καταχωρήσεων.

Παραδείγματα απώλειας της διαθεσιμότητας περιλαμβάνουν περιπτώσεις όπου τα δεδομένα έχουν διαγραφεί είτε τυχαία είτε από μη εξουσιοδοτημένο πρόσωπο. Απώλεια της διαθεσιμότητας ενδέχεται επίσης να προκύψει όταν διαταράσσεται σε σημαντικό βαθμό η κανονική λειτουργία ενός οργανισμού, για παράδειγμα, λόγω διακοπής ρεύματος ή λόγω διαδικτυακής επίθεσης ασφαλείας, με αποτέλεσμα να καθίστανται, για κάποιο χρονικό διάστημα, μη διαθέσιμα τα δεδομένα προσωπικού χαρακτήρα. Απώλεια διαθεσιμότητας υπάρχει και αν «καταστραφεί» ένα αρχείο με προσωπικά δεδομένα, χωρίς δυνατότητα επανάκτησης (π.χ, «χτύπημα» του σκληρού δίσκου στον οποίο αυτά έχουν αποθηκευτεί ψηφιακά χωρίς να υπάρχει κανενός είδους αντίγραφο ασφαλείας ή καταστροφή έντυπων φακέλων από, π.χ., πλημμύρα, για τους οποίους δεν υπάρχουν αντίγραφα).

Ο ΓΚΠΔ δεν επιβάλλει συγκεκριμένα μέτρα ασφάλειας: γίνεται μεν μία ειδική αναφορά στην ψευδωνυμοποίηση και στην κρυπτογράφηση (οι οποίες περιγράφονται στη συνέχεια, ενώ περαιτέρω ανάλυσή τους θα ακολουθήσει στην Ενότητα 15), όχι όμως ως υποχρεωτικές αλλά ως ενδεδειγμένες προς εξέταση για την αναγκαιότητα υλοποίησής τους, υπό το πρίσμα της διαχείρισης κινδύνων ασφάλειας. Πράγματι, όπως προαναφέρθηκε, τα μέτρα ασφάλειας θα πρέπει να αποφασίζονται από τον κάθε οργανισμό (υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία) κατόπιν μίας προσεκτικής αποτίμησης κινδύνων, λαμβάνοντας υπόψη όλες τις παραμέτρους που



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

περιγράφει το άρθρο 32. Σε κάθε περίπτωση, η ασφάλεια αποτελεί μία συνεχή διαδικασία, αφού η αποτελεσματικότητα των μέτρων ασφάλειας πρέπει να επανα-αξιολογείται βάσει συστηματικής διαδικασίας: για παράδειγμα, νέες επιθέσεις ασφαλείας ανακύπτουν συνεχώς, οπότε πρέπει να αξιολογείται έγκαιρα η ανάγκη κατάλληλης επικαιροποίησης/αναβάθμισης των υπαρχόντων μέτρων ασφάλειας.

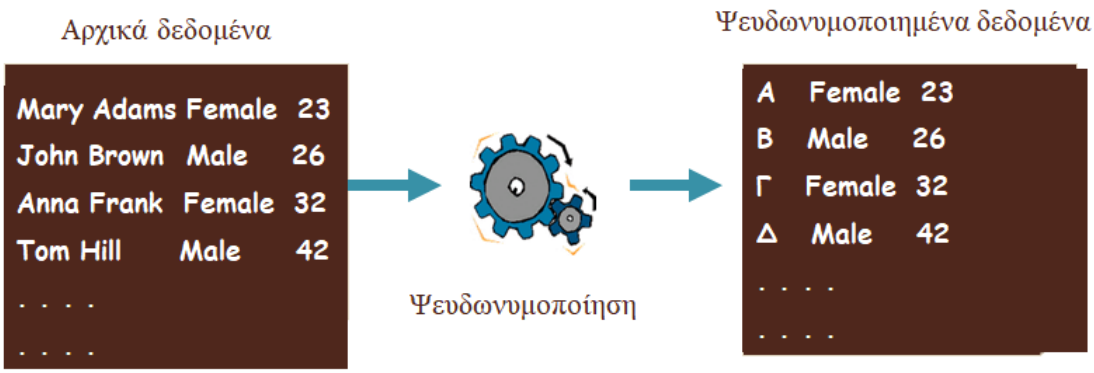
- ☞ Υπάρχουν διάφορες τυποποιημένες μεθοδολογίες διαχείρισης κινδύνων ασφάλειας, τις οποίες θα μπορούσε να εφαρμόσει ένας οργανισμός: ο ΓΚΠΔ δεν «υπαγορεύει» κάποια συγκεκριμένη.
- ☞ Επίσης, ο ΓΚΠΔ δεν επιβάλλει την λήψη κάποιας πιστοποίησης ασφάλειας (π.χ. ISO 27001). Αυτό δεν σημαίνει ότι δεν είναι χρήσιμο για έναν οργανισμό να προβεί στις απαραίτητες διαδικασίες έτσι ώστε να συμμορφώνεται με κάποιο διεθνώς αναγνωρισμένο πρότυπο ασφάλειας ή/και να λάβει πιστοποίηση προς τούτο. Ωστόσο, μία τέτοια πιστοποίηση δεν είναι υποχρεωτική, ενώ επίσης η τυχόν ύπαρξή της δεν αποτελεί από μόνη της πανάκεια ως προς τη συμμόρφωση του οργανισμού με τις υποχρεώσεις ασφάλειας που απορρέουν από το άρθρο 32 του ΓΚΠΔ.

### 10.1.1. Οι έννοιες της ψευδωνυμοποίησης και της κρυπτογράφησης

Η ψευδωνυμοποίηση ήταν ανέκαθεν γνωστή ως μία τεχνική «*αντικατάστασης των αναγνωριστικών στοιχείων ενός προσώπου με νέα αναγνωριστικά, τα οποία όμως δεν επιτρέπουν από μόνα τους την ταυτοποίηση του προσώπου*» [53]. Τα νέα αυτά αναγνωριστικά ονομάζονται *ψευδώνυμα*. Ίσως ο πιο απλός τρόπος να γίνει κατ' αρχάς κατανοητή η έννοια της ψευδωνυμοποίησης είναι το παράδειγμα στην Εικόνα 3, στην οποία μπορούμε να δούμε ότι τα πραγματικά ονοματεπώνυμα των υποκειμένων των δεδομένων (τα οποία σαφώς, σε συγκεκριμένο πλαίσιο, δύνανται να ταυτοποιήσουν επακριβώς τα φυσικά πρόσωπα) έχουν αντικατασταθεί από αναγνωριστικά άλλου τύπου (ψευδώνυμα) της μορφής Α, Β, Γ, Δ – εκ των οποίων δεν μπορεί κάποιος τρίτος να εντοπίσει σε ποια πρόσωπα αντιστοιχούν.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης




**Εικόνα 3 - Μία απλή περίπτωση ψευδωνυμοποίησης**

Το πρώτο – με βάση τη γνώση μας - νομικό κείμενο στο οποίο εισάγεται η έννοια της ψευδωνυμοποίησης είναι ο ΓΚΠΔ. Ειδικότερα, σύμφωνα με τον αντίστοιχο ορισμό στο άρθρο 4 του ΓΚΠΔ:

«*Ψευδωνυμοποίηση είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο*».

Άρα, σύμφωνα με το ΓΚΠΔ, η ψευδωνυμοποίηση είναι μία επεξεργασία που αποσκοπεί στην απόκρυψη της ταυτότητας των προσώπων – ωστόσο, η επαναταυτοποίηση μπορεί να καταστεί εφικτή, εφόσον αξιοποιηθούν *συμπληρωματικές πληροφορίες*, οι οποίες όμως πρέπει ακριβώς για αυτό να μην τηρούνται μαζί με τα ψευδωνυμοποιημένα δεδομένα και να προστατεύονται. Στο απλό παράδειγμα που περιγράφεται στην Εικόνα 3, οι συμπληρωματικές αυτές πληροφορίες είναι ο πίνακας αντιστοιχίσεων «Mary Adams ↔ A», «John Brown ↔ B» κ.ο.κ. – ο οποίος πράγματι πρέπει να προστατεύεται από αθέμιτες προσπελάσεις.

☞ Η ψευδωνυμοποίηση δεν είναι σημαντική μόνο για την ασφάλεια της επεξεργασίας. Είναι ως έννοια στενά συνυφασμένη με την αρχή της ελαχιστοποίησης των δεδομένων. Για παράδειγμα, όταν ο επιδιωκόμενος σκοπός



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επεξεργασίας μπορεί να επιτευχθεί με χρήση ψευδωνύμων αντί των πραγματικών αναγνωριστικών του χρήστη, τότε ουσιαστικά η ψευδωνυμοποίηση καθίσταται υποχρεωτική διότι διαφορετικά παραβιάζεται η αρχή της ελαχιστοποίησης των δεδομένων. Κάτι τέτοιο μπορεί να ισχύει ιδίως – αν και όχι αποκλειστικώς – σε περιπτώσεις επιστημονικής έρευνας (βλ. άρθρο 89 του ΓΚΠΔ – ενώ ειδική συζήτηση υπάρχει στην Ενότητα 14). Αυτός είναι και ο λόγος εξάλλου που γίνεται ειδική αναφορά στην ψευδωνυμοποίηση, όπως είδαμε, και στο άρθρο 25 του ΓΚΠΔ σχετικά με την προστασία των δεδομένων ήδη από το σχεδιασμό (βλ. Ενότητα 8). Μεγαλύτερη συζήτηση για την ψευδωνυμοποίηση, η οποία δύναται να επιτύχει διάφορους σκοπούς, παρατίθεται στην Ενότητα 15.

Αν και θα γίνει ειδικότερη ανάλυση στην Ενότητα 15, είναι σημαντικό να τονιστεί ήδη από αυτό το σημείο ότι **<u>τα ψευδωνυμοποιημένα δεδομένα εξακολουθούν να θεωρούνται δεδομένα προσωπικού χαρακτήρα</u>**. Χρήσιμες πηγές για την ψευδωνυμοποίηση είναι τα εγχειρίδια του ENISA [54], [55].

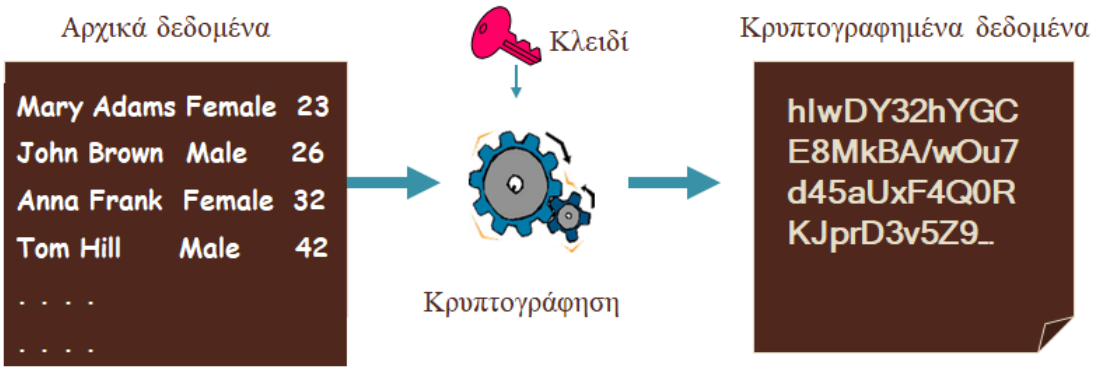
Η κρυπτογράφηση από την άλλη πλευρά είναι ο κατ' εξοχήν μηχανισμός για την προστασία της εμπιστευτικότητας των δεδομένων συνολικά. Και εδώ παραθέτουμε ένα αντίστοιχο απλό σχήμα (βλ. Εικόνα 4), στο οποίο φαίνεται ότι τα αρχικά προσωπικά δεδομένα έχουν μετατραπεί σε μία μη αναγνώσιμη, ακατάληπτη μορφή (κρυπτογραφημένα δεδομένα). Αυτό συντελέστηκε μέσω μίας διαδικασίας που λέγεται *αλγόριθμος κρυπτογράφησης*, στην οποία υπεισέρχεται και μία ποσότητα που είθισται να λέγεται *κλειδί κρυπτογράφησης* : εάν κρυπτογραφηθούν τα ίδια ακριβώς δεδομένα, με τον ίδιο ακριβώς αλγόριθμο κρυπτογράφησης αλλά με διαφορετικό κλειδί, θα προκύψουν διαφορετικά κρυπτογραφημένα δεδομένα. Η κρυπτογράφηση είναι αντιστρεπτή ως διαδικασία – δηλαδή, έχοντας το κρυπτογραφημένο κείμενο, μπορεί να ανακτηθεί το αρχικό – εφόσον είναι γνωστά τόσο το ποιος αλγόριθμος κρυπτογράφησης χρησιμοποιήθηκε[36] όσο και το κλειδί αποκρυπτογράφησης[37]. Η

[36] Πρέπει βέβαια να σημειωθεί ότι το ποιοι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται κάθε φορά δεν είναι μία πληροφορία που μένει μυστική – υπάρχουν συγκεκριμένα κρυπτογραφικά πρότυπα που χρησιμοποιούνται. Άρα, θεωρούμε ότι ένας επίδοξος υποκλοπέας έχει (και πράγματι έχει ή μπορεί εύκολα να έχει) γνώση του ποιος αλγόριθμος χρησιμοποιήθηκε.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ασφάλειά τους έγκειται στη μυστικότητα του κλειδιού αποκρυπτογράφησης – όσο αυτό δεν το γνωρίζει κάποιος, δεν μπορεί να ανακτήσει τα αρχικά δεδομένα (υπό την προϋπόθεση βέβαια ότι χρησιμοποιείται κρυπτογραφικός αλγόριθμος που είναι ασφαλής σε σχέση με την τρέχουσα, κάθε φορά, τεχνολογία).




**Εικόνα 4 - Μία απλή περίπτωση κρυπτογράφησης**

Θα πρέπει να σημειωθεί ότι η κρυπτογράφηση δύναται να επιτύχει και άλλους στόχους ασφάλειας, όπως την ακεραιότητα των δεδομένων (αφού υπάρχουν κρυπτογραφικές τεχνικές που επιτρέπουν, σε έναν νόμιμο αποδέκτη, να διαπιστώνει αν ένα αρχείο έχει αλλοιωθεί/τροποποιηθεί ή όχι), αλλά και την πιστοποίηση της ταυτότητας του δημιουργού ενός αρχείου ή/και του αποστολέα αυτού (για παράδειγμα, οι ψηφιακές υπογραφές δεν είναι τίποτα άλλο παρά εφαρμογή συγκεκριμένων τεχνικών κρυπτογραφίας). Το σύνολο των κρυπτογραφικών τεχνικών, με τα διάφορα οφέλη τους, εκφεύγουν προφανώς του αντικειμένου του παρόντος: περισσότερη συζήτηση θα γίνει στην Ενότητα 15, ενώ μία χρήσιμη πηγή, για όσους θέλουν να εμβαθύνουν, είναι η [56].

☞ Από τα ανωτέρω καθίσταται σαφές ότι η κρυπτογράφηση είναι διαφορετική της ψευδωνυμοποίησης και εν τέλει εξυπηρετεί, στη γενική περίπτωση, άλλους στόχους ασφάλειας: για παράδειγμα, δεν μπορεί να γίνει στατιστική ανάλυση επί

[37] Το κλειδί αποκρυπτογράφησης μπορεί να ταυτίζεται με το κλειδί κρυπτογράφησης (περίπτωση συμμετρικού κρυπτογραφικού αλγόριθμου) αλλά μπορεί και όχι (περίπτωση ασύμμετρου κρυπτογραφικού αλγόριθμου).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κρυπτογραφημένων δεδομένων[38], κάτι το οποίο δεν ισχύει για τα ψευδωνυμοποιημένα δεδομένα. Πάντως, υπάρχει μία συσχέτιση των δύο αυτών εννοιών υπό την έννοια ότι θα μπορούσε – ως μία εκ πολλών δυνατοτήτων προκειμένου να προκύψουν κατάλληλα ψευδωνυμοποιημένα δεδομένα - να χρησιμοποιηθεί κρυπτογραφικός αλγόριθμος για την επίτευξη ψευδωνυμοποίησης (βλ., π.χ. [54], [55]).

## 10.2 Διαχείριση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα

Ως παραβίαση δεδομένων προσωπικού χαρακτήρα ορίζεται, σύμφωνα με το άρθρο 4 του ΓΚΠΔ, ««*η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία*». Συνεπώς, κάθε τέτοια παραβίαση της ασφάλειας συνιστά περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα. Ουσιαστικά, εφόσον λάβει χώρα περιστατικό παραβίασης προσωπικών δεδομένων, έχει πληγεί τουλάχιστον ένας εκ των στόχων ασφάλειας – ήτοι εμπιστευτικότητα, ακεραιότητα ή/και διαθεσιμότητα. Ως εκ τούτου, όλα όσα αναφέρονται στο παράδειγμα της Ενότητας 10.1 αποτελούν ουσιαστικά, ανεξαιρέτως, παραδείγματα περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα.

Γενικότερα, η αποτελεσματική διαχείριση τέτοιων περιστατικών – δηλαδή η θέσπιση και υλοποίηση διαδικασιών για την αποτελεσματική και έγκαιρη αντιμετώπισή τους – αποτελεί ένα σημαντικό οργανωτικό μέτρο ασφάλειας (και, ως τέτοιο, θα μπορούσε να θεωρηθεί ότι η ανάγκη αποτελεσματικής τους διαχείρισης προκύπτει έμμεσα και από τις γενικές υποχρεώσεις ασφάλειας του προαναφερθέντος άρθρου 32). Ο ΓΚΠΔ ωστόσο προχωρά ένα βήμα περαιτέρω και θέτει πολύ συγκεκριμένες υποχρεώσεις για τους υπευθύνους επεξεργασίας αναφορικά με τη διαχείριση περιστατικών παραβίασης.

[38] Βέβαια, υπάρχουν προηγμένες τεχνικές κρυπτογράφησης που επιτρέπουν κάποιο σύνολο υπολογισμών επί κρυπτογραφημένων δεδομένων, και χωρίς τη γνώση του κλειδιού αποκρυπτογράφησης. Μία συζήτηση θα γίνει στην Ενότητα 15.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Συγκεκριμένα, σύμφωνα με τα όσα προδιαγράφονται στα άρθρα 33 και 34 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας έχει τις εξής υποχρεώσεις:

1) Μόλις λάβει γνώση του περιστατικού, οφείλει – εφόσον εκ του περιστατικού ενδέχεται να προκληθεί κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων – να υποβάλει γνωστοποίηση στην αρμόδια εποπτική αρχή[39] εντός 72 ωρών. Σε περίπτωση που η γνωστοποίηση υποβληθεί μετά την πάροδο 72 ωρών, τότε πρέπει να συνοδεύεται με τεκμηρίωση για την εν λόγω καθυστέρηση.
2) Εάν οι κίνδυνοι για τα θιγόμενα πρόσωπα είναι υψηλοί, τότε ο υπεύθυνος επεξεργασίας πρέπει τα ενημερώσει αμελλητί.
3) Σε κάθε περίπτωση (είτε συντρέχει κίνδυνος, ανεξαρτήτως έκτασης αυτού, είτε όχι), ο υπεύθυνος επεξεργασίας οφείλει να καταγράψει το περιστατικό εσωτερικά.

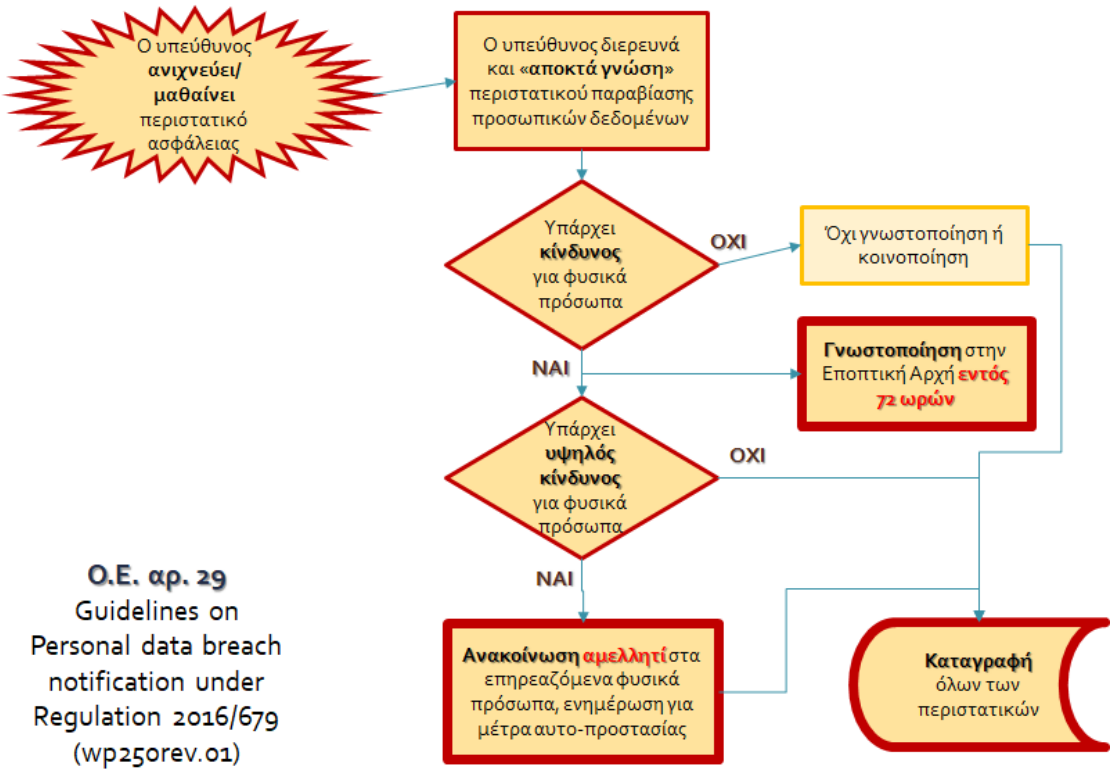
Πριν αναλύσουμε περαιτέρω το περιεχόμενο της ως άνω αναφερόμενης γνωστοποίησης του περιστατικού στην Αρχή, το περιεχόμενο της ενημέρωσης – όταν αυτή γίνεται – των θιγόμενων προσώπων, καθώς επίσης και το περιεχόμενο της εσωτερικής καταγραφής/τεκμηρίωσης που γίνεται για κάθε περιστατικό, θα πρέπει να δώσουμε έμφαση στο ότι, εκ των ανωτέρω υποχρεώσεων, συνάγεται ότι ο υπεύθυνος επεξεργασίας καλείται να κάνει πολύ γρήγορα μία στάθμιση/αξιολόγηση της σοβαρότητας των συνεπειών από το κάθε περιστατικό: η στάθμιση αυτή θα καθορίσει, τελικά, και τις ακριβείς του υποχρεώσεις. Μάλιστα, αναφορικά με την ενημέρωση των θιγόμενων προσώπων (όταν αυτή απαιτείται), παρόλο που δεν υπάρχει ρητή αναφορά σε χρονικό περιθώριο εντός του οποίου πρέπει να λαμβάνει χώρα, η φράση «αμελλητί» σημαίνει «το συντομότερο δυνατόν» - και, άρα, πρακτικά, αν κατά την υποβολή της γνωστοποίησης εντός 72 ωρών στην Αρχή έχουν ήδη αξιολογηθεί οι κίνδυνοι, από τον υπεύθυνο επεξεργασίας, ως υψηλοί, η ενημέρωση στα θιγόμενα πρόσωπα πρέπει να έχει προηγηθεί η να γίνει αμέσως μετά, χωρίς καθυστέρηση.

[39] Προφανώς, για περιστατικό παραβίασης δεδομένων φορέα του Δημόσιου Τομέα, η αρμόδια αρχή είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Οι ανωτέρω υποχρεώσεις περιγράφονται εύληπτα στο ακόλουθο σχήμα (βασισμένο στο [52]




**Σχήμα 1 - Διάγραμμα για τη διαδικασία αναφορικά με τη διαχείριση περιστατικών παραβίασης δεδομένων**

Το πνεύμα που διέπει τις διατάξεις των άρθρων 33 και 34 είναι η έμφαση που πρέπει να δίνει ο υπεύθυνος επεξεργασίας στο να κάνει αμέσως ενέργειες για την αποτελεσματική αντιμετώπιση των περιστατικών, προκειμένου να αμβλυνθούν οι συνέπειες από αυτό για τα επηρεαζόμενα πρόσωπα. Ουσιαστικά όμως, αναδεικνύει και την ανάγκη να διαθέτει ο υπεύθυνος επεξεργασίας διαδικασίες για τον έγκαιρο εντοπισμό τους. Σύμφωνα με την αιτιολογική σκέψη 87 του ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας θα πρέπει να έχουν ως γνώμονα ότι *θα πρέπει να μπορεί να εξακριβώνεται κατά πόσον έχουν τεθεί σε εφαρμογή όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων. Περαιτέρω, θα πρέπει να διαπιστώνεται ότι η κοινοποίηση πραγματοποιήθηκε χωρίς αδικαιολόγητη*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*καθυστέρηση, λαμβανομένων υπόψη ιδίως της φύσης και της σοβαρότητας της παραβίασης δεδομένων προσωπικού χαρακτήρα, καθώς και των συνεπειών και των δυσμενών αποτελεσμάτων της για το υποκείμενο των δεδομένων.*

**Τι πληροφορίες περιέχει μία γνωστοποίηση περιστατικού στην Αρχή**

Μία γνωστοποίηση περιστατικού στην Αρχή πρέπει να περιλαμβάνει τις κάτωθι πληροφορίες:

α) να περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα - π.χ.[40] απώλεια ή κλοπή συσκευής/εξοπλισμού, απώλεια ή κλοπή φυσικού αρχείου, ή τοποθέτησή του σε μη ασφαλές μέρος, απώλεια αλληλογραφίας ή ανάγνωση αυτής από μη εξουσιοδοτημένο παραλήπτη, επίθεση ασφαλείας (hacking), κακόβουλο λογισμικό (π.χ. ιός, ransomware), e-mail εξαπάτησης (phishing), όχι σωστή καταστροφή εγγράφων/αρχείων (είτε έντυπα είτε ηλεκτρονικά), δημοσίευση/κοινοποίηση δεδομένων εκ παραδρομής, επίδειξη/χορήγηση/διαβίβαση δεδομένων λάθος προσώπου κ.α.

Στην περιγραφή της φύσης του περιστατικού συμπεριλαμβάνονται, εάν είναι εφικτό, οι κατηγορίες των επηρεαζόμενων από το περιστατικό υποκειμένων των δεδομένων (π.χ. εργαζόμενοι, προμηθευτές, χρήστες διαδικτυακών υπηρεσιών, ασθενείς κτλ.) καθώς και – κατά προσέγγιση – το πλήθος τους, όπως επίσης οι κατηγορίες των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα, όπως και το – κατά προσέγγιση – πλήθος των αρχείων αυτών.

β) Το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες.

γ) Τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα. Το σκέλος αυτό σχετίζεται άμεσα με την προαναφερθείσα στάθμιση/αξιολόγηση που οφείλει να κάνει ο υπεύθυνος επεξεργασίας, ως προς το αν οι κίνδυνοι για τα επηρεαζόμενα πρόσωπα είναι υψηλοί (οπότε και θα πρέπει να ενημερωθούν). Στην Εικόνα 5 αποτυπώνονται οι διάφορες πτυχές που πρέπει να

[40] Τα ενδεικτικά παραδείγματα προέρχονται από τις οδηγίες του εντύπου γνωστοποίησης που παρέχει η Αρχή – βλ. σχετικώς το διαδικτυακό σύνδεσμο **https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis/upovoli_gnwstopoihshs_paraviashs**



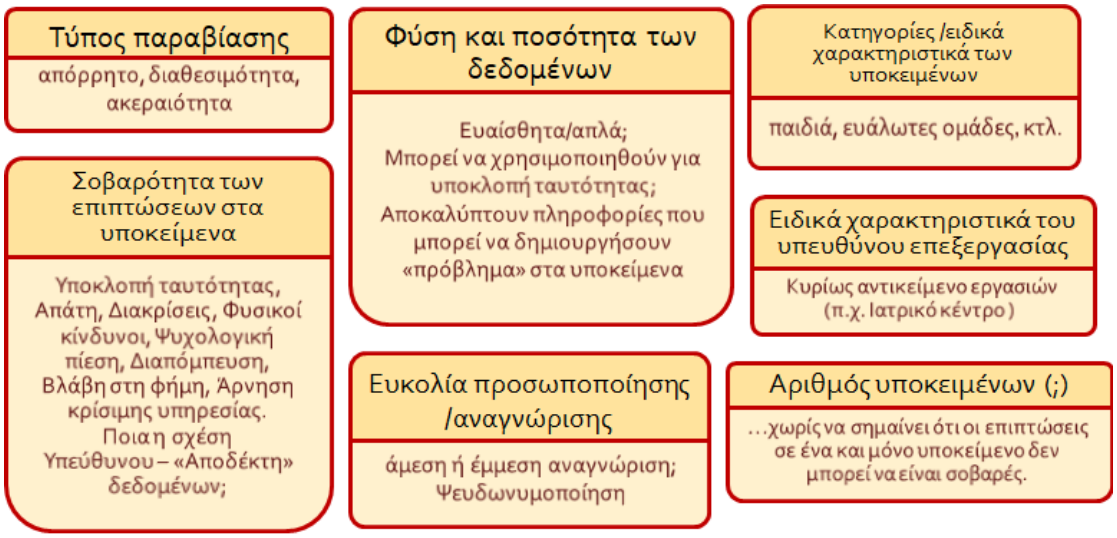
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εξετάζονται από τον υπεύθυνο επεξεργασίας κατά τη φάση αξιολόγησης της βαρύτητας του περιστατικού.

δ) Τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, τα μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Ακόμα και αν οι πληροφορίες αυτές δεν είναι όλες διαθέσιμες κατά την υποβολή της γνωστοποίησης, αυτή θα πρέπει να υποβληθεί, με ελλιπείς έστω πληροφορίες, ως αρχική – εντός 72 ωρών - και να ακολουθήσει στη συνέχεια, χωρίς αδικαιολόγητη καθυστέρηση, επικαιροποίησή της με υποβολή συμπληρωματικής γνωστοποίησης («σταδιακή» γνωστοποίηση).

Επισημαίνεται επίσης ότι, πέραν των ανωτέρω, ο υπεύθυνος επεξεργασίας θα πρέπει να τεκμηριώσει (όπως προαναφέρθηκε), σε περίπτωση που η γνωστοποίηση υποβληθεί μετά την πάροδο των 72 ωρών, τους λόγους της καθυστέρησης αυτής, καθώς επίσης και αν ενημέρωσε ή προτίθεται να ενημερώσει τα θιγόμενα πρόσωπα, με βάση την αξιολόγηση των συνεπειών που πραγματοποίησε.




**Εικόνα 5 - Παράμετροι που συνυπολογίζονται για την αξιολόγηση του κινδύνου από ένα περιστατικό παραβίασης**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- ☞ Δεν υπάρχει σαφής ορισμός ως προς το ποιο είναι το χρονικό σημείο από το οποίο θεωρείται ότι ο υπεύθυνος επεξεργασίας «λαμβάνει γνώση» του περιστατικού (και, άρα, «εκκινεί» ο χρόνος των 72 ωρών για την προθεσμία υποβολής της γνωστοποίησης). Σύμφωνα με το [52], το ακριβές χρονικό σημείο εξαρτάται από τις περιστάσεις της συγκεκριμένης παραβίασης. Ένας υπεύθυνος επεξεργασίας θα πρέπει να θεωρείται ότι αποκτά «γνώση» όταν έχει εύλογο βαθμό βεβαιότητας ότι έχει προκύψει περιστατικό ασφάλειας το οποίο έχει ως αποτέλεσμα να τεθούν σε κίνδυνο τα δεδομένα προσωπικού χαρακτήρα. Σε κάθε περίπτωση, πρέπει να δίνεται έμφαση στην έγκαιρη ανάληψη δράσης για τη διερεύνηση ενός περιστατικού.
- ☞ Ακόμα και αν ο υπεύθυνος επεξεργασίας κρίνει ότι οι κίνδυνοι για τα υποκείμενα των δεδομένων δεν είναι υψηλοί και, άρα, δεν απαιτείται ενημέρωσή τους, η Αρχή μπορεί να ζητήσει να το πράξει (βλ. άρθρο 34 παρ. 4 του ΓΚΠΔ).

Στόχος άλλωστε της διαδικασίας της γνωστοποίησης είναι να διαπιστώσει η εποπτική αρχή αν ο υπεύθυνος επεξεργασίας αξιολόγησε ορθά τους κινδύνους και αν η ενημέρωση των επηρεαζόμενων υποκειμένων των δεδομένων, σε περίπτωση που κριθεί ότι απαιτείται, είναι ορθή, ώστε να μπορεί να παρέμβει διορθωτικά.

**Τι πληροφορίες περιέχει μία κοινοποίηση του περιστατικού στα θιγόμενα πρόσωπα και πώς αυτή γίνεται**

Οι πληροφορίες που πρέπει να κοινοποιούνται στα θιγόμενα πρόσωπα δεν είναι ουσιαστικά διαφορετικές από αυτές που προαναφέρθηκαν για τη γνωστοποίηση στην Αρχή. Ουσιαστικά, η ενημέρωση θα πρέπει να περιέχει μία σύντομη περιγραφή της φύσεως της παραβίασης, το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας των δεδομένων ή άλλου σημείου επικοινωνίας, περιγραφή των ενδεχόμενων συνεπειών της παραβίασης και περιγραφή των ληφθέντων ή των προτεινόμενων προς λήψη μέτρων από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρων για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της. Ως παράδειγμα μέτρων που έχουν ληφθεί για την αντιμετώπιση της παραβίασης και την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της, ο υπεύθυνος επεξεργασίας θα μπορούσε να αναφέρει (όπως



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αναφέρεται ενδεικτικά και στο [52]) ότι, αφού γνωστοποίησε την παραβίαση στην αρμόδια εποπτική αρχή, έλαβε συμβουλές σχετικά με την αντιμετώπιση του περιστατικού και της άμβλυνσης των συνεπειών. Ο υπεύθυνος επεξεργασίας θα πρέπει επίσης, κατά περίπτωση, να παρέχει ειδικές συμβουλές στα πρόσωπα για την προστασία τους από ενδεχόμενες δυσμενείς συνέπειες της παραβίασης, όπως, π.χ., αλλαγή κωδικού πρόσβασης.

Η ενημέρωση στα θιγόμενα πρόσωπα πρέπει να είναι ατομική σε κάθε ένα εκ των θιγόμενων προσώπων. Περαιτέρω, προκειμένου να διασφαλίζεται η σαφήνεια και διαφάνεια της ενημέρωσης αυτής, τα ειδικά μηνύματα που θα αποστέλλονται δεν θα πρέπει να αποστέλλονται μαζί με άλλες πληροφορίες, όπως, π.χ., με ενημερωτικά δελτία. Παραδείγματα μεθόδων ανακοίνωσης μέσω απευθείας αποστολής μηνυμάτων για ενημέρωση σχετικά με περιστατικό παραβίασης δεδομένων είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα μηνύματα SMS αλλά και τα άμεσα μηνύματα (instant messages).

Ενδέχεται η ατομική ενημέρωση να μην είναι ευχερής και να απαιτεί δυσανάλογες προσπάθειες – π.χ. όταν είναι απροσδιόριστος ή/και εξαιρετικά μεγάλος ο αριθμός των ατόμων που επλήγησαν από το περιστατικό ή όταν δεν υπάρχουν στοιχεία επικοινωνίας τους. Τότε, ο υπεύθυνος επεξεργασίας θα πρέπει να προβαίνει σε δημόσια ανακοίνωση ή να λαμβάνει άλλο παρόμοιο μέτρο έτσι ώστε τα υποκείμενα των δεδομένων να ενημερώνονται με εξίσου αποτελεσματικό τρόπο (άρθρο 34 παρ. 3 στοιχ. γ' του ΓΚΠΔ). Όπως αναφέρεται στο [52], τέτοιοι τρόποι ενημέρωσης μπορεί να συνίστανται σε ανάρτηση σε περίοπτη θέση σε διαδικτυακούς τόπους ή/και σε έντυπα μέσα ενημέρωσης. Σύμφωνα επίσης με την αιτιολογική σκέψη 86 του ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας μπορούν να επικοινωνήσουν με την Αρχή και για συμβουλή αναφορικά με την ενημέρωση στα θιγόμενα πρόσωπα – όπως, π.χ., ποιος είναι ο κατάλληλος τρόπος επικοινωνίας μαζί τους ή τι περιεχόμενο πρέπει να έχει το κείμενο ενημέρωσης.

☞ Το δικαίωμα των υποκειμένων των δεδομένων να ενημερώνονται σε περίπτωση



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

περιστατικού παραβίασης δεδομένων που τα αφορά και από το οποίο ελλοχεύουν υψηλοί κίνδυνοι δύναται να περιορίζεται, σύμφωνα με τις σχετικές προβλέψεις του άρθρου 23 του ΓΚΠΔ (βλ. Ενότητα 6) – δηλαδή εφόσον υπάρχει ειδική νομοθετική πρόβλεψη, για συγκεκριμένους σκοπούς όπως περιγράφονται στο εν λόγω άρθρο, και εφόσον το εν λόγω νομοθετικό μέτρο είναι αναγκαίο και αναλογικό. Όπως συζητήσαμε στην Ενότητα 6, κάθε τέτοια εξαίρεση από την ενημέρωση πρέπει να ερμηνεύεται περιοριστικά.

**Τι πληροφορίες περιέχει η καταγραφή του περιστατικού εσωτερικά στον οργανισμό**

Όπως προαναφέρθηκε, όλα ανεξαιρέτως τα περιστατικά παραβίασης δεδομένων πρέπει να καταγράφονται εσωτερικά στον οργανισμό, ακόμα και αν δεν ανακύπτει εξ αυτών κανένας κίνδυνος (δηλαδή καταγράφονται ακόμα και τα περιστατικά που δεν γνωστοποιούνται στην Αρχή). Π.χ. τέτοιες περιπτώσεις κατά τις οποίες δεν ανακύπτει κίνδυνος μπορεί να είναι οι εξής:

1) Απώλεια/κλοπή φορητού αποσπώμενου δίσκου (π.χ. USB stick) που περιέχει και προσωπικά δεδομένα, ο οποίος όμως είναι κρυπτογραφημένος[41] με ισχυρό («state-of-the-art») αλγόριθμο κρυπτογράφησης, ενώ το κλειδί αποκρυπτογράφησης δεν διέρρευσε.
2) Βλάβη δικτύου που κατέστησε μη διαθέσιμες τις υπηρεσίες προς το κοινό για ένα μικρό χρονικό διάστημα (και άρα, για αυτό το μικρό διάστημα, τα υποκείμενα των δεδομένων δεν μπορούσαν, π.χ., να ασκήσουν τα δικαιώματά τους).

Η καταγραφή, σύμφωνα με το άρθρο 33 παρ. 5, πρέπει να αποτυπώνει τα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες αλλά και τα ληφθέντα διορθωτικά μέτρα. Ο υπεύθυνος επεξεργασίας θα πρέπει να φροντίζει ώστε το περιεχόμενο αυτού του «εσωτερικού μητρώου» να

[41] Αν και η κρυπτογράφηση θα μελετηθεί περαιτέρω στην Ενότητα 15, στο παρόν σημείο ας γνωρίζουμε ότι η κρυπτογράφηση μετατρέπει τα δεδομένα σε ακατάληπτη μορφή έτσι ώστε, ακόμα και αν κάποιος αποκτήσει πρόσβαση σε αυτά, δεν μπορεί να τα διαβάσει παρά μόνο αν διαθέτει το κατάλληλο κλειδί αποκρυπτογράφησης.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επιτρέπει στην Αρχή, η οποία δύναται να το ζητήσει οποτεδήποτε, να επαληθεύσει τη συνολική συμμόρφωσή του με τις υποχρεώσεις του άρθρου 33.

**Παραδείγματα**

Ακολουθούν κάποια ενδεικτικά παραδείγματα περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, προκειμένου να αποσαφηνιστούν κάποιες χαρακτηριστικές περιπτώσεις όπου απαιτείται γνωστοποίηση στην Αρχή, καθώς και ειδικότερα, εκείνες που απαιτούν και ενημέρωση των θιγόμενων προσώπων. Σε κάθε περίπτωση ωστόσο, επαφίεται στον υπεύθυνο επεξεργασίας να κάνει, ανά περιστατικό, ορθή στάθμιση/αξιολόγηση των κινδύνων σύμφωνα με τις παραμέτρους που περιγράφονται στην Εικόνα 5, την οποία θα πρέπει να μπορεί να τεκμηριώσει

Τα παραδείγματα που ακολουθούν βασίζονται σε κάποια που περιέχονται στις κατευθυντήριες γραμμές του ΕΣΠΔ [57], στις οποίες ο αναγνώστης μπορεί να ανατρέξει για περισσότερο υλικό – συμπεριλαμβανομένων των ενδεδειγμένων ενεργειών στις οποίες θα πρέπει να προβεί ο υπεύθυνος επεξεργασίας προς αντιμετώπιση του περιστατικού.

**Παράδειγμα:** Κακόβουλο λογισμικό τύπου ransomware έπληξε το δίκτυο ενός Δημόσιου φορέα με αποτέλεσμα να καθίστανται μη διαθέσιμα όλα τα αρχεία τύπου .doc και .pdf που ήταν αποθηκευμένα σε κεντρικούς εξυπηρετητές (servers) – τα περισσότερα εκ των οποίων περιείχαν προσωπικά δεδομένα τόσο εργαζομένων όσο και πολιτών. Ο επιτιθέμενος ζητά, μέσω ηλεκτρονικού μηνύματος, λύτρα για να «ξεκλειδώσει» τα αρχεία και να είναι προσπελάσιμα ξανά. Μετά από ενδελεχή ανάλυση, προκύπτει με σαφήνεια ότι δεν έγινε διαρροή των αρχείων εκτός του φορέα – δηλαδή ο επιτιθέμενος «κλείδωσε» τα αρχεία, χωρίς να τα λάβει ο ίδιος ή να αποκτήσει άλλη πρόσβαση σε αυτά. Για τα εν λόγω αρχεία, υπήρχε αντίγραφο ασφαλείας, από το οποίο ήταν εφικτή εντός κάποιων λίγων ωρών η επαναφορά των αρχείων.
Η εν λόγω περίπτωση αποτελεί ένα παράδειγμα από το οποίο δεν προκύπτουν κίνδυνοι για τα υποκείμενα των δεδομένων, αφού δεν επλήγη η εμπιστευτικότητα,



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ενώ τα δεδομένα ήταν μη ευχερώς διαθέσιμα για λίγες ώρες – οπότε η απώλεια διαθεσιμότητας υπήρξε για μικρό διάστημα. Άρα, δεν απαιτείται γνωστοποίηση στην Αρχή, ούτε βέβαια στα υποκείμενα των δεδομένων. Αυτό όμως δεν σημαίνει ότι το Υπουργείο, ως υπεύθυνος επεξεργασίας, δεν πρέπει να διερευνήσει τους λόγους για τους οποίους κατέστη εφικτή η παρείσφρυση του κακόβουλου λογισμικού και να λάβει δέοντα διορθωτικά μέτρα (π.χ. ενημέρωση/εκπαίδευση προσωπικού σχετικά με «άνοιγμα» ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου).

Η ανωτέρω αξιολόγηση μπορεί να αλλάξει αν θεωρήσουμε ότι κάποιες παράμετροι αναφορικά με το περιστατικό είναι διαφορετικές. Για παράδειγμα, αν τα αντίγραφα ασφαλείας είναι μόνο σε έγχαρτη και όχι ηλεκτρονική μορφή, οπότε απαιτείται κάποιο διάστημα λίγων ημερών για την πλήρη επαναφορά τους (π.χ. 5 – 7 ημέρες), τότε υπάρχουν κάποιοι κίνδυνοι για τα υποκείμενα των δεδομένων (αν π.χ. επείγονται να λάβουν κάποιο αντίγραφο εγγράφου τους), οπότε και θα πρέπει να υπάρξει γνωστοποίηση του περιστατικού στην Αρχή. Οι κίνδυνοι πιθανώς να μην αξιολογούνται ως υψηλοί στο σενάριο αυτό, οπότε δεν χρειάζεται να ενημερωθούν τα θιγόμενα πρόσωπα: αυτό όμως θα πρέπει να κριθεί προσεχτικά ανά περίπτωση. Για παράδειγμα, αν ο υπεύθυνος επεξεργασίας είναι νοσοκομείο και το περιστατικό αφορά δεδομένα υγείας ασθενών, οπότε αυτή η απώλεια (ευχερούς) διαθεσιμότητας των δεδομένων δύναται να επιφέρει συνέπειες σε διαδικασίες του νοσοκομείου αναφορικά με τη νοσηλεία/θεραπεία/ιατρικές πράξεις, τότε οι κίνδυνοι είναι υψηλοί και τα υποκείμενα των δεδομένων θα πρέπει να ενημερωθούν.

Τέλος, η αξιολόγηση των κινδύνων διαφοροποιείται πλήρως αν, στο ανωτέρω περιστατικό, δεν υπάρχουν καθόλου αντίγραφα ασφαλείας ή αν τα δεδομένα επίσης διέρρευσαν προς τον επιτιθέμενο. Σε αυτές τις περιπτώσεις υπάρχουν σαφώς κίνδυνοι οπότε και θα πρέπει το περιστατικό να γνωστοποιηθεί στην Αρχή, ενώ με πολύ μεγάλη πιθανότητα οι κίνδυνοι θα είναι υψηλοί, οπότε και θα πρέπει να ενημερωθούν και τα υποκείμενα των δεδομένων (θα πρέπει να εξεταστεί ακριβώς η φύση των δεδομένων, το είδος των υποκειμένων των δεδομένων που αφορά, το πλήθος τους κτλ. προκειμένου να αξιολογηθούν οι κίνδυνοι από την απώλεια διαθεσιμότητας ή/και εμπιστευτικότητας).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Παράδειγμα:** Σε ένα σχολείο γίνεται διάρρηξη, από την οποία προκύπτει κλοπή δύο φορητών υπολογιστών. Οι υπολογιστές περιέχουν αρχεία μαθητών (ονοματεπώνυμα, διευθύνσεις, τηλέφωνα επικοινωνίας, έτη γέννησης, βαθμοί, αναρρωτικές άδειες κτλ.). Από το εν λόγω περιστατικό υπάρχουν σαφώς υψηλοί κίνδυνοι – ανεξάρτητα του ότι υπάρχει πιθανότητα ο σκοπός της διάρρηξης να ήταν ο τεχνολογικός εξοπλισμός και όχι το περιεχόμενό τους (εξάλλου, κανείς δεν μπορεί να είναι σίγουρος για το σκοπό της διάρρηξης), οπότε και θα πρέπει να ενημερωθούν τα υποκείμενα των δεδομένων (εφόσον πρόκειται για ανήλικους, οι ασκούντες τη γονική μέριμνα) και, αυτονοήτως, πρέπει να υπάρξει γνωστοποίηση και στην Αρχή. Η ενημέρωση είναι ανεξάρτητη του αν τα δεδομένα τηρούνται και σε άλλο σημείο (οπότε δεν υπάρχει απώλεια διαθεσιμότητας παρά μόνο εμπιστευτικότητας) – πολλώ δε μάλλον αν δεν τηρείται αντίγραφό τους.

Εάν ωστόσο οι σκληροί δίσκοι των υπολογιστών ήταν εξαρχής κρυπτογραφημένοι, με ασφαλή αλγόριθμο κρυπτογράφησης, χωρίς να έχει διαρρεύσει το κλειδί με το οποίο αποκρυπτογραφούνται, τότε δεν προκύπτει κανένας κίνδυνος και συνεπώς δεν απαιτείται γνωστοποίηση στην Αρχή ούτε βεβαίως ενημέρωση των προσώπων.

**Παράδειγμα:** Φορέας Α που πραγματοποιεί εκπαιδευτικά σεμινάρια έστειλε λίστα συμμετεχόντων (ονοματεπώνυμα και ηλεκτρονικές διευθύνσεις) εκ παραδρομής σε λάθος παραλήπτη, ο οποίος είναι ένας άλλος φορέας Β που είχε φιλοξενήσει αντίστοιχο σεμινάριο το προηγούμενο έτος. Από το συγκεκριμένο σφάλμα δεν προκύπτουν κίνδυνοι, εφόσον ο φορέας Α ενημερώσει αμέσως το φορέα Β να διαγράψει το αρχείο που έλαβε εκ παραδρομής, και λαμβάνοντας υπόψη και τη φύση των δεδομένων. Συνεπώς, δεν απαιτείται γνωστοποίηση στην Αρχή – και, κατ' επέκταση, ούτε ενημέρωση των επηρεαζόμενων προσώπων.

Γενικότερα ωστόσο, ένα τέτοιο περιστατικό μπορεί να αξιολογηθεί διαφορετικά αν το είδος των δεδομένων είναι διαφορετικό – π.χ. αν το αρχείο περιέχει αριθμούς ταυτότητας των συμμετεχόντων, τηλεφωνικούς τους αριθμούς ή διατροφικές



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προτιμήσεις ή/και αν ο παραλήπτης είναι άγνωστος (π.χ. με διεύθυνση που είναι μικρός αναγραμματισμός αυτής του σωστού παραλήπτη). Σε τέτοιες περιπτώσεις υπάρχουν, κατ' αρχήν, κίνδυνοι και άρα γνωστοποίηση στην Αρχή πρέπει να υποβληθεί, ενώ δεν αποκλείεται οι κίνδυνοι να πρέπει να αξιολογηθούν ως υψηλοί οπότε και θα πρέπει να ενημερωθούν και τα θιγόμενα πρόσωπα.

**Παράδειγμα:** Φορέας που παρέχει ηλεκτρονικές υπηρεσίες αναφορικά με αιτήματα λήψης κοινωνικών επιδομάτων (βάσει π.χ. δεδομένων υγείας ή οικονομικής κατάστασης) ενημερώνεται από πολίτη που υπέβαλε αίτηση ότι, όταν προσπάθησε να δει την αίτησή του, απέκτησε πρόσβαση σε αίτηση άλλου προσώπου. Ο φορέας διαπίστωσε ότι υπήρχε σφάλμα στο λογισμικό, το οποίο διόρθωσε αμέσως. Με ελέγχους που πραγματοποίησε βεβαιώθηκε ότι αντίστοιχη θέαση δεδομένων σε τρίτους υπήρξε σε άλλες τρεις περιπτώσεις.

Από τη φύση των δεδομένων των οποίων τα δεδομένα διέρρευσαν σε τρίτους προκύπτει ότι υπάρχουν κίνδυνοι για τα θιγόμενα πρόσωπα και άρα το περιστατικό πρέπει να γνωστοποιηθεί στην Αρχή. Με πολύ μεγάλη πιθανότητα οι κίνδυνοι θα πρέπει να αξιολογηθούν ως υψηλοί οπότε και θα πρέπει να ενημερωθούν τα θιγόμενα πρόσωπα (τέσσερα στο σύνολο παραπάνω) – αυτό θα πρέπει να καθοριστεί από τον υπεύθυνο επεξεργασίας με βάση τις λεπτομέρειες του περιστατικού (π.χ. αν η αίτηση η ίδια περιέχει δεδομένα υγείας ή οικονομικής κατάστασης, τότε οι κίνδυνοι θα πρέπει να θεωρούνται υψηλοί).

Στην Ενότητα 15, όπου θα αναλυθούν κάποια τεχνικά μέτρα ασφάλειας, θα υπάρξουν εκ νέου κάποια παραδείγματα, προσανατολισμένα στην αξιοποίηση των τεχνολογιών που περιγράφονται εκεί.

## Ο ρόλος του εκτελούντα την επεξεργασία

Οι ως άνω υποχρεώσεις αφορούν τον υπεύθυνο επεξεργασίας και όχι τον εκτελούντα. Κατά συνέπεια, αν μία επεξεργασία συντελείται από εκτελούντα την επεξεργασία για



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

λογαριασμό ενός υπευθύνου επεξεργασίας και συμβεί περιστατικό παραβίασης δεδομένων στην πλευρά του εκτελούντα, οι σχετικές υποχρεώσεις (γνωστοποίησης του περιστατικού στην Αρχή ή/και ενημέρωση των θιγόμενων προσώπων κατόπιν αξιολόγησης των κινδύνων κτλ.) βαρύνουν τον υπεύθυνο επεξεργασίας. Ωστόσο, και ο εκτελών την επεξεργασία έχει, τελικά, ουσιαστικό ρόλο. Κατ' αρχάς, όπως ήδη προαναφέρθηκε στην Ενότητα 7, στο άρθρο 28 παρ. 3 στοιχ. στ' αναφέρεται ότι η σύμβαση ή άλλη πράξη μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία προβλέπει ότι ο εκτελών την επεξεργασία «*συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36* (…)». Συνεπώς, η εν λόγω συνδρομή περιλαμβάνει και τη διαχείριση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα.

Ειδικότερα, το άρθρο 33 παράγραφος 2 ορίζει ότι εάν ένας εκτελών την επεξεργασία αποκτήσει γνώση περιστατικού παραβίασης των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται για λογαριασμό του υπεύθυνου επεξεργασίας, τότε ο εκτελών την επεξεργασία πρέπει να ενημερώνει τον υπεύθυνο επεξεργασίας «αμελλητί». Η υποχρέωση αυτή είναι στενά συνυφασμένη με την ανωτέρω αναφερθείσα υποχρέωση του υπεύθυνου επεξεργασίας για έγκαιρη ανίχνευση και αντιμετώπιση του περιστατικού (συμπεριλαμβανομένων των υποχρεώσεών του εκ των άρθρων 33 και 34): ο εκτελών την επεξεργασία δεν χρειάζεται να κάνει καμία κρίση/στάθμιση του περιστατικού, αλλά βοηθά τον υπεύθυνο επεξεργασίας. Στην περίπτωση που ο εκτελών την επεξεργασία παρέχει υπηρεσίες σε πολλαπλούς υπεύθυνους επεξεργασίας, οι οποίοι επηρεάζονται όλοι από το ίδιο περιστατικό, ο εκτελών την επεξεργασία θα πρέπει να αναφέρει τις λεπτομέρειες του περιστατικού σε κάθε υπεύθυνο επεξεργασίας [52]. Σε κάθε περίπτωση, η ενημέρωση μπορεί να είναι σταδιακή – δηλαδή δεν δικαιολογείται καθυστέρηση ενημέρωσης από την πλευρά του εκτελούντα προς τον υπεύθυνο επεξεργασίας λόγω του ότι ο εκτελών, π.χ., ενδεχομένως να μην έχει πλήρη εικόνα της έκτασης του περιστατικού.

☞ Ένας εκτελών την επεξεργασία θα μπορούσε να προβεί σε γνωστοποίηση για λογαριασμό του υπευθύνου επεξεργασίας, εάν ο υπεύθυνος επεξεργασίας έχει



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

παράσχει στον εκτελούντα την επεξεργασία την κατάλληλη εξουσιοδότηση και αυτό αποτελεί μέρος των συμβατικών ρυθμίσεων μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία. Αυτή η γνωστοποίηση πρέπει να γίνεται σύμφωνα με τα άρθρα 33 και 34. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η νομική ευθύνη για τη γνωστοποίηση εξακολουθεί να βαρύνει τον υπεύθυνο επεξεργασίας [52].

- **Ερώτηση δραστηριότητας**: Για τις ακόλουθες περιπτώσεις περιστατικών παραβίασης δεδομένων, εξηγείστε: α) ποιος στόχος ασφάλειας επλήγη (εμπιστευτικότητα, ακεραιότητα ή/και διαθεσιμότητα), β) για ποιες πρέπει να υποβληθεί γνωστοποίηση στην Αρχή και, γ) για ποιες πρέπει να ενημερωθούν τα θιγόμενα πρόσωπα.
- Περιστατικό 1: Δεδομένα προσωπικού χαρακτήρα μεγάλου αριθμού φοιτητών (ονοματεπώνυμα, αριθμοί ταυτότητας, αριθμοί φοιτητικού μητρώου, έτος και σχολή φοίτησης, λήψη υποτροφίας κοινωνικής μέριμνας) εστάλησαν εκ παραδρομής σε εσφαλμένο κατάλογο ηλεκτρονικών διευθύνσεων με περισσότερους από 1000 αποδέκτες. Οι αποδέκτες είναι υπάλληλοι άλλων Δημόσιων φορέων ή/και Πανεπιστημίων με τους οποίους στο παρελθόν είχαν υπάρξει επικοινωνίες για άλλα ζητήματα.
- Περιστατικό 2: Δήμος αποστέλλει ενημερωτικό δελτίο (newsletter) με τα νέα του Δήμου σε ηλεκτρονικές διευθύνσεις δημοτών. Ωστόσο, εκ παραδρομής, οι διευθύνσεις δεν εστάλησαν μέσω κρυφής κοινοποίησης («bcc») αλλά τέθηκαν ως διευθύνσεις παραληπτών («to») με αποτέλεσμα να καθίστανται διαθέσιμες σε όλους.
- Περιστατικό 3: Λόγω βλάβης υπολογιστικού συστήματος, η ιστοσελίδα Υπουργείου μέσω της οποίας οι πολίτες μπορούν να υποβάλουν αιτήσεις και να λάβουν σχετική πληροφόρηση, είναι ανενεργή για 3 ώρες.
- Περιστατικό 4: Ομοίως με το περιστατικό 4, αλλά η ιστοσελίδα καθίσταται ανενεργή λόγω διαδικτυακής επίθεσης. Δεν επηρεάζονται τα αποθηκευμένα προσωπικά δεδομένα του Υπουργείου.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Περιστατικό 5: Κατά τη διαδικασία αναβάθμισης πληροφοριακού συστήματος και ενσωμάτωσης αρχείων με προσωπικά δεδομένα από το παλαιό σύστημα στο νέο, παρατηρούνται κάποιες αστοχίες και η ενσωμάτωση δεν έγινε σωστά – συγκεκριμένα, κάποια δεδομένα δεν «περάστηκαν» καθόλου στο νέο σύστημα, ενώ κάποια άλλα «περάστηκαν» λανθασμένα (όπως αντιστοίχιση ημερομηνίας γέννησης λάθος προσώπου σε συγκεκριμένα φυσικά πρόσωπα ή/και λάθος όνομα πατρός). Αν και η αναβάθμιση έγινε σε δοκιμαστικό περιβάλλον, τα ανωτέρω ζητήματα εντοπίστηκαν αφού το νέο σύστημα τέθηκε σε παραγωγική λειτουργία. Τα αρχικά αρχεία είχαν διατηρηθεί αυτούσια σε αντίγραφα ασφαλείας και είναι εφικτή η επαναφορά τους μέσα σε διάστημα 1-2 ημερών.
- Περιστατικό 6: Ομοίως με το περιστατικό 5, αλλά θεωρείστε ότι τα αρχικά αρχεία δεν είχαν διατηρηθεί σε αντίγραφα ασφαλείας.

- **Ερώτηση δραστηριότητας**: Δήμος παρέχει μέσω της ιστοσελίδας του υπηρεσία ηλεκτρονικών πληρωμών, όπου οι χρήστες μπορούν να πληρώνουν παράβολα, πρόστιμα, χαρτόσημα κτλ. με χρέωση πιστωτικών ή άλλων καρτών που χρησιμοποιούνται ως μέσο ηλεκτρονικής πληρωμής και έχουν εκδοθεί στο όνομα των υπόχρεων. Ο Δήμος ενημερώνεται από μία Τράπεζα ότι ανιχνεύτηκαν «ύποπτες» κινήσεις καρτών σε 5 περιπτώσεις, όπου και οι 5 κάτοχοι αυτών είχαν προηγούμενα πραγματοποιήσει συναλλαγή μέσω του διαδικτυακού τόπου του Δήμου – η ίδια η Τράπεζα ενημέρωσε τους κατόχους των καρτών και προέβη και σε απενεργοποίησή τους. Ο Δήμος απενεργοποίησε αμέσως την υπηρεσία ηλεκτρονικών πληρωμών και διαπίστωσε την πηγή του προβλήματος (διαδικτυακή επίθεση λόγω μη ανανέωσης λογισμικού της πλατφόρμας διαδικτυακών πληρωμών, οπότε υπήρχε ευπάθεια στην έκδοση του λογισμικού που ήταν σε λειτουργία και, λόγω αυτής, εγκαταστάθηκε κακόβουλο λογισμικό), όπου και το απεκατέστησε αμέσως και μετά από μία μέρα η υπηρεσία πληρωμών τέθηκε εκ νέου σε λειτουργία, ενώ απομακρύνθηκε το κακόβουλο λογισμικό που



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εγκαταστάθηκε λόγω της ανωτέρω ευπάθειας και το οποίο, τελικά, προκάλεσε τη διαρροή. Ο Δήμος επίσης επιβεβαίωσε ότι μόνο για αυτές τις 5 περιπτώσεις υπήρξε διαρροή δεδομένων πιστωτικών καρτών. Δεδομένου ότι οι κάτοχοί τους ενημερώθηκαν από την Τράπεζα, ο Δήμος αποφασίζει να μην προχωρήσει σε ενημέρωσή τους. Σχολιάστε συνολικά την αντίδραση του Δήμου.

## 10.3 Εκτίμηση αντικτύπου ως προς την προστασία δεδομένων προσωπικού χαρακτήρα

Το άρθρο 35 του ΓΚΠΔ εισάγει μία σημαντική υποχρέωση για υπευθύνους επεξεργασίας, η οποία αφορά συγκεκριμένες μόνο πράξεις επεξεργασίας: πρόκειται για την εκτίμηση αντικτύπου ως προς την προστασία δεδομένων (ΕΑΠΔ) – γνωστή και με το πρωτότυπο ακρωνύμιο DPIA (Data Protection Impact Assessment). Πρόκειται για έναν όρο που σχεδόν με την ίδια έννοια χρησιμοποιούνταν επί έτη υπό το όνομα «PIA» (Privacy Impact Assessment). Ουσιαστικά, η ΕΑΠΔ αποτελεί μία διαδικασία κατά την οποία γίνεται με συστηματικό τρόπο η περιγραφή μίας επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αξιολογείται η αναγκαιότητα και αναλογικότητα της, προσδιορίζονται οι ειδικότεροι εξ αυτής κίνδυνοι και, εν τέλει, συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η εν λόγω επεξεργασία των δεδομένων, με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους. Ως εκ τούτου, αποτελεί σημαντικό εργαλείο λογοδοσίας, αφού ο υπεύθυνος επεξεργασίας μπορεί να αποδεικνύει ότι μελέτησε διεξοδικά τους κινδύνους και έλαβε τα δέοντα μέτρα για την αντιμετώπισή τους [58].

Οι άνθρωποι του χώρου της ασφάλειας πληροφοριακών συστημάτων ενδεχομένως να θεωρούν ότι η ΕΑΠΔ είναι αντίστοιχη με αυτό που ονομάζουν *διαχείριση κινδύνων ασφάλειας*: ουσιαστικά όμως είναι κάτι πολύ ευρύτερο, καθώς η ΕΑΠΔ δεν εξετάζει μόνο κινδύνους ασφάλειας αλλά κάθε κίνδυνο που άπτεται των αρχών της



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επεξεργασίας προσωπικών δεδομένων (όπως, π.χ., συλλογή υπέρμετρων δεδομένων, δυνατότητα συνδυασμού προσωπικών δεδομένων που επιτρέπει τη δημιουργία προφίλ ατόμων με εξαγωγή συμπερασμάτων χωρίς κάτι τέτοιο να είναι συμβατό με το σκοπό της επεξεργασίας, δυσχέρειες στην άσκηση των δικαιωμάτων των υποκειμένων δεδομένων κτλ.). Σε κάθε περίπτωση ωστόσο, η συμμετοχή ανθρώπων της ασφάλειας πληροφοριακών συστημάτων ενός οργανισμού είναι απαραίτητη κατά την εκπόνηση ΕΑΠΔ. Επίσης, όπως ρητά αναφέρεται στην παρ. 2 του άρθρου 35 του ΓΚΔΠ, κατά την εκπόνηση μίας ΕΑΠΔ ζητείται η γνώμη του ΥΠΔ.

Η ΕΑΠΔ πρέπει να περιέχει τουλάχιστον τα ακόλουθα (άρθρο 35 παρ. 7 του ΓΚΠΔ):

α) συστηματική περιγραφή των πράξεων επεξεργασίας και των σκοπών της επεξεργασίας,

β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων,

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφαλείας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς τον ΓΚΠΔ.

Η ΕΑΠΔ είναι υποχρεωτική μόνο για επεξεργασίες που ενδέχεται να επιφέρουν υψηλό κίνδυνο και πρέπει να εκπονούνται πριν την έναρξη της επεξεργασίας. Προς τούτο, στην παρ. 3 του άρθρου 35 αναφέρονται περιπτώσεις οι οποίες ενδέχεται, ιδίως, να επιφέρουν υψηλό κίνδυνο (και, άρα, απαιτούν ΕΑΠΔ):

α) συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

γ) συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Η αιτιολογική σκέψη 91 του ΓΚΔΠ αναλύει λίγο περισσότερο το σκεπτικό υπό το οποίο οι ως άνω περιπτώσεις ενδέχεται να οδηγήσουν σε υψηλό κίνδυνο. Σύμφωνα με αυτή:

«*αυτό θα πρέπει να ισχύει ιδίως για πράξεις επεξεργασίας μεγάλης κλίμακας που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο, για παράδειγμα λόγω της ευαισθησίας τους, όταν σύμφωνα με τα υφιστάμενα επίπεδα τεχνολογικής γνώσης χρησιμοποιείται μια νέα τεχνολογία σε ευρεία κλίμακα, καθώς και για άλλες πράξεις επεξεργασίας οι οποίες έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ιδίως όταν οι πράξεις αυτές δυσχεραίνουν την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων. Θα πρέπει επίσης να διενεργείται εκτίμηση αντικτύπου όσον αφορά την προστασία των δεδομένων όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία ενόψει της λήψης αποφάσεων σε σχέση με συγκεκριμένα φυσικά πρόσωπα έπειτα από συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών που αφορούν φυσικά πρόσωπα και βασίζονται στην κατάρτιση προφίλ βάσει των εν λόγω δεδομένων ή έπειτα από την επεξεργασία συγκεκριμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, βιομετρικών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας. Εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων απαιτείται επίσης για την παρακολούθηση δημόσια προσπελάσιμων χώρων σε μεγάλη κλίμακα, ιδίως όταν χρησιμοποιούνται οπτικοηλεκτρονικές συσκευές ή για οποιεσδήποτε άλλες εργασίες όποτε η αρμόδια εποπτική αρχή θεωρεί ότι η επεξεργασία ενδέχεται να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ιδίως επειδή εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή σύμβαση ή επειδή πραγματοποιούνται συστηματικά σε μεγάλη κλίμακα*».



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Σε ποιες περιπτώσεις είναι υποχρεωτική η ΕΑΠΔ**

Η κάθε εποπτική αρχή έχει την υποχρέωση, βάσει της παρ. 4 του άρθρου 35, να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου. Για την Ελλάδα, η Αρχή έχει εκδώσει έναν τέτοιο κατάλογο (βλ. Απόφαση 65/2018 [59], η οποία έχει δημοσιευτεί και στο ΦΕΚ Β΄ 1622/10-5-2019), λαμβάνοντας υπόψη και τις σχετικές κατευθυντήριες γραμμές [58][42]. Σύμφωνα με τον κατάλογο αυτόν, τα κριτήρια βάσει των οποίων λαμβάνεται απόφαση για την διενέργεια ΕΑΠΔ εν όψει κάποιας επεξεργασίας ομαδοποιούνται στις παρακάτω τρεις κατηγορίες:

**1η κατηγορία:** με βάση τα είδη και τους σκοπούς επεξεργασίας, εφόσον πρόκειται για συστηματική επεξεργασία ή/και μεγάλης κλίμακας επεξεργασία (όπως αναλύεται στη συνέχεια).

**2η κατηγορία**: με βάση το είδος των δεδομένων και/ή τις κατηγορίες των υποκειμένων των δεδομένων, εφόσον πρόκειται για συστηματική επεξεργασία ή/και μεγάλης κλίμακας επεξεργασία (όπως αναλύεται στη συνέχεια).

**3η κατηγορία**: Με βάση τα πρόσθετα χαρακτηριστικά και/ή τα χρησιμοποιούμενα μέσα της επεξεργασίας.

Η διενέργεια ΕΑΠΔ είναι υποχρεωτική όταν πληρούται τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας. Είναι επίσης υποχρεωτική όταν συντρέχει ένα τουλάχιστον κριτήριο ως προς την 3η κατηγορία και η επεξεργασία αφορά είδη και σκοπούς επεξεργασίας της 1ης κατηγορίας (ανεξαρτήτως του αν η επεξεργασία είναι συστηματική ή μεγάλης κλίμακας), ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της 2ης κατηγορίας (επίσης ανεξαρτήτως του αν η επεξεργασία είναι συστηματική ή μεγάλης κλίμακας).

Για την έννοια της «*επεξεργασίας μεγάλης κλίμακας*», όπως επισημαίνει η Αρχή στον ως άνω κατάλογό της, δεν υπάρχει σαφής ορισμός, στηριζόμενος σε συγκεκριμένα αριθμητικά δεδομένα. Για την αξιολόγηση μίας επεξεργασίας ως μεγάλης κλίμακας

[42] Ο κατάλογος αυτός εκδόθηκε στο πλαίσιο του μηχανισμού συνεκτικότητας που εισάγει ο ΓΚΠΔ και εγκρίθηκε από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (βλ. Ενότητα 12)

πρέπει να λαμβάνονται υπόψη διάφορες παράμετροι όπως ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων (είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού), ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία, η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων και το γεωγραφικό εύρος της δραστηριότητας επεξεργασίας.

Ακολουθεί η περιγραφή των επεξεργασιών, σύμφωνα με τον ως άνω κατάλογο [59]. Ο κατάλογος προφανώς αναφέρεται σε κάθε είδους υπεύθυνο επεξεργασίας: οι πράξεις επεξεργασίας που αφορούν ιδίως δημόσιους φορείς ή και δημόσιους φορείς τονίζονται με χρωματικό πλαίσιο. Ειδικότερες προϋποθέσεις για διενέργεια ΕΑΠΔ από φορείς του Δημοσίου Τομέα αναλύονται στη συνέχεια.

**1η κατηγορία: βάσει του είδους και σκοπών της επεξεργασίας**

1) Συστηματική αξιολόγηση, βαθμολόγηση, πρόβλεψη, πρόγνωση και κατάρτιση προφίλ, ιδίως πτυχών που αφορούν την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή τις κινήσεις ή την πιστοληπτική ικανότητα των υποκειμένων των δεδομένων.

Σχετικά παραδείγματα είναι η περίπτωση, κατά την οποία χρηματοπιστωτικό ίδρυμα ελέγχει τους πελάτες του με βάση δεδομένα πιστοληπτικής ικανότητας ή δεδομένα για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας ή δεδομένα για εγκλήματα απάτης, ή η περίπτωση, κατά την οποία εταιρεία βιοτεχνολογίας παρέχει απευθείας στους καταναλωτές γενετικές δοκιμές για να εκτιμήσει και να προβλέψει τους κινδύνους νόσου/υγείας.

2) Συστηματική επεξεργασία δεδομένων που αποσκοπεί στη λήψη αυτοματοποιημένων αποφάσεων, οι οποίες παράγουν έννομα αποτελέσματα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σχετικά με τα υποκείμενα των δεδομένων ή επηρεάζουν σημαντικά τα υποκείμενα των δεδομένων κατά ανάλογο τρόπο και μπορούν να οδηγήσουν σε αποκλεισμό ή διακρίσεις σε βάρος του φυσικού προσώπου.

Σχετικά παραδείγματα είναι η αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση ή η αυτόματη άρνηση ασφαλιστικής παροχής.

3) Συστηματική επεξεργασία δεδομένων που ενδέχεται να εμποδίζει το υποκείμενο να ασκήσει τα δικαιώματά του ή να χρησιμοποιήσει μια υπηρεσία ή σύμβαση, ιδίως όταν λαμβάνονται υπόψη δεδομένα που συλλέγονται από τρίτους.

Σχετικά παραδείγματα είναι η περίπτωση, κατά την οποία τράπεζα ελέγχει τους πελάτες της χρησιμοποιώντας μια βάση δεδομένων πιστοληπτικής ικανότητας για να αποφασίσει αν θα τους χορηγήσει δάνειο ή όχι, η καταχώρηση του υποκειμένου σε «μαύρη» λίστα (π.χ. λίστα «κακοπληρωτών»), η καταχώριση του υποκειμένου σε whistleblowing συστήματα.

4) Συστηματική επεξεργασία δεδομένων που αφορά την κατάρτιση προφίλ για το σκοπό της προώθησης προϊόντων και υπηρεσιών εφόσον τα δεδομένα συνδυάζονται με δεδομένα που συλλέγονται από τρίτους.

5) Συστηματική και σε μεγάλη κλίμακα επεξεργασία για την παρακολούθηση, την παρατήρηση ή τον έλεγχο των φυσικών προσώπων με χρήση δεδομένων που συλλέγονται μέσω συστημάτων βιντεοεπιτήρησης ή μέσω δικτύων ή με οποιοδήποτε άλλο μέσο σε δημόσιο χώρο, δημοσίως προσβάσιμο χώρο ή ιδιωτικό χώρο προσιτό σε απεριόριστο αριθμό προσώπων. Περιλαμβάνει την παρακολούθηση των κινήσεων ή της τοποθεσίας/γεωγραφικής θέσης σε πραγματικό ή μη χρόνο ταυτοποιημένων ή ταυτοποιήσιμων φυσικών προσώπων.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Σχετικά παραδείγματα είναι η χρήση καμερών σε εμπορικό κέντρο ή σε σταθμούς μέσων μαζικής μεταφοράς, ή η επεξεργασία δεδομένων θέσης των επιβατών σε αεροδρόμιο ή σε μέσα μαζικής μεταφοράς. Επίσης, η παρακολούθηση μέσω wi-fi συστημάτων (wi-fi tracking) επισκεπτών σε εμπορικά κέντρα ή επεξεργασία δεδομένων μέσω drones.

6) Μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία και τη δημόσια υγεία για σκοπούς δημοσίου συμφέροντος, όπως η εισαγωγή και χρήση συστημάτων ηλεκτρονικής συνταγογράφησης και η εισαγωγή και χρήση ηλεκτρονικού φακέλου ή ηλεκτρονικής κάρτας υγείας.

7) Μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό την εισαγωγή, οργάνωση, παροχή και έλεγχο της χρήσης υπηρεσιών ηλεκτρονικής διακυβέρνησης (όπως ορίζονται στο άρθρο 3 του ν.3979/2011).

**2η κατηγορία: βάσει του είδους των δεδομένων ή/και τις κατηγορίες των υποκειμένων των δεδομένων**

1) Μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων (περιλαμβανομένων των γενετικών και των βιομετρικών με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου) που αναφέρονται στο άρθρο 9 παρ. 1 και των δεδομένων που αναφέρονται στο άρθρο 10 του ΓΚΠΔ.

2) Συστηματική και σε μεγάλη κλίμακα επεξεργασία δεδομένων ιδιαίτερης σημασίας ή εξαιρετικού χαρακτήρα όπως:

a. δεδομένα κοινωνικής πρόνοιας (δεδομένα σχετικά με τη φτώχεια, την ανεργία, την κοινωνική εργασία κλπ.)

b. δεδομένα ηλεκτρονικών επικοινωνιών, περιλαμβανομένων των δεδομένων περιεχομένου όπως του ηλεκτρονικού ταχυδρομείου,



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μεταδεδομένων και των δεδομένων γεωγραφικής θέσης/τοποθεσίας, με εξαίρεση την καταγραφή τηλεφωνικών συνδιαλέξεων σύμφωνα με το άρθρο 4 παρ. 3 του ν.3471/2006[43],

c. δεδομένα που αφορούν εθνικό αριθμό ταυτότητας ή άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής ή αλλαγή των προϋποθέσεων και όρων επεξεργασίας και χρήσης αυτών και των συναφών με αυτά δεδομένων προσωπικού χαρακτήρα,

d. δεδομένα που περιλαμβάνονται σε προσωπικά έγγραφα, ημερολόγια, σημειώσεις από ηλεκτρονικό αναγνώστη (e-reader) και σε εφαρμογές καταγραφής βίου (life logging), που προσφέρουν δυνατότητες τήρησης σημειώσεων και πολύ προσωπικών πληροφοριών,

e. δεδομένα που συλλέγονται ή παράγονται από συσκευές (όπως αυτές με αισθητήρες) ιδίως μέσω των εφαρμογών του "Διαδικτύου των πραγμάτων – IoT" (όπως έξυπνες τηλεοράσεις, έξυπνες οικιακές συσκευές, συνδεδεμένα παιχνίδια, έξυπνες πόλεις, έξυπνοι μετρητές ενέργειας κλπ) και/ή με τη χρήση άλλων μέσων.

3) Συστηματική παρακολούθηση – εφόσον είναι επιτρεπτή – της θέσης/τοποθεσίας καθώς και του περιεχομένου και των μεταδεδομένων των επικοινωνιών των εργαζομένων με εξαίρεση τα αρχεία καταγραφής για λόγους ασφάλειας εφόσον η επεξεργασία περιορίζεται στα απολύτως απαραίτητα δεδομένα και είναι ειδικά τεκμηριωμένη. Σχετικό παράδειγμα που εμπίπτει στην υποχρέωση διενέργειας ΕΑΠΔ αποτελεί η χρήση συστημάτων DLP.

4) Συστηματική επεξεργασία βιομετρικών δεδομένων των εργαζομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου καθώς και γενετικών δεδομένων των εργαζομένων.

**3η κατηγορία - Πρόσθετα χαρακτηριστικά ή/και χρησιμοποιούμενα μέσα της**

[43] Βλ. συναφώς την Ενότητα 13



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**επεξεργασίας**

1) Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογιών ή οργανωτικών λύσεων, οι οποίες μπορεί να περιλαμβάνουν νέες μορφές συλλογής και χρήσης δεδομένων, με ενδεχόμενο υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όπως η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης, ή εφαρμογές mhealth ή άλλες «έξυπνες» εφαρμογές, από τις οποίες δημιουργείται προφίλ των χρηστών (π.χ. καθημερινές συνήθειες), ή εφαρμογές τεχνητής νοημοσύνης ή τεχνολογίες δημόσια προσπελάσιμων blockchain που περιλαμβάνουν προσωπικά δεδομένα.
2) Συνδυασμό και/ή συσχέτιση προσωπικών δεδομένων από πολλαπλές πηγές ή τρίτους, από δύο ή περισσότερες πράξεις επεξεργασίας που υλοποιούνται για διαφορετικούς σκοπούς ή/και από διαφορετικούς υπευθύνους επεξεργασίας με τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων.
3) Σε περίπτωση που η επεξεργασία αφορά δεδομένα, τα οποία δεν έχουν συλλεγεί από το υποκείμενο και η ενημέρωση των υποκειμένων σύμφωνα με το άρθρο 14 ΓΚΠΔ αποδεικνύεται αδύνατη ή θα προϋπέθετε δυσανάλογη προσπάθεια ή είναι πιθανό να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας.

**Ειδικότερα παραδείγματα** (βασισμένα στο [58])

Τα παραδείγματα που ακολουθούν εστιάζουν στα χαρακτηριστικά μίας επεξεργασίας που θα μπορούσε να πραγματοποιηθεί από Δημόσιο φορέα ως υπεύθυνο επεξεργασίας και εμπίπτουν σε αυτές για τις οποίες η ΕΑΠΔ είναι υποχρεωτική, χωρίς να εξετάζεται, για τα συγκεκριμένα παραδείγματα, η ύπαρξη ή όχι νομικής βάσης για τις εν λόγω επεξεργασίες, η οποία είναι ούτως ή άλλως, διαφορετικό προαπαιτούμενο.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**<u>Παράδειγμα:</u>** Χρήση συστήματος βιντεοσκόπησης για την παρακολούθηση της οδικής συμπεριφοράς σε αυτοκινητοδρόμους. Ο υπεύθυνος επεξεργασίας σκοπεύει να χρησιμοποιεί έξυπνο σύστημα ανάλυσης βίντεο για να απομονώνει τα οχήματα και να αναγνωρίζει αυτόματα τις πινακίδες τους. Για τη συγκεκριμένη επεξεργασία είναι υποχρεωτική η διενέργεια ΕΑΠΔ, αφού πρόκειται για χρήση καινοτόμων τεχνολογιών (3ο κριτήριο) για την παρακολούθηση, την παρατήρηση ή τον έλεγχο των φυσικών προσώπων σε δημόσιο χώρο (1ο κριτήριο). Μάλιστα, η εν λόγω επεξεργασία μπορεί να θεωρηθεί μεγάλης κλίμακας, οπότε ΕΑΠΔ απαιτείται ακόμα και χωρίς το «έξυπνο» σύστημα ανάλυσης βίντεο λόγω του ότι εμπίπτει αυτοτελώς στο 1ο κριτήριο (προφανώς βέβαια, στην πρώτη περίπτωση είναι περισσότεροι οι κίνδυνοι που θα πρέπει να αναλυθούν και να αντιμετωπιστούν από την ΕΑΠΔ).

**<u>Παράδειγμα:</u>** Οργανισμός δημιουργεί εθνική βάση δεδομένων αξιολόγησης υποθέσεων απάτης. Για τη συγκεκριμένη επεξεργασία είναι υποχρεωτική η διενέργεια ΕΑΠΔ, αφού πρόκειται για σαφώς μεγάλης κλίμακα επεξεργασία δεδομένων ευαίσθητων του άρθρου 10 του ΓΚΠΔ (2ο κριτήριο), από την οποία μάλιστα προκύπτουν και έννομα αποτελέσματα για τα υποκείμενα των δεδομένων (εάν χρησιμοποιούνται δε αυτοματοποιημένα μέσα για την δημιουργία προφίλ και εξαγωγής συμπερασμάτων με έννομα αποτελέσματα, τότε αυτό αυτοτελώς συνιστά λόγο εκπόνησης ΕΑΠΔ και με βάση το 1ο κριτήριο).

**<u>Παράδειγμα (βλ. και Γνωμοδότηση 3/2020 της Αρχής</u>** [60]**<u>):</u>** Χρήση συστημάτων βιντεοεπιτήρησης από υπεύθυνο επεξεργασίας για παρακολούθηση συγκεντρώσεων, για την καταστολή εγκλημάτων που συνιστούν επιβουλή της δημόσιας τάξης. Για τη συγκεκριμένη επεξεργασία είναι υποχρεωτική η διενέργεια ΕΑΠΔ, αφού πρόκειται για συστηματική και σε μεγάλη κλίμακα παρακολούθηση, παρατήρηση και έλεγχο των φυσικών προσώπων σε δημόσιο χώρο (1ο κριτήριο). Τούτο ισχύει ανεξάρτητα του αν χρησιμοποιούνται και ειδικές τεχνολογίες όπως, π.χ., drone, οπότε και συντρέχει επιπροσθέτως και το 3ο κριτήριο (και, στη δεύτερη αυτή περίπτωση, οι κίνδυνοι που θα πρέπει η



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΑΠΔ να εξετάσει και να αντιμετωπίσει – εφόσον είναι αντιμετωπίσιμοι - είναι μεγαλύτεροι).

**Πώς εκπονείται η ΕΑΠΔ**

Η ΕΑΠΔ εκπονείται από τον υπεύθυνο επεξεργασίας πριν την έναρξη της επεξεργασίας. Είναι σημαντικό ωστόσο να επικαιροποιείται καθ' όλον τον κύκλο ζωής του έργου, ενώ επίσης ενδέχεται να χρειαστεί επικαιροποίηση και μετά την έναρξη της επεξεργασίας, εάν κριθεί ότι κάποιες αποφάσεις χρήζουν επανεξέτασης ή/και κάποια μέτρα που έχουν ληφθεί χρήζουν βελτίωσης: συνεπώς, πρέπει να θεωρείται μία δυναμική και όχι στατική διαδικασία.

Ο ΓΚΠΔ θέτει έναν σημαντικό ρόλο στον ΥΠΔ αναφορικά με την ΕΑΠΔ: Ο υπεύθυνος επεξεργασίας πρέπει να ζητεί τη γνώμη του ΥΠΔ, σύμφωνα με το άρθρο 35 παρ. 2 (εφόσον βέβαια έχει οριστεί), ο οποίος (ΥΠΔ) θα πρέπει επίσης να παρακολουθεί την υλοποίηση της ΕΑΠΔ (άρθρο 39 παρ. 1 στοιχ. γ'). Σύμφωνα με την αρχή της λογοδοσίας, και λαμβάνοντας εξάλλου υπόψη και το γενικότερο ρόλο του ΥΠΔ σε έναν οργανισμό, η γνώμη του ΥΠΔ αναφορικά με την ΕΑΠΔ θα πρέπει να καταγράφεται, όπως βεβαίως και οι συναφείς τελικές αποφάσεις που έλαβε ο υπεύθυνος επεξεργασίας.

☞ Σύμφωνα με το άρθρο 35 παρ. 9 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας οφείλει, όποτε ενδείκνυται, να ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους. Δεν δίνεται ειδικότερη καθοδήγηση στο κείμενο του ΓΚΠΔ αναφορικά με τις περιπτώσεις για τις οποίες ενδείκνυται η λήψη γνώμης των υποκειμένων των δεδομένων. Ωστόσο, υπό το φως της αρχής της λογοδοσίας, ο υπεύθυνος επεξεργασίας θα πρέπει να τεκμηριώνει τον λόγο για τον οποίο δεν ζήτησε τη γνώμη των υποκειμένων των δεδομένων, εφόσον αποφασίζει ότι δεν ενδείκνυται [58].



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Επισημαίνεται ιδιαίτερα ότι η υποχρέωση εκπόνησης ΕΑΠΔ αφορά υπευθύνους επεξεργασίας και όχι εκτελούντες την επεξεργασία. Ωστόσο, εάν η επεξεργασία υλοποιείται πλήρως ή εν μέρει από έναν εκτελούντα την επεξεργασία, τότε ο εκτελών θα πρέπει να συνδράμει τον υπεύθυνο επεξεργασίας στη διενέργεια της ΕΑΠΔ και να παράσχει κάθε αναγκαία πληροφορία (βλ. άρθρο 28 παρ. 3 στοιχ. στ΄του ΓΚΔΠ).

Δεν υπάρχει μία συγκεκριμένη μεθοδολογία για την εκπόνηση ΕΑΠΔ η οποία να θεωρείται «πανάκεια». Υπάρχουν διάφορες μεθοδολογίες οι οποίες έχουν προταθεί και οι οποίες περιγράφονται στο Παράρτημα 1 του [58]. Ανεξαρτήτως της μεθοδολογίας που θα υιοθετηθεί, στο [58] παρατίθεται ένα σύνολο κριτηρίων τα οποία θα πρέπει να εξετάζουν οι υπεύθυνοι επεξεργασίας προκειμένου να αποφαίνονται αν το περιεχόμενο της ΕΑΠΔ είναι πλήρες. Συγκεκριμένα:

- Πρέπει να παρέχεται ***συστηματική περιγραφή των πράξεων επεξεργασίας*** (άρ. 35 παρ. 7 στοιχ. α'):
    - λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας
    - καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος τήρησης
    - παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας
    - προσδιορίζονται οι πόροι στους οποίους αποθηκεύονται ή από τους οποίους διέρχονται τα δεδομένα (υλικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)
    - λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας[44]
- Πρέπει να εκτιμώνται η ***αναγκαιότητα και η αναλογικότητα*** των πράξεων επεξεργασίας (άρ. 35 παρ. 7 στοιχ. β')
    - μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει:
        - καθορισμένων, ρητών και νόμιμων σκοπών (άρ. 5 παρ. 1 στοιχ. β')

[44] Βλ. υπο-ενότητα 10.4

- της νομιμότητας της επεξεργασίας (άρ. 6)
- κατάλληλων, συναφών και περιορισμένων στα αναγκαία δεδομένων (άρ. 5 παρ. 1 στοιχ. γ')
- της περιορισμένης διάρκειας τήρησης (άρ. 5 παρ. 1 στοιχείο ε')

o μέτρα που συμβάλλουν στη **διαφύλαξη των δικαιωμάτων** των υποκειμένων των δεδομένων:

- πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρ. 12, 13 και 14)
- δικαίωμα πρόσβασης και δικαίωμα στη φορητότητα των δεδομένων (άρ. 15 και 20)
- δικαίωμα διόρθωσης και διαγραφής (άρ. 16, 17 και 19)
- δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρ. 18, 19 και 21)
- σχέσεις με τους εκτελούντες την επεξεργασία (άρ. 28)
- διασφαλίζονται οι περιστάσεις που περιβάλλουν τις διεθνείς διαβιβάσεις (Κεφ. V)
- προηγούμενη διαβούλευση (άρ. 36)[45]

• Πρέπει τελούν ***υπό διαχείριση οι κίνδυνοι*** για τα δικαιώματα και τις ελευθερίες των υποκειμένων:

o έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων·

- έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90),
- εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων,

[45] Η έννοια της προηγούμενης διαβούλευσης σε μία ΕΑΠΔ εξηγείται στη συνέχεια της παρούσας υποενότητας

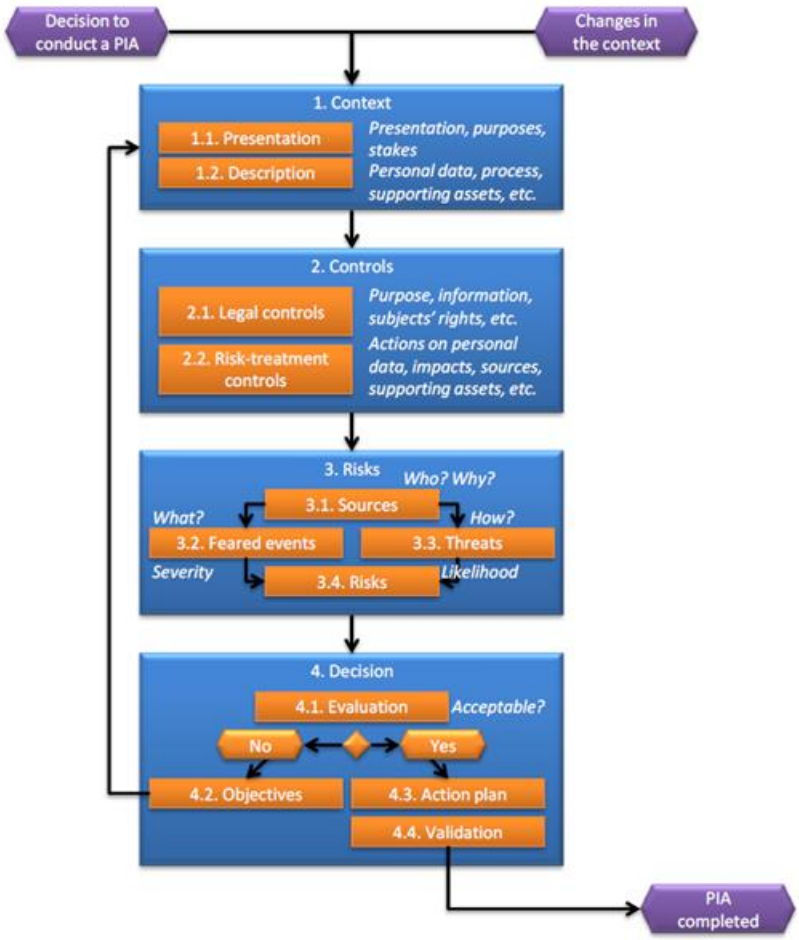


Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- εξακριβώνονται απειλές που θα μπορούσαν να επιφέρουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων,
- εκτιμώνται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90)

  - καθορίζονται τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (άρ. 35 παρ. 7 στοιχ. δ΄ και αιτιολογική σκέψη 90)

- συμμετέχουν τα ενδιαφερόμενα μέρη:
  - ζητείται η γνώμη του Υπευθύνου Προστασίας Δεδομένων (άρ. 35 παρ. 2)
  - ζητείται η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους, όταν ενδείκνυται (άρ. 35 παρ. 9).




**Εικόνα 6 - Βήματα εκπόνησης ΕΑΠΔ (Πηγή: CNIL)**



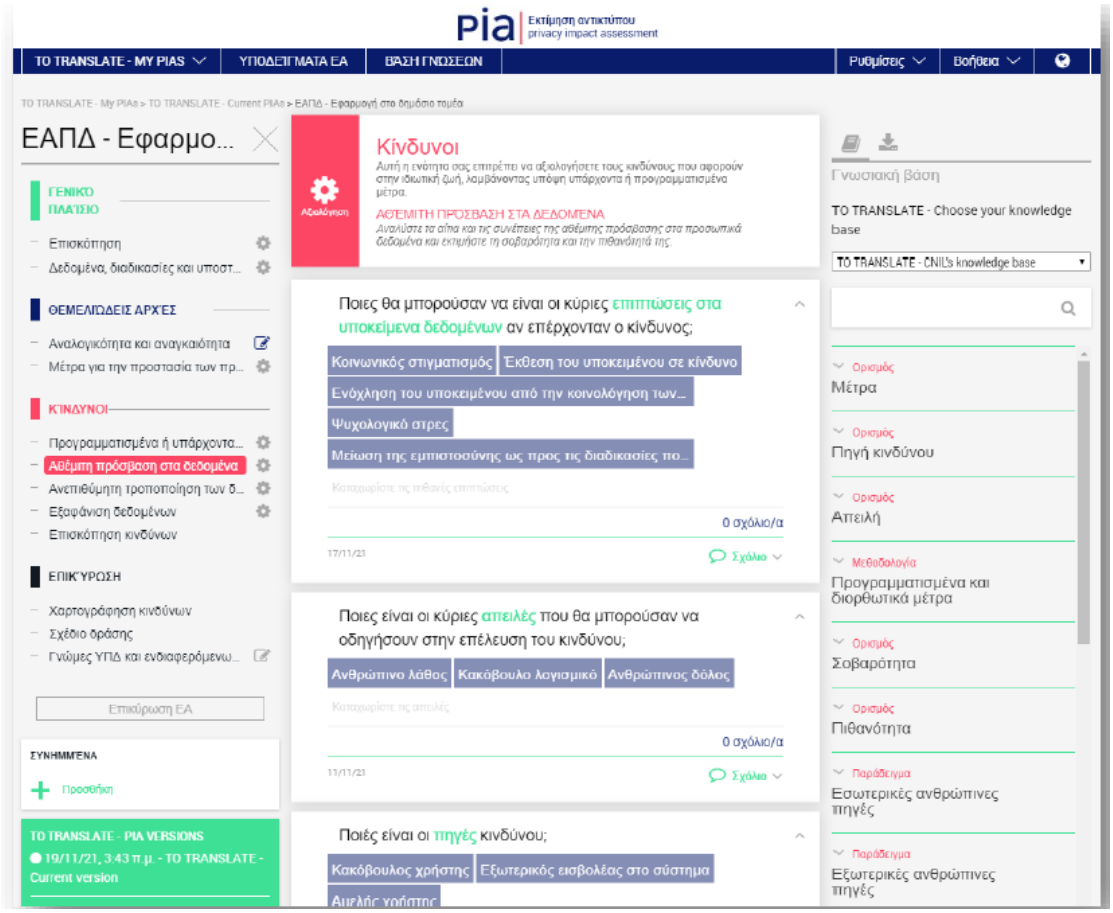
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Μία εκ των μεθοδολογιών για εκπόνηση ΕΑΠΔ έχει αναπτυχθεί από τη Γαλλική Αρχή Προστασίας Δεδομένων (CNIL), η οποία έχει μετουσιωθεί σε λογισμικό ανοιχτού κώδικα το οποίο είναι ελεύθερα διαθέσιμο από τον διαδικτυακό τόπο της CNIL [61]. Το εν λόγω λογισμικό παρέχει, μέσα από ένα γραφικό περιβάλλον, ένα σύνολο ερωτήσεων που καλείται να απαντήσει ένας υπεύθυνος επεξεργασίας όταν εκπονεί μία ΕΑΠΔ, εμφανίζοντας στο τέλος με μορφή διαγράμματος την απεικόνιση του κινδύνου (όπως τον αξιολογεί ο υπεύθυνος επεξεργασίας μέσα από τις απαντήσεις του) αλλά και τα μέτρα που αντιστοιχούν στην αντιμετώπιση του κάθε κινδύνου. Χρήσιμο συνοδευτικό υλικό υπάρχει στον ως άνω διαδικτυακό σύνδεσμο. Τα ερωτήματα που καλείται να απαντήσει ο χρήστης του λογισμικού εντάσσονται στη λογική που περιγράφονται στο [58]: ουσιαστικά, πρώτα παρατίθεται μία περιγραφή της επεξεργασίας (χαρακτηριστικά της, είδος προσωπικών δεδομένων που υφίστανται επεξεργασία, πόροι που υποστηρίζουν την επεξεργασία, ροές δεδομένων, προσβάσεις/αποδέκτες κτλ.), ακολουθεί η ανάλυση των σκοπών αυτής, της νομικής της βάσης, της τεκμηρίωσης της σαφήνειας του σκοπού, της διαφάνειας αυτής, της προσφορότητας αυτής, της ελαχιστοποίησης των δεδομένων, του τρόπου ικανοποίησης των δικαιωμάτων κ.α. Κατόπιν, γίνεται ο εντοπισμός κινδύνων και αποτυπώνεται ποια μέτρα εξετάζονται για το μετριασμό τους: οι κίνδυνοι είναι μία συνάρτηση τόσο της σοβαρότητας των συνεπειών όσο και της πιθανότητας εμφάνισής τους. Τέλος, γίνεται η αξιολόγηση των κινδύνων και η λήψη σχετικών αποφάσεων: η απόφαση μπορεί να είναι είτε αποδοχή (δηλαδή ο υπεύθυνος επεξεργασίας θεωρεί ότι οι κίνδυνοι έχουν αντιμετωπιστεί επαρκώς) είτε επανεξέταση (δηλαδή ο υπεύθυνος επεξεργασίας θεωρεί ότι πρέπει να εξεταστεί εκ νέου η ΕΑΠΔ) είτε διαβούλευση με την εποπτική Αρχή (βλ. στη συνέχεια).

Ενδεικτικό δείγμα οθόνης του λογισμικού της CNIL για την εκπόνηση μίας ΕΑΠΔ δίνεται στην Εικόνα 7 (αφορά το σημείο της διαδικασίας όπου καταγράφονται οι κίνδυνοι από αθέμιτη πρόσβαση στα δεδομένα, για μία συγκεκριμένη επεξεργασία που χρησιμοποιείται απλά ως παράδειγμα).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης




**Εικόνα 7 - Δείγμα οθόνης από το λογισμικό της CNIL (έκδοση: Ιούνιος 2021)**

☞ Από τα ανωτέρω καθίσταται σαφές ότι αν εκπονηθεί σωστά μία ΕΑΠΔ και αντιμετωπιστούν, βάσει αυτής, αποτελεσματικά όλοι οι κίνδυνοι, τότε για την εν λόγω επεξεργασία θα έχει εκπληρωθεί και η αρχή της προστασίας δεδομένων ήδη από το σχεδιασμό. Ωστόσο, όπως είδαμε και στην Ενότητα 8, η προστασία δεδομένων ήδη από το σχεδιασμό είναι μία γενική αρχή που πρέπει να διέπει κάθε επεξεργασία, ανεξαρτήτως κινδύνου, ενώ η ΕΑΠΔ είναι υποχρεωτική μόνο για επεξεργασίες υψηλού κινδύνου (όπως τις εξειδικεύει η εκάστοτε εποπτική αρχή με τον κατάλογο που εκδίδει).

Τέλος, σημειώνεται ότι όταν η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας παρουσιάζουν πολλές ομοιότητες με επεξεργασία για την οποία έχει διενεργηθεί ΕΑΠΔ, τότε δεν χρειάζεται να εκπονηθεί εκ νέου ΕΑΠΔ αλλά μπορούν



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

να αξιοποιηθούν τα αποτελέσματα της προηγούμενης.

**Διαβούλευση με την εποπτική Αρχή**

Αφού ολοκληρωθεί η ΕΑΠΔ, είναι πιθανό ο υπεύθυνος επεξεργασίας να κρίνει ότι κάποιοι κίνδυνοι δεν είναι δυνατό να αντιμετωπιστούν επαρκώς και παραμένουν υψηλοί. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη της εποπτικής αρχής πριν από την επεξεργασία: πρόκειται για την έννοια της *προηγούμενης διαβούλευσης* (βλ. άρθρο 36 παρ. 1 του ΓΚΠΔ). Κατά τη διαβούλευση ο υπεύθυνος επεξεργασίας παρέχει κάθε πληροφόρηση που απαιτείται προκειμένου η Αρχή να παρέχει γραπτώς συμβουλές, ενώ υπάρχει και χρονικό περιθώριο 8 εβδομάδων για την Αρχή (με δυνατότητα παράτασης προθεσμίας κατά έξι εβδομάδες, αν υπάρχει πολυπλοκότητα στη σχεδιαζόμενη επεξεργασία).

**Παράδειγμα:** Δημόσιος φορέας έχει την υποχρέωση από νόμο να αναρτά στο διαδίκτυο όλα τα επιδόματα που χορηγεί σε φυσικά πρόσωπα, για σκοπούς διαφάνειας. Ένα από τα επιδόματα σχετίζεται με στήριξη εθνοτικής μειονότητας. Ο φορέας διενεργεί την ΕΑΠΔ, προσδιορίζει κάποια μέτρα για την ελαχιστοποίηση των δεδομένων και τον περιορισμό των κινδύνων, αλλά σε κάθε περίπτωση, καθώς οφείλει να εφαρμόσει το νόμο, προκύπτει ανάρτηση ειδικών κατηγοριών προσωπικών δεδομένων για κάποιους ταυτοποιήσιμους πολίτες. Καθώς η δημοσιοποίηση ειδικών κατηγοριών προσωπικών δεδομένων επιφέρει εξ ορισμού υψηλό κίνδυνο, τον οποίο ο φορέας θεωρεί ως αποδεκτό, ο φορέας οφείλει να προβεί σε διαβούλευση με την εποπτική αρχή.

**Η ΕΑΠΔ στο Δημόσιο Τομέα**

Τα ανωτέρω ισχύουν προφανώς για κάθε περίπτωση υπευθύνου επεξεργασίας, είτε πρόκειται για φορέα του Δημοσίου Τομέα είτε για ιδιωτικό φορέα. Ωστόσο, κρίσιμο είναι να εξεταστεί ειδικότερα η περίπτωση όπου μία σκοπούμενη από Δημόσιο φορέα επεξεργασία προσωπικών δεδομένων, από την οποία δύνανται να προκύψουν υψηλοί



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, πρόκειται να ενσωματωθεί σε νομοθετική διάταξη. Αντίστροφα, γεννώνται ενδεχομένως ερωτήματα για υπάρχουσες επεξεργασίες υψηλού κινδύνου από φορείς του Δημοσίου Τομέα, οι οποίες προβλέπονται σε νομοθετική διάταξη και η οποία τέθηκε σε εφαρμογή προ του ΓΚΠΔ (όταν δεν υπήρχε η υποχρέωση εκπόνησης ΕΑΠΔ).

Ως προς τα ανωτέρω, στο [58] αναφέρεται ότι δεν απαιτείται νέα εκτίμηση αντικτύπου όταν:

- Η επεξεργασία αφορά έννομη υποχρέωση του υπευθύνου επεξεργασίας (αρ. 6 (1) (γ)) ή σε εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημοσίας εξουσίας (αρ. 6 (1) (ε)) και
- έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, και
- το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη ΕΑΠΔ ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης.

(εκτός εάν τα Κράτη-Μέλη κρίνουν απαραίτητη τη διενέργεια της εν λόγω εκτίμησης πριν από τις δραστηριότητες επεξεργασίας).

Συνεπώς, προκρίνεται ρητά, εν όψει νέου νομοθετήματος, η εκπόνηση ΕΑΠΔ κατά την κατάρτιση του αντίστοιχου νομοθετήματος: εφόσον έχει γίνει στο στάδιο αυτό, δεν χρειάζεται νέα ΕΑΠΔ. Βέβαια, όπως επίσης σημειώνεται στο [58], "*όταν διενεργείται ΕΑΠΔ στο στάδιο της επεξεργασίας της νομοθεσίας που παρέχει τη νομική βάση της επεξεργασίας, ενδέχεται να απαιτείται επανεξέταση πριν από την εφαρμογή της, διότι η ψηφισθείσα νομοθεσία ενδέχεται να διαφέρει από τη νομοθετική πρόταση με τρόπο που να επηρεάζει ζητήματα προστασίας των δεδομένων και της ιδιωτικής ζωής. Επιπλέον, μπορεί να μη διατίθενται επαρκή τεχνικά στοιχεία που αφορούν την πραγματική επεξεργασία κατά τον χρόνο θέσπισης της νομοθεσίας, ακόμη και αν αυτή συνοδευόταν από ΕΑΠΔ. Στις εν λόγω περιπτώσεις, ενδέχεται να παραμένει αναγκαία η διενέργεια συγκεκριμένης ΕΑΠΔ πριν από τη διενέργεια των δραστηριοτήτων επεξεργασίας»*. Ως εκ τούτου, και λαμβάνοντας υπόψη ότι πολλές φορές μία νομική

διάταξη έχει γενικό χαρακτήρα και διάφορα επιμέρους θέματα ρυθμίζονται σε, π.χ. Υπουργική Απόφαση με κατάλληλη νομοθετική εξουσιοδότηση, θα πρέπει, μετά και τη θέσπιση του αντίστοιχου νομοθετήματος, να εκπονείται ΕΑΠΔ από τον υπεύθυνο επεξεργασίας, προκειμένου να ληφθούν οι κατάλληλες αποφάσεις για διάφορες πτυχές της επεξεργασίας.

Σημειώνεται ότι ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων έχει εκδώσει χρήσιμες κατευθυντήριες γραμμές για τους Δημόσιους φορείς, αναφορικά με την ανάλυση της αναγκαιότητας ενός σχεδιαζόμενου μέτρου [62], ενώ έχει εκδώσει και κατευθυντήριες γραμμές για την αναλογικότητα των μέτρων που περιορίζουν τα θεμελιώδη δικαιώματα της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων [63].

Όπως επίσης προβλέπεται στο [58], για υφιστάμενες πράξεις επεξεργασίας δεν απαιτείται ΕΑΠΔ, εφόσον οι πράξεις αυτές έχουν ήδη ελεγχθεί από εποπτική αρχή σύμφωνα με το προ του ΓΚΠΔ νομικό πλαίσιο και δεν έχει επέλθει καμία ουσιαστική μεταβολή. Για παράδειγμα, εφόσον υπό το ν. 2472/1997 η Αρχή είχε εξετάσει μία επεξεργασία και είχε χορηγήσει σχετικά με αυτή άδεια στον υπεύθυνο επεξεργασίας, τότε δεν χρειάζεται νέα ΕΑΠΔ για αυτήν την επεξεργασία (π.χ. περίπτωση χορήγησης αδειών σε νοσοκομεία για επεξεργασία ευαίσθητων δεδομένων υγείας ή περίπτωση χορήγησης άδειας για την επεξεργασία μέσω του Συστήματος Ηλεκτρονικής Συνταγογράφησης) – εφόσον βέβαια δεν έχουν επέλθει αλλαγές. Πλέον βέβαια, καθώς οι άδειες είχαν περιορισμένη χρονική ισχύ, τριών ή πέντε ετών, οι περισσότερες άδειες έχουν λήξει συνεπώς απαιτείται η διενέργεια ΕΑΠΔ.

**Ερώτηση δραστηριότητας**: Σε ποιες από τις παρακάτω περιπτώσεις απαιτείται η εκπόνηση ΕΑΠΔ; Για αυτές που απαιτείται, τεκμηριώστε αν ενδείκνυται, κατά τη γνώμη σας, να ζητηθεί η γνώμη των υποκειμένων των δεδομένων.

1) Δημόσιος φορέας επιθυμεί να αξιοποιήσει ένα εργαλείο DLP (Data Loss Prevention) για την αποτροπή πιθανής διαρροής δεδομένων που επεξεργάζεται. Το εργαλείο αυτό, για να «ανιχνεύει» τυχόν διαρροές, ελέγχει κάθε κίνηση εισερχόμενη ή εξερχόμενη του δικτύου που προορίζεται σε υπάλληλο ή προέρχεται από υπάλληλο (π.χ. ηλεκτρονική αλληλογραφία): με έξυπνες τεχνικές ανιχνεύει λέξεις-κλειδιά στην



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κίνηση του δικτύου που είναι πιθανό (αλλά όχι βέβαιο) να συνεπάγονται διαρροή δεδομένων, όπως π.χ. ΑΜΚΑ, ΑΦΜ κτλ.

2) Δήμος επιθυμεί να εγκαταστήσει κάμερες σε συγκεκριμένο δημόσιο χώρο για τον οποίο είναι αρμόδιος, λόγω πολλών συμβάντων που γίνονται βραδινές ώρες, όπου η είσοδος του χώρου κλείνει και δεν επιτρέπεται η είσοδος.

3) Υπουργείο θα αποστείλει μαζικά προσωποποιημένα ηλεκτρονικά μηνύματα σε όλους τους πολίτες οι οποίοι έχουν εγγραφεί στις ηλεκτρονικές του υπηρεσίες, προκειμένου να τους ενημερώσει για σημαντική αλλαγή στη νομοθεσία η οποία τους αφορά.

4) Οργανισμός Συγκοινωνιών θα εγκαταστήσει κάμερες στις αποβάθρες σταθμών τραίνου, για σκοπούς ασφάλειας.

5) Δήμος επιθυμεί την εγκατάσταση καμερών σε προαύλιους χώρους σχολείου, λόγω συμβάντων που γίνονται νυχτερινές ώρες.

6) Δημόσιος φορέας θα αναθέσει σε εξωτερική εταιρεία, ως εκτελούσα την επεξεργασία, τη διαχείριση της μισθοδοσίας των υπαλλήλων του.

7) Βάσει νόμου, ανατίθεται σε Δημόσια Αρχή η χρήση τεχνικών τεχνητής νοημοσύνης για την αποκάλυψη περιπτώσεων φοροδιαφυγής. Μία ΕΑΠΔ εκπονήθηκε πριν τη ψήφιση του σχετικού νομοθετήματος, η οποία αποτυπώνεται στην αιτιολογική έκθεση αυτού. Ειδικότερα ζητήματα, όπως υπό ποιες προϋποθέσεις θα αξιοποιούνται αυτές οι τεχνικές, τι ρυθμίσεις (configuration) θα έχουν, αν θα παράγονται αποκλειστικά αυτοματοποιημένα αποτελέσματα ή αν θα παρεμβαίνει ανθρώπινος παράγοντας, θέματα που άπτονται της άσκησης των δικαιωμάτων των υποκειμένων κτλ. θα ρυθμιστούν με Υπουργική Απόφαση.

## 10.4 Κώδικες δεοντολογίας

Ο ΓΚΠΔ εισάγει στο άρθρο 40 την έννοια των κωδίκων δεοντολογίας, ως ένα προαιρετικό εργαλείο λογοδοσίας. Η έννοια των κωδίκων δεοντολογίας του άρθρου 40 προσομοιάζει αλλά δεν ταυτίζεται με την έννοια με την οποία ο εν λόγω όρος ήταν ήδη γνωστός. Θα μπορούσε να ειπωθεί, απλοϊκά ίσως, ότι αποτελούν «κανόνες καλής πρακτικής» αλλά σε πολύ συγκεκριμένο πλαίσιο και με συγκεκριμένα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

χαρακτηριστικά.

Συγκεκριμένα, οι κώδικες δεοντολογίας του ΓΚΠΔ έχουν τα εξής χαρακτηριστικά:

1) Είναι τομεακοί, υπό την έννοια ότι ρυθμίζουν ειδικότερα έναν τομέα λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά αυτού αναφορικά με τη συμμόρφωση με το ΓΚΠΔ, προσδιορίζοντας ζητήματα όπως (βλ. άρθρο 40 παρ. 2) τη θεμιτή και με διαφάνεια επεξεργασία, τα έννομα συμφέροντα που επιδιώκουν οι υπεύθυνοι επεξεργασίας σε συγκεκριμένα πλαίσια, τη συλλογή δεδομένων προσωπικού χαρακτήρα, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα, την ενημέρωση του κοινού και των υποκειμένων των δεδομένων, την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, την ενημέρωση και την προστασία των παιδιών και τον τρόπο απόκτησης της συγκατάθεσης του ασκούντος τη γονική μέριμνα του παιδιού, τα μέτρα και τις διαδικασίες που αναφέρονται στα άρθρα 24 και 25 και τα μέτρα για τη διασφάλιση της ασφάλειας της επεξεργασίας που αναφέρεται στο άρθρο 32, τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές και την ανακοίνωση των εν λόγω παραβιάσεων δεδομένων προσωπικού χαρακτήρα στα υποκείμενα των δεδομένων, τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς, ή εξωδικαστικές διαδικασίες και άλλες διαδικασίες επίλυσης διαφορών για την επίλυση διαφορών μεταξύ υπευθύνων επεξεργασίας και υποκειμένων των δεδομένων όσον αφορά την επεξεργασία.
2) Καταρτίζονται από ενώσεις ή φορείς που εκπροσωπούν υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία (βλ. άρθρο 40 παρ. 2). Συνεπώς, **δεν μπορεί ένας οργανισμός να καταρτίσει αυτοτελώς έναν κώδικα δεοντολογίας** – κατά την έννοια του άρθρου 40 του ΓΚΠΔ – για τις επεξεργασίες που πραγματοποιεί: ο κώδικας πρέπει να καταρτιστεί από φορέα ή ένωση που εκπροσωπεί τον οργανισμό και ακολούθως ο οργανισμός, με διαδικασίες που θα πρέπει να προβλέπει ο ίδιος ο κώδικας, να προσχωρήσει σε αυτόν.
3) Οι κώδικες πρέπει να εξειδικεύουν την πρακτική εφαρμογή του ΓΚΠΔ και να αντικατοπτρίζουν με ακρίβεια τη φύση της δραστηριότητας ή του τομέα

επεξεργασίας. Θα πρέπει να παρέχουν σαφείς βελτιώσεις τομεακού επιπέδου όσον αφορά στη συμμόρφωση με τη νομοθεσία για την προστασία των δεδομένων. Ένας κώδικας δεν θα πρέπει απλώς να αναδιατυπώνει τον ΓΚΠΔ. Αντίθετα, θα πρέπει να αποσκοπεί σε μια συγκεκριμένη, πρακτική και ακριβή κωδικοποίηση του τρόπου εφαρμογής του ΓΚΠΔ. Τα συμφωνημένα πρότυπα και κανόνες πρέπει να είναι μη διφορούμενα, συγκεκριμένα, εφικτά και εκτελεστά (ελέγξιμα) [64].

4) Κατά την κατάρτιση ενός κώδικα δεοντολογίας ή κατά την τροποποίηση ή την επέκταση ενός τέτοιου κώδικα, ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία θα πρέπει να διαβουλεύονται με τα ενδιαφερόμενα μέρη, μεταξύ άλλων και με υποκείμενα των δεδομένων, όπου αυτό είναι εφικτό, και να λαμβάνουν υπόψη όσες παρατηρήσεις υποβάλλονται και όσες απόψεις διατυπώνονται στο πλαίσιο αυτών των διαβουλεύσεων (βλ. αιτιολογική σκέψη 99 του ΓΚΠΔ).
5) Ο κώδικας χρήζει κατάλληλων μηχανισμών για τη διασφάλιση της δέουσας παρακολούθησης της εφαρμογής των κανόνων του, καθώς και αποτελεσματικών και ουσιαστικών μέτρων ελέγχου και επιβολής της συμμόρφωσής του (βλ. άρθρο 40 παρ. 4 του ΓΚΠΔ)[46].
6) Το σχέδιο κώδικα δεοντολογίας υποβάλλεται στην αρμόδια εποπτική αρχή προς έγκριση (ήτοι, για εθνικό κώδικα δεοντολογίας, στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) – βλ. άρθρο 40 παρ 5 του ΓΚΠΔ. Εφόσον ο κώδικας εγκριθεί, η Αρχή δημοσιεύει τον κώδικα (άρθρο 40 παρ 6 του ΓΚΠΔ)[47].

Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας από τους σχετικούς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς

[46] Εάν ο κώδικας αφορά επεξεργασίες που διενεργούνται από μη δημόσιες αρχές ή φορείς, πρέπει να προβλέπει φορέα παρακολούθησης (monitoring body), σύμφωνα με το άρθρο 41 του ΓΚΠΔ. Ωστόσο, για περιπτώσεις δημόσιων φορέων ή αρχών, δεν υπάρχει υποχρέωση για φορέα παρακολούθησης του κώδικα (βλ. άρθρο 41 παρ. 5 του ΓΚΠΔ).

[47] Ειδικότερες διαδικασίες προβλέπονται για περίπτωση κωδίκων δεοντολογίας διασυνοριακού χαρακτήρα – οι οποίοι όμως δεν αφορούν δημόσιους φορείς και αρχές.

εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (βλ. άρθρο 35 παρ. 8 του ΓΚΠΔ). Περαιτέρω, η τήρηση εγκεκριμένου κώδικα δεοντολογίας δύναται επίσης να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις της παραγράφου 1 του άρ. 32 αναφορικά με την ασφάλεια της επεξεργασίας. Επίσης, όπως θα συζητηθεί και στην Ενότητα 12, κατά τη λήψη απόφασης από την εποπτική αρχή σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη ένα σύνολο παραμέτρων, μεταξύ των οποίων και η τήρηση εγκεκριμένων κωδίκων δεοντολογίας σύμφωνα με το άρ. 40.

**Παράδειγμα:** Ένας Δήμος επιθυμεί να καταρτιστεί κώδικας δεοντολογίας κατά την έννοια του άρθρου 40 του ΓΚΠΔ που θα εξειδικεύει κανόνες αναφορικά με τη συμμόρφωση με το ΓΚΠΔ για το σύνολο των επεξεργασιών που πραγματοποιεί. Σύμφωνα με το άρθρο 40 όμως, οι κώδικες αυτοί δεν αναπτύσσονται από υπευθύνους επεξεργασίας αλλά από φορείς/ενώσεις που τους εκπροσωπούν. Στη συγκεκριμένη περίπτωση, ένας τέτοιος κώδικας θα μπορούσε να δημιουργηθεί, π.χ., από Κεντρική ή Περιφερειακή ένωση Δήμων, για το σύνολο των Δήμων που εντάσσονται σε αυτή.

**Ερώτηση δραστηριότητας**: Ένα Πανεπιστήμιο έχει υιοθετήσει εσωτερικό κώδικα δεοντολογίας για το σύνολο των ερευνητικών προγραμμάτων που εκπονεί, στον οποίο ρυθμίζονται, μεταξύ άλλων, και ζητήματα προστασίας προσωπικών δεδομένων που ενδεχομένως προκύπτουν κατά την εκπόνηση ερευνητικών προγραμμάτων. Το Πανεπιστήμιο θεωρεί ότι έχει συμμορφωθεί με τις επιταγές του άρθρου 40 του ΓΚΠΔ. Σχολιάστε σχετικά ως προς το αν έχει δίκιο ή όχι, εξηγώντας το σκεπτικό σας.

## 10.5 Πιστοποιήσεις

Οι πιστοποιήσεις του άρθρου 42 του ΓΚΠΔ αποτελούν ένα ακόμα προαιρετικό εργαλείο λογοδοσίας. Ειδικότερα, σύμφωνα με το εν λόγω άρθρο, δύνανται να θεσπιστούν μηχανισμοί πιστοποίησης προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον ΓΚΠΔ των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Ο ΓΚΠΔ δεν ορίζει ρητώς τον



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

όρο «πιστοποίηση»: σύμφωνα με το ΕΣΠΔ [65], η πιστοποίηση αναφέρεται στην επιβεβαίωση τρίτου μέρους αναφορικά με πράξεις επεξεργασίας υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία. Άρα, δεν πιστοποιούνται οργανισμοί συνολικά αλλά πράξεις επεξεργασίας που οι οργανισμοί εκτελούν. Το πιστοποιητικό είναι μία δήλωση συμμόρφωσης. Σε κάθε περίπτωση βέβαια, η πιστοποίηση δεν περιορίζει την ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για συμμόρφωση προς τον ΓΚΠΔ ούτε θίγει τα καθήκοντα και τις αρμοδιότητες των εποπτικών αρχών (άρ. 42 παρ. 4 του ΓΚΠΔ).

Οι πιστοποιήσεις χορηγούνται από ειδικά προς τούτο διαπιστευμένους φορείς πιστοποίησης. Στην Ελλάδα, οι φορείς πιστοποίησης διαπιστεύονται από το ΕΣΥΔ (Εθνικό Σύστημα Διαπίστευσης), σύμφωνα με τα όσα προβλέπονται στο άρθρο 37 παρ. 1 του ν. 4624/2019. Η διαπίστευση ενός φορέα πιστοποίησης γίνεται βάσει του προτύπου EN-ISO/IEC17065:2012 και σύμφωνα με συμπληρωματικές απαιτήσεις διαπίστευσης που έχουν οριστεί από την Αρχή[48] (βλ. Απόφαση 25/2020 της Αρχής [66]). Ο ρόλος του φορέα πιστοποίησης είναι να εκδίδει, να επανεξετάζει, να ανανεώνει και να ανακαλεί πιστοποιήσεις (άρθρο 42 παρ. 5 και 7 του ΓΚΠΔ) βάσει ενός μηχανισμού πιστοποίησης και εγκεκριμένων από την Αρχή κριτηρίων (άρθρο 42 παρ. 5 του ΓΚΔΠ). Αυτό απαιτεί από τον ιδιοκτήτη του σχήματος πιστοποίησης να δημιουργήσει και να καθορίσει κριτήρια πιστοποίησης, τα οποία θα πρέπει να εγκριθούν από την Αρχή.

Αναφορικά με τα κριτήρια πιστοποίησης, όπως αναφέρει το ΕΣΠΔ [65], η θέσπισή τους θα πρέπει να εστιάζει στην επαληθευσιμότητα, στη βαρύτητα και στην καταλληλότητα των κριτηρίων πιστοποίησης για την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ. Τα κριτήρια πιστοποίησης θα πρέπει να διατυπώνονται κατά τρόπο ώστε να είναι σαφή και κατανοητά και να είναι δυνατή η πρακτική εφαρμογή τους. Το πεδίο εφαρμογής της πιστοποίησης στοχεύει σε πράξεις ή σειρές πράξεων επεξεργασίας. Σε αυτές μπορούν να συγκαταλέγονται διαδικασίες διακυβέρνησης ως οργανωτικά μέτρα, συνεπώς ως αναπόσπαστα μέρη μιας πράξης επεξεργασίας (π.χ. η

[48] Σύμφωνα με το μηχανισμό συνεκτικότητας του άρθρου 63 του ΓΚΠΔ, οι εν λόγω συμπληρωματικές απαιτήσεις εγκρίθηκαν από το ΕΣΠΔ.

διαδικασία που έχει θεσπιστεί για τη διαχείριση καταγγελιών στο πλαίσιο της επεξεργασίας δεδομένων υπαλλήλων για τον σκοπό της καταβολής μισθού [65]).

Η πιστοποίηση χορηγείται σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία για μέγιστη περίοδο τριών ετών και μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι εξακολουθούν να πληρούνται οι σχετικές απαιτήσεις. Η πιστοποίηση ανακαλείται, ανάλογα με την περίπτωση, από τους φορείς πιστοποίησης ή από την αρμόδια εποπτική αρχή (βλ. άρθρο 42 παρ. 7 του ΓΚΠΔ).

**Παράδειγμα:** Ένα Υπουργείο θα ήθελε να πιστοποιηθεί για τις πράξεις επεξεργασίας που κάνει για την ασφαλή αυθεντικοποίηση των χρηστών που εγγράφονται στις ηλεκτρονικές του υπηρεσίες και την περαιτέρω επεξεργασία των δεδομένων αυτών (συμπεριλαμβανομένων των τρόπων άσκησης δικαιωμάτων κτλ.). Για να γίνει αυτό, απαιτούνται: α) να υπάρχει ένας μηχανισμός πιστοποίησης για την εν λόγω περίπτωση (μπορεί να τον αναπτύξει το ίδιο το Υπουργείο, αλλά μπορεί να έχει ήδη αναπτυχθεί από κάποιον άλλο φορέα, είτε Δημόσιο είτε όχι, και το Υπουργείο να αναλάβει να τον υλοποιήσει), β) τα κριτήρια πιστοποίησης του εν λόγω μηχανισμού να έχουν εγκριθεί από την Αρχή, γ) Το ΕΣΥΔ να διαπιστεύσει τουλάχιστον ένα φορέα πιστοποίησης για τον εν λόγω μηχανισμό πιστοποίησης, δ) ο φορέας πιστοποίησης, κατόπιν του ελέγχου που θα κάνει με βάση τις διαδικασίες του, να εκδώσει πιστοποιητικό προς το Υπουργείο για τις συγκεκριμένες πράξεις επεξεργασίας.

## 10.6 Βιβλιογραφία για περισσότερη μελέτη


1. ENISA, “Handbook on security of personal data processing”, Dec. 2017. Διαθέσιμο στο **https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing**
2. ENISA, “Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation”, Jan. 2019. Διαθέσιμο στο




Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions**

3. ENISA, “Pseudonymisation techniques and use practices”, Dec. 2019. Διαθέσιμο στο **https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices**
4. European Data Protection Board, “Guidelines 01/2021 on Examples regarding Data Breach Notification” (under public consultation). Διαθέσιμο στο **https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en**
5. K. G. Paterson, “Applied Cryptography”, The Cyber Security Body of Knowledge, 2021. Διαθέσιμο στο **https://www.cybok.org/media/downloads/Applied_Cryptography_v1.0.0.pdf**
6. Working Party 29, «Guidelines on Data Protection Impact Assessment (DPIA)”, 2017. Διαθέσιμο στο **https://ec.europa.eu/newsroom/article29/items/611236/en** (και στα ελληνικά)
7. Working Party 29, «Guidelines on data breach notification under Regulation 2016/679”, 2018. Διαθέσιμο στο **https://ec.europa.eu/newsroom/article29/items/612052/en** (και στα ελληνικά)



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 11. Η εφαρμογή των υποχρεώσεων στο δημόσιο τομέα

Κατά τη διάρκεια της προετοιμασίας για την εφαρμογή του ΓΚΠΔ οι εποπτικές αρχές προέβησαν σε διάφορες δραστηριότητες για την ενημέρωση και ευαισθητοποίηση των φορέων σε σχέση με την εφαρμογή του ΓΚΠΔ. Για παράδειγμα, η ΑΠΔΠΧ εξέδωσε φυλλάδιο με «οδηγό προετοιμασίας» και ενημερωτικό βίντεο[49] ενώ ενεπλάκη σε διάφορες εκπαιδευτικές δραστηριότητες όπως το χρηματοδοτούμενο από την Ε.Ε. πρόγραμμα "PROBLEM BASED TRAINING ON THE DATA PROTECTION REFORM PACKAGE IN GR AND CY" [70]. Οι εποπτικές αρχές πρότειναν συμμόρφωση μέσω σταδίων, ώστε να είναι απλή η υλοποίηση των νέων υποχρεώσεων του Κανονισμού για κάθε φορέα, είτε δημόσιο είτε ιδιωτικό.

Βέβαια, ο δημόσιος τομέας έχει ιδιαιτερότητα ως προς τη σχέση του με το ΓΚΠΔ, καθώς υπάρχουν ορισμένες διατάξεις του που δεν τον επηρεάζουν ουσιαστικά ενώ έχει να «αντιμετωπίσει» μόνο την εποπτική αρχή του Κ-Μ και όχι τις διαδικασίες συνεργασίας και συνεκτικότητας (βλ. Ενότητα 12). Επίσης, δραστηριότητες του δημοσίου, όπως σχετικά με τους ελέγχους στα σύνορα, το άσυλο και τη μετανάστευση ή για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια, εκφεύγουν του πεδίου εφαρμογής του ΓΚΠΔ. Ως προς αυτές εφαρμόζονται ειδικές (για τις εν λόγω δημόσιες αρχές) διατάξεις.

Ο ΓΚΠΔ διευκολύνει επίσης τις δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας, καθώς δεν θεωρούνται ως αποδέκτες. Συνεπώς, δεν τίθεται θέμα ειδικής ενημέρωσης όταν λαμβάνουν αιτιολογημένα και περιορισμένα δεδομένα, τα οποία είναι απαραίτητα για τις ελεγκτικές τους δραστηριότητες. Βέβαια, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις εν λόγω δημόσιες αρχές θα πρέπει πάντα να συμμορφώνεται προς τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας.

Άλλες ιδιαιτερότητες αφορούν:

- Τις νομικές βάσεις: Η συγκατάθεση είναι «μειωμένης» σημασίας, σε σχέση με

[49] **https://www.youtube.com/watch?v=oahoQP2YaAY** (πρόσβαση 18/1/2022)



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

τον ιδιωτικό τομέα. Το Δημόσιο μπορεί και πρέπει να κάνει χρήση της διάταξης των άρθρων 6 παρ. 2 γ' και ε΄, ώστε οι επεξεργασίες του να βασίζονται σε διατάξεις νόμου, ενώ δεν μπορεί, κατά κανόνα, να κάνει χρήση της διάταξης του άρθρου 6 παρ. 2 στ' (υπέρτερο έννομο συμφέρον).

- Τα δικαιώματα: Το «δικαίωμα στη λήθη» έχει περιορισμένη εφαρμογή για επεξεργασίες που διενεργεί δημόσιος φορέας στο πλαίσιο άσκησης των καθηκόντων του, ενώ είναι εξαιρετικά απίθανη η εφαρμογή του «δικαιώματος στη φορητότητα».

Συνεπώς, ένας Δημόσιος φορέας που λειτουργεί ξεκάθαρα εντός του πλαισίου των –νομικά τεκμηριωμένων- αρμοδιοτήτων του, μπορεί να «αντιμετωπίσει» το ΓΚΠΔ – υπό την έννοια να συμμορφωθεί με τις προβλέψεις τους - με απλά αλλά μεθοδικά βήματα.

☞ Για τη Δημόσια Διοίκηση ο ΓΚΠΔ είναι ένα ακόμα βήμα για περισσότερη διαφάνεια της δράσης της. Είναι μια τεράστια ευκαιρία για να αυξηθεί η εμπιστοσύνη των πολιτών προς το δημόσιο.

Στα επόμενα βήματα παρουσιάζουμε μια προσέγγιση της ΑΠΔΠΧ [71] κατάλληλα τροποποιημένη για την ενέργειες φορέων του Δημοσίου για την εφαρμογή του Κανονισμού. Επισημαίνεται βέβαια ότι, πλέον, δεν πρόκειται για προετοιμασία, αλλά για υποχρέωση, καθώς ο ΓΚΠΔ εφαρμόζεται ήδη από τις 25/5/2018.

## 11.1 Ετοιμάστε ένα σχέδιο

Πρέπει να αντιμετωπίστε τη συμμόρφωση με το ΓΚΠΔ ως ένα (μικρό ή μεγάλο) και σημαντικό έργο.

- ☐ Καταγράψτε, συνοπτικά, τα βήματα που πρέπει να κάνετε ως δημόσιος φορέας για να πετύχετε τη συμμόρφωσή σας με το ΓΚΠΔ.
- ☐ Ορίστε χρόνους για την υλοποίηση του έργου, βρείτε τα κατάλληλα άτομα για τη υλοποίηση κάθε σταδίου.
- ☐ Κάντε μια πρόβλεψη ελλείψεων.
- ☐ Προτεραιοποιήστε, ώστε να καλύψετε πρώτα τις «μεγάλες» ελλείψεις

Στόχος σας: η τελική συμμόρφωση σε «εύλογο» χρονικό διάστημα, δεδομένων των συνθηκών στο φορέα σας



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 11.2 Ετοιμάστε ένα σχέδιο

Τα πρόσωπα-«κλειδιά» του φορέα πρέπει να κατανοήσουν ότι η πιθανότητα να σας δημιουργηθούν προβλήματα συμμόρφωσης είναι μεγάλη. Οι επιπτώσεις από μια απόφαση της ΑΠΔΠΧ που επιβάλλει κυρώσεις στο φορέα μπορεί να αποτελέσουν μεγάλο πλήγμα για την εικόνα του φορέα και την εμπιστοσύνη των πολιτών προς αυτόν. Περαιτέρω, ο ΓΠΚΔ μπορεί να επιφέρει αύξηση στο φόρτο εργασίας του φορέα ακόμα κι αν δεν κάνετε τίποτα. Καθώς οι πολίτες είναι ολοένα και πιο ενημερωμένοι, η πιθανότητα να ασκήσουν δικαιώματα του ΓΚΠΔ αυξάνει.

- ☐ Ενημερώστε τη διοίκηση για την ανάγκη συμμόρφωσης με το ΓΚΠΔ.
- ☐ Επισημάνετε τους κινδύνους από τυχόν μη συμμόρφωση.
- ☐ Εξασφαλίστε τη συνδρομή της διοίκησης για τις επόμενες ενέργειες, ιδίως όσον αφορά ανθρώπινους και οικονομικούς πόρους.

## 11.3 Ορίστε Υπεύθυνο Προστασίας Δεδομένων

Αν δεν το έχετε κάνει, ήδη παραβιάζετε το άρθρο 37 του ΓΚΠΔ, καθώς αποτελεί υποχρέωση για κάθε δημόσιο φορέα. Ο Υπεύθυνος Προστασίας Δεδομένων μπορεί να σας βοηθήσει για την εφαρμογή του ΓΚΠΔ. Αν και ο ρόλος του είναι συμβουλευτικός και όχι αποφασιστικός, μπορεί να συνεισφέρει στην ταχύτερη συμμόρφωση με τις προτάσεις του. Η θέση του είναι βέβαια καινοφανής για το ελληνικό δημόσιο, καθώς λειτουργεί εκτός ιεραρχίας και δημοσιοϋπαλληλικής δομής και λογοδοτεί απευθείας στο υψηλότερο επίπεδο.

- ☐ Ορίστε Υπεύθυνο Προστασίας Δεδομένων.
- ☐ Εξασφαλίστε ότι διαθέτει κατάλληλα επαγγελματικά προσόντα και εμπειρογνωσία στο δίκαιο και τις πρακτικές περί προστασίας δεδομένων, καθώς και στο αντικείμενο του φορέα.
- ☐ Ανακοινώστε τα στοιχεία στην ΑΠΔΠΧ.
- ☐ Δημοσιεύστε τα στοιχεία στην ιστοσελίδα σας.
- ☐ Εξασφαλίστε ότι συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα του φορέα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Εξετάστε πιθανή τροποποίηση του οργανογράμματος του φορέα.
- ☐ Εξασφαλίστε επαρκείς πόρους για την άσκηση των καθηκόντων του.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 11.4 Καταγράψτε

Αναγνωρίστε τα αρχεία με προσωπικά δεδομένα που τηρείτε, ανά δραστηριότητά σας. Άλλωστε, οι δημόσιοι φορείς εμπίπτουν στην υποχρέωση τήρησης αρχείων δραστηριοτήτων επεξεργασίας. Χρησιμοποιήστε τα αρχεία αυτά ως ένα πρώτο βήμα για την «τακτοποίηση» των αρχείων σας. Εξετάστε, τουλάχιστον, τις παρακάτω πηγές για δραστηριότητες επεξεργασίας προσωπικών δεδομένων:

- ☐ Αρχείο εγγράφων πρωτοκόλλου
    - Σίγουρα περιέχουν στοιχεία πολιτών, στοιχεία που περιλαμβάνονται σε έγγραφα.
- ☐ Αρχείο προσωπικού.
- ☐ Αρχεία σε ηλεκτρονικές εφαρμογές:
    - Βρείτε το σκοπό για τα αρχεία αυτά (π.χ. ηλεκτρονικές υπηρεσίες που συνδέονται με το αρχείο πρωτοκόλλου / αρχεία καταγραφής δικαιωμάτων και καταγραφής ενεργειών για τους χρήστες / αρχεία εφαρμογής κατάλληλων δικαιωμάτων πρόσβασης κ.ά.).
- ☐ Ειδικά μητρώα που ενδέχεται να τηρείτε.
- ☐ Αρχεία για σκοπούς «ασφάλειας»: κάμερες, καταγραφή επισκεπτών, καταγραφή στοιχείων πρόσβασης στην ιστοσελίδα
- ☐ Αρχεία για σκοπούς επικοινωνίας (π.χ. λίστα με email, newsletter)

## 11.5 Εξετάστε τη συμμόρφωσή σας

Για κάθε ένα από τους σκοπούς που αναγνωρίσατε στο παραπάνω βήμα, βρείτε:

- ☐ **Γιατί** τηρείτε τα δεδομένα;
    - Με βάση ποια **διάταξη**
- ☐ Πώς έχετε **λάβει** τα δεδομένα;
- ☐ Πώς έγινε η **αρχική συλλογή** των δεδομένων από τα υποκείμενα; Μήπως έγινε συλλογή από άλλη πηγή και όχι από τα υποκείμενα των δεδομένων;
- ☐ Πόσο **χρόνο** προτίθεστε να τηρείτε τα δεδομένα και γιατί;
- ☐ Πόσο **ασφαλής** είναι η τήρηση των δεδομένων
    - Κρυπτογραφούνται;
    - Ψευδωνυμοποιούνται;
    - Από ποια μέλη του προσωπικού σας πρέπει να είναι προσβάσιμα και



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

με τι δικαιώματα πρόσβασης;

- ☐ Μοιράζεστε (**διαβιβάζετε**) τα δεδομένα με άλλους; Προσδιορίστε
  - Π.χ. Δημόσιοι φορείς – Εταιρείες – Πολίτες
- ☐ Οι εταιρείες με τις οποίες συνεργάζεστε είναι έτοιμες για το ΓΚΠΔ;
  - Έχετε κατάλληλες συμβάσεις;
- ☐ Συλλέγετε δεδομένα με **συγκατάθεση**;
  - Ελέγξτε αν η συγκατάθεση πληροί τα κριτήρια του ΓΚΠΔ
- ☐ **Διαβιβάζετε δεδομένα εκτός Ε.Ε.**; Εξασφαλίστε τη νομιμότητα
  - Υπάρχει νόμος ή έστω Μ.Ο.U.;

## 11.6 Εξετάστε τη συμμόρφωσή σας

Αναθεωρήστε τις πολιτικές προστασίας δεδομένων και την παρεχόμενη ενημέρωση. Εξετάστε τι είδους ενημέρωση παρέχετε σήμερα στους πολίτες, σε όλα τα σημεία επαφής με αυτούς. Η ενημέρωση που παρέχετε πρέπει να περιέχει όλα τα στοιχεία που αναγράφονται στα άρθρα 13 και 14 του ΓΚΠΔ, άρα παλαιού τύπου ενημερώσεις δεν είναι επαρκείς.

- ☐ Δημοσιεύστε κατάλληλη Πολιτική Προστασίας Δεδομένων στην ιστοσελίδα σας.
- ☐ Εξασφαλίστε ότι η ενημέρωση περιέχει όλα τα στοιχεία των άρθρων 13 και 14.
- ☐ Εξασφαλίστε ότι η ενημέρωση γίνεται για κάθε σκοπό επεξεργασίας.
- ☐ Ελέγξτε τα πρότυπα έντυπα ή εφαρμογές που παρέχετε προς τους πολίτες, ώστε να περιέχουν κατάλληλη ενημέρωση, όταν συλλέγετε προσωπικά δεδομένα.
- ☐ Αν συλλέγετε δεδομένα από τρίτες πηγές, αναλύστε και βρείτε τον κατάλληλο τρόπο για να παρέχεται ενημέρωση και σε αυτή την περίπτωση.

## 11.7 Αναθεωρήστε τις εσωτερικές διαδικασίες για την ικανοποίηση των δικαιωμάτων του ΓΚΠΔ

Ο ΓΚΠΔ προβλέπει νέα και επαυξημένα δικαιώματα για τους πολίτες και ανταπόκριση σε αυτά σε στενά χρονικά διαστήματα. Η υποχρέωση αυτή εφαρμόζεται



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

και για το δημόσιο. Συνεπώς, είναι χρήσιμο να είστε έτοιμοι για να ανταπεξέλθετε στα αιτήματα αυτά, με κατάλληλες διαδικασίες και ενημερωμένο προσωπικό.

- ☐ Ενημερώστε το προσωπικό σας, ειδικά αυτό σε θέσεις που υποδέχεται κοινό και έγγραφα, ώστε να αναγνωρίζει αιτήματα άσκησης δικαιωμάτων του ΓΚΠΔ.
- ☐ Αναγνωρίστε πιθανά υπερβολικά διοικητικά κόστη από την ικανοποίηση τέτοιων αιτημάτων και προετοιμαστείτε. Θυμηθείτε ότι, κατ' αρχήν, η άσκηση των δικαιωμάτων είναι δωρεάν για τον πολίτη.
- ☐ Ετοιμάστε πρότυπα έγγραφα
    - για ικανοποίηση δικαιωμάτων
    - για άρνηση ικανοποίησης με αιτιολόγηση

Είναι καλό κάθε φορέας να είναι έτοιμος για δύσκολες περιπτώσεις, ώστε να αναγνωρίζει περιπτώσεις προβλημάτων, πολλαπλών ή απρόβλεπτων αιτημάτων. Σε περίπτωση αβεβαιότητας, το προσωπικό πρέπει να γνωρίζει ότι μπορεί να ζητήσει τη συμβουλή του Υπεύθυνου Προστασίας Δεδομένων.

## 11.8 Εκτιμήστε τις επιπτώσεις σε νέες δραστηριότητες επεξεργασίας

Η εκτίμηση αντικτύπου είναι μια ορθή πρακτική και μπορεί να αποκαλύψει «ατέλειες» του φορέα σας στην τήρηση της νομοθεσίας. Κάθε φορά που σχεδιάζετε ένα νέο μέτρο ή προετοιμάζετε την εφαρμογή ενός νέου μέτρου, το οποίο περιέχει επεξεργασία δεδομένων προσωπικού χαρακτήρα, είναι απαραίτητο να εξετάζεται αν απαιτείται εκτίμηση αντικτύπου.

- ☐ Όταν σε διάταξη προβλέπονται μέτρα που συνεπάγονται επεξεργασία για την οποία απαιτείται εκτίμηση αντικτύπου χρήσιμο είναι αυτή να γίνεται πριν την ψήφιση της διάταξης, ως τμήμα της γενικής εκτίμησης αντικτύπου της διάταξης. Διαφορετικά, απαιτείται η διενέργειά της πριν την έναρξη της επεξεργασίας.
- ☐ Αν υπάρχει αμφιβολία και προκύπτει υψηλός κίνδυνος, πραγματοποιήστε διαβούλευση με την Αρχή Προστασίας Δεδομένων.
- ☐ Σε κάθε δημόσιο έργο, το οποίο εισάγει νέα επεξεργασία προσωπικών δεδομένων, η εκτίμηση αντικτύπου πρέπει να αποτελεί τμήμα της αρχικής



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μελέτης.

- Εξασφαλίστε τόσο το “Data Protection by Design” όσο και το “Data Protection by Default”.

☐ Εξετάστε:

- Ποιος θα πραγματοποιήσει την εκτίμηση αντικτύπου;
- Ποιοι εργαζόμενοι σας/τμήματά σας πρέπει να εμπλακούν;
- Ποιος θα αξιολογήσει τα αποτελέσματα της εκτίμησης αντικτύπου;

☐ Εξετάστε αν πριν από τη λήψη σημαντικών νομοθετικών μέτρων έχετε ζητήσει τη γνώμη της ΑΠΔΠΧ.

## 11.9 Ετοιμαστείτε για περιστατικά παραβίασης

Οι στατιστικές, αλλά και η κοινή πρακτική, καταδεικνύουν ότι όσο καλά και να είναι τα μέτρα ασφάλειας ενός φορέα, δεν υπάρχει τέλεια ασφάλεια. Πρακτικά, αυτό σημαίνει ότι σε βάθος χρόνου είναι σίγουρο ότι σε οποιονδήποτε φορέα θα συμβεί ένα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα. Προφανώς, ένα τέτοιο περιστατικό, αν ο φορέας γνωρίζει πώς να το χειριστεί, δεν θα φέρει την καταστροφή.

Επιπλέον των καθιερωμένων μέτρων ασφάλειας, εξετάστε αν:

☐ Μπορείτε να ανιχνεύετε και να αξιολογείτε αν ένα περιστατικό είναι παραβίαση προσωπικών δεδομένων.

☐ Είστε έτοιμοι να γνωστοποιήστε περιστατικό στην ΑΠΔΠΧ.

- Έχετε μελετήσει τη φόρμα υποβολής γνωστοποίησης και έχετε προετοιμάσει τα πεδία σε σχέση με το φορέα σας.
- Τα χρονικά διαστήματα είναι «ασφυκτικά»: 72 ώρες για τη γνωστοποίηση στην ΑΠΔΠΧ, όσο πιο γρήγορα γίνεται στους πολίτες

☐ Είστε έτοιμοι να ενημερώνετε τους πολίτες για περιστατικά παραβίασης που μπορεί να τους επηρεάσουν.

- Έχετε ετοιμάσει πρότυπες επιστολές για επικοινωνία και έχετε μελετήσει τρόπους γραφής που θα βοηθήσουν τον πολίτη, χωρίς να σας προκαλέσουν βλάβη.

☐ Χρησιμοποιείστε όσο μπορείτε τεχνικές κρυπτογράφησης, ειδικά κατά τη διαβίβαση ή τη μεταφορά δεδομένων.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

☐ Εκπαιδεύστε τους υπαλλήλους σας οι οποίοι εκτιμάτε ότι μπορεί να είναι οι συχνότερες πηγές ανθρώπινου λάθους.

- Το μεγαλύτερο ποσοστό περιστατικών παραβίασης οφείλονται σε ανθρώπινη αβλεψία.

☐ Εξετάστε αν σας καλύπτει η υφιστάμενη πολιτική ασφάλειας ή αν πρέπει να αναπτύξετε ειδική πολιτική χειρισμού περιστατικών παραβίασης.

## 11.10 Εξασφαλίστε τη διαρκή σας συμμόρφωση σταδιακά

Η συμμόρφωση με τον Κανονισμό δεν είναι μια εργασία που θα γίνει μόνο μια φορά. Καθώς οι συνθήκες αλλάζουν, έτσι αλλάζουν οι μέθοδοι επεξεργασίας και κυρίως οι κίνδυνοι σε σχέση τα προσωπικά δεδομένα. Είναι ευθύνη κάθε υπεύθυνου επεξεργασίας να αναθεωρεί τις διαδικασίες του.

☐ Αντιμετωπίστε την προστασία των προσωπικών δεδομένων με τη λογική Plan-Do-Check-Act.

☐ Αν υπάρχει αντίστοιχο σύστημα για τη διαχείρισης της ασφάλειας πληροφοριών (ISMS), προσπαθήστε να ενοποιήστε τις διαδικασίες.

☞ Θυμηθείτε: Οι νοοτροπίες των ανθρώπων αλλάζουν πολύ πιο αργά από τα συστήματα. Θα πρέπει να πείσετε ότι η αλλαγή είναι προς το συμφέρον όλων.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 12. Εποπτεία και επιβολή της τήρησης του ΓΚΠΔ

Όπως ήδη είδαμε, ο ΓΚΠΔ έχει καθιερώσει ένα σύστημα προστασίας δεδομένων προσωπικού χαρακτήρα το οποίο έχει ως μια από τις θεμελιώδεις του συνιστώσες τη λειτουργία εποπτικών αρχών, οι οποίες έχουν βασικό καθήκον να επιβλέπουν και, αν χρειαστεί, να επιβάλλουν τη νομοθεσία. Το μοντέλο αυτό δεν είναι νέο· οι εποπτικές αρχές προστασίας δεδομένων ήδη λειτουργούσαν υπό το καθεστώς της οδηγίας 95/46/ΕΚ, ενώ προβλέπονται και από τη σύμβαση 108 του Συμβουλίου της Ευρώπης. Με το ΓΚΠΔ ένας επιπλέον παράγοντας είναι ότι οι αρχές αυτές, οφείλουν να λειτουργούν με ενιαία λογική. Οι διατάξεις του Κανονισμού είναι άμεσα εφαρμόσιμες σε όλη την ΕΕ, συνεπώς, αναμένει κανείς οι αποφάσεις τους να είναι παρόμοιες για παρόμοια ζητήματα και σε όλα τα Κ-Μ. Το μοντέλο που επιλέχθηκε για την λειτουργία των εποπτικών αρχών του ΓΚΠΔ είναι απλό στη λογική του.

- Σε κάθε Κ-Μ υπάρχει μια (τουλάχιστον) εποπτική αρχή.
- Σε δραστηριότητες επεξεργασίας που αφορούν πολλά Κ-Μ, εκδίδεται μια απόφαση, από μια αρχή, με συμφωνία των υπολοίπων.
- Σε Ευρωπαϊκό επίπεδο υπάρχει ένας οργανισμός που συντονίζει τη λειτουργία των αρχών και επιλύει τις διαφορές τους. Ο οργανισμός αυτός απαρτίζεται από τον προϊστάμενο μίας εποπτικής αρχής κάθε Κ-Μ και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων ή τους αντίστοιχους εκπροσώπους τους..

Το κεφάλαιο VI του Κανονισμού αφιερώνεται στο να ρυθμίσει τη λειτουργία των εποπτικών αρχών ενώ το κεφάλαιο VII αφιερώνεται στο να ρυθμίσει τις μεθόδους συνεργασίας των εποπτικών αρχών των διαφόρων Κ-Μ.

## 12.1 Ανεξάρτητες και δημόσιες εποπτικές αρχές

Ο ΓΚΠΔ προβλέπει ότι σε κάθε Κ-Μ μία ή περισσότερες ανεξάρτητες δημόσιες αρχές επιφορτίζονται με την παρακολούθηση της εφαρμογής του. Ας αναλύσουμε την υποχρέωση αυτή:

- **Μία ή περισσότερες**: Η προφανής επιλογή είναι ότι κάθε Κ-Μ έχει μια εποπτική αρχή. Αλλά υπάρχουν Κ-Μ τα οποία λόγω της ιδιαίτερης οργάνωσής τους έχουν επιλέξει να λειτουργούν περισσότερες αρχές. Τυπικότερο παράδειγμα είναι η Ομοσπονδιακή Δημοκρατία της Γερμανίας, όπου υπάρχει μια αρχή σε κάθε κρατίδιο και μια σε ομοσπονδιακό επίπεδο, με



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

διαφορετικές αρμοδιότητες. Η εθνική νομοθεσία ορίζει τον τρόπο συνεργασίας των αρχών αυτών.

- **Ανεξάρτητες**: Κάθε εποπτική αρχή εκτελεί τα καθήκοντά της και ασκεί τις εξουσίες της με πλήρη ανεξαρτησία. Η έννοια της ανεξαρτησίας είναι αρκετά καθορισμένη στο ευρωπαϊκό δίκαιο και στο ΓΚΠΔ. Πρακτικά σημαίνει:
    - Ανεξαρτησία μελών: Τα μέλη των αρχών τελούν τα καθήκοντά τους και ασκούν τις εξουσίες τους χωρίς εξωτερικές επιρροές και δεν ζητούν ούτε λαμβάνουν οδηγίες από κανέναν. Προς τούτο ορίζονται ασυμβίβαστα στα επαγγέλματα μελών, ενώ από τη στιγμή που θα οριστεί ένα μέλος δεν μπορεί να αλλάξει με απόφαση της εκτελεστικής εξουσίας, εκτός κι αν υπάρχουν πολύ σοβαροί λόγοι (π.χ. κάποια παράβαση νόμου ή καταδίκη για πειθαρχικό παράπτωμα)
    - Ανεξαρτησία πόρων: Τα Κ-Μ οφείλουν να παρέχουν στις αρχές ανθρώπινους, τεχνικούς και οικονομικούς πόρους, καθώς και τις αναγκαίες εγκαταστάσεις και υποδομές. Ο ΓΚΠΔ βέβαια, δεν ορίζει συγκεκριμένο αριθμό προσωπικού ή οικονομικών πόρων, αλλά αυτό μπορεί να ελεγχθεί από την Ευρωπαϊκή Επιτροπή.
    - Ανεξαρτησία επιλογής προσωπικού: Ο νόμος για τη λειτουργία κάθε εποπτικής αρχής πρέπει να προβλέπει ότι η αρχή επιλέγει και διαθέτει δικούς της υπαλλήλους, οι οποίοι διοικούνται αποκλειστικά από την εν λόγω αρχή. Συνεπώς, οι διαδικασίες για το προσωπικό των αρχών, ακόμα κι αν ακολουθούν το δίκαιο της κάθε χώρας, πρέπει να επιβλέπονται μόνο από τους επικεφαλής της αρχής. Για παράδειγμα, κανείς Υπουργός δεν μπορεί να έχει επιρροή στις διαδικασίες αυτές.
    - Οικονομικός έλεγχος: Οι αρχές δεν υπόκεινται σε οικονομικό έλεγχο, όσον αφορά την επιλογή της κατανομής των πόρων. Αλλά, αυτό δε σημαίνει ότι δεν οφείλουν να ακολουθούν τη νομοθεσία της χώρας όσον αφορά τον τρόπο διενέργειας των δαπανών. Μάλιστα, ως προς αυτό, ελέγχονται (π.χ. στην Ελλάδα από το Ελεγκτικό Συνέδριο). Συνεπώς, οι αρχές υπόκεινται σε οικονομικό έλεγχο, ο οποίος δεν επηρεάζει την ανεξαρτησία τους.
- **Δημόσιες**: Καθώς ο αρχές επιβλέπουν θεμελιώδες δικαίωμα, μπορεί να είναι



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μόνο δημόσιες.

Τι δεν ορίζει ο ΓΚΠΔ;

Ο τρόπος λειτουργίας και λήψης αποφάσεων των εποπτικών αρχών εναπόκειται αποκλειστικά στο εθνικό δίκαιο. Σε άλλες χώρες οι εποπτικές αρχές λειτουργούν ως συμβούλια (πολυπρόσωπα όργανα, όπως στην Ελλάδα), σε άλλες ως Επίτροποι (μονοπρόσωπα όργανα, όπως στην Κύπρο). Ο Κανονισμός ορίζει ότι κάθε μέλος των εποπτικών αρχών πρέπει να διορίζεται με διαφανή διαδικασία από:

- το κοινοβούλιο κάθε κράτους
- την κυβέρνηση κάθε κράτους
- τον αρχηγό του κράτους τους
- ή από ανεξάρτητο φορέα στον οποίο έχει ανατεθεί, με νόμο του Κ-Μ, ο διορισμός.

Οι προϋποθέσεις για τα μέλη της εποπτικής αρχής και οι βασικοί κανόνες για τη σύσταση της εποπτικής αρχής περιλαμβάνονται στον ΓΚΠΔ και τα Κ-Μ οφείλουν να τους χρησιμοποιούν όταν, με βάση την εσωτερική νομοθεσία, συστήνουν τις αρχές ή ορίζουν τα μέλη τους.

☞ Τα κράτη μέλη συστήνουν τις εποπτικές αρχές, ανάλογα με τη συνταγματική, οργανωτική και διοικητική δομή τους.

## 12.2 Καθήκοντα εποπτικών αρχών

Ο ΓΚΠΔ στο άρθρο 57 ορίζει ρητά τα καθήκοντα των εποπτικών αρχών. Μάλιστα τα καθήκοντα αυτά δε χρειάζεται να επαναληφθούν στους εθνικούς νόμους, όπου υπάρχει όμως η δυνατότητα να προστεθούν περισσότερες αρμοδιότητες σε μια εποπτική αρχή, αρκεί να μην είναι ασύμβατες με αυτές του ΓΚΠΔ.

Κάθε εποπτική αρχή έχει ένα γενικό τεκμήριο αρμοδιότητας, να «*παρακολουθεί και επιβάλλει την εφαρμογή του κανονισμού*» και να «*εκπληρώνει κάθε άλλο καθήκον σχετικό με την προστασία δεδομένων προσωπικού χαρακτήρα*» ενώ αναλυτικότερα οι αρμοδιότητές τους διακρίνονται σε:

- **Ενημέρωσης και ευαισθητοποίησης**:
    - Προωθούν την ευαισθητοποίηση του κοινού σε σχέση με τα προσωπικά δεδομένα με ειδική έμφαση σε δραστηριότητες που



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

απευθύνονται ειδικά σε παιδιά.

- Προωθούν την ευαισθητοποίηση των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία.

- **Συμβουλευτικές**:
  - Συμβουλεύουν, με τρόπο που ορίζεται σε εθνικό νόμο, το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα.
  - Παρέχουν πληροφορίες στα υποκείμενα των δεδομένων, μετά από αίτημά τους, όσον αφορά την άσκηση των δικαιωμάτων τους.
  - Παρέχουν συμβουλή μετά από διαβούλευση με βάση το αρ. 36.
- **Ελεγκτικές - ερευνητικές**:
  - Χειρίζονται τις καταγγελίες, ερευνώντας τες, στο μέτρο που ενδείκνυται.
  - Διενεργούν έρευνες, αυτεπάγγελτα είτε με βάση πληροφορίες από άλλες εποπτικές αρχές ή δημόσιες υπηρεσίες.
- **Ρυθμιστικές**:
  - Παρακολουθούν τις τεχνολογικές και τις εμπορικές πρακτικές.
  - Μπορούν να θεσπίσουν τυποποιημένες συμβατικές ρήτρες.
  - Καταρτίζουν καταλόγους για πράξεις που απαιτούν ΕΑΠΔ.
  - Ενθαρρύνουν την κατάρτιση κωδίκων δεοντολογίας και αν χρειαστεί διατυπώνουν γνώμη και εγκρίνουν τέτοιους κώδικες δεοντολογίας.
  - Ενθαρρύνουν τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας των δεδομένων και εγκρίνουν τα κριτήρια πιστοποίησης. Μπορούν να διενεργούν περιοδική επανεξέταση πιστοποιήσεων που έχουν εκδώσει.
  - Σχεδιάζουν και δημοσιεύουν απαιτήσεις διαπίστευσης φορέα για την παρακολούθηση κωδίκων δεοντολογίας και φορέα πιστοποίησης και μπορούν να διενεργούν τη διαπίστευση, αν προβλέπεται.
- **Αδειοδοτικές**:
  - Επιτρέπουν συμβατικές ρήτρες
  - Εγκρίνουν δεσμευτικούς εταιρικούς κανόνες
- **Συνεργασίας**:



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Συνεργάζονται με τις άλλες εποπτικές αρχές.
- Συμβάλλουν στις δραστηριότητες του Συμβουλίου Προστασίας Δεδομένων.

Από τα παραπάνω, είναι σαφές ότι οι εποπτικές αρχές δεν έχουν ευρεία συμβουλευτική αρμοδιότητα, εκτός κι αν αυτό αφορά τη διαδικασία θέσπισης νομοθετικών μέτρων. Στο στάδιο της νομοθέτησης οι αρχές μπορούν να δρουν προληπτικά, καθώς αποτελούν ένα βασικό σύμβουλο του κράτους. Αλλά αυτό δεν ισχύει όταν μια επεξεργασία έχει φύγει από το στάδιο της νομοθέτησης και του σχεδιασμού. Στο στάδιο της εφαρμογής, υπερισχύει η αρχή της λογοδοσίας και κάθε δραστηριότητα επεξεργασίας πρέπει να τεκμηριώνεται ορθά από τον εκάστοτε υπεύθυνο επεξεργασίας, είτε αυτός είναι δημόσιος φορέας είτε όχι. Ενώ με το παλαιότερο θεσμικό πλαίσιο ένας υπεύθυνος επεξεργασίας είχε τη δυνατότητα να απευθύνει ερώτημα στην Αρχή, ώστε να έχει μια κρίση για τη νομιμότητα μιας επεξεργασίας, αυτό πλέον –λόγω λογοδοσίας- δεν προβλέπεται.

☞ Ως απόρροια της αρχής της λογοδοσίας, η Αρχή δεν έχει υποχρέωση απάντησης σε περίπτωση που ένας υπεύθυνος επεξεργασίας απευθύνεται στην Αρχή, με ερώτημα σε σχέση με τη νομιμότητα κάποια επεξεργασίας [72].

Σημαντικό είναι επίσης ότι οι εθνικές εποπτικές αρχές έχουν περιορισμένη δυνατότητα γενικών γνωμοδοτήσεων σε σχέση με τις διατάξεις του ΓΚΠΔ. Όπως θα δούμε στη συνέχεια, αυτή η αρμοδιότητα αποτελεί αρμοδιότητα του ΕΣΠΔ.

## 12.3 Συνεργασία και συνεκτικότητα

Για να μπορέσουν οι εποπτικές αρχές των Κ-Μ να πετύχουν συνεκτική εφαρμογή του ΓΚΠΔ απαιτείται να συνεργάζονται. Πράγματι, δεν θα είχε νόημα η έννοια της συνεκτικής εφαρμογής του Κανονισμού αν μπορούσε κάθε Αρχή να ερμηνεύει διαφορετικά τις διατάξεις του. Άρα, οι ερμηνείες πρέπει να είναι «κοινής αποδοχής» και επιπλέον, όταν μια υπόθεση αφορά πολλά Κ-Μ, πρέπει να υπάρχει τρόπος συνεργασίας.

Η μόνη εξαίρεση που υπάρχει, αφορά τον έλεγχο δραστηριοτήτων στο δημόσιο τομέα:

☞ Όσον αφορά το Δημόσιο Τομέα, κάθε εθνική εποπτική αρχή έχει **αποκλειστική**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**αρμοδιότητα!**

Αυτό σημαίνει ότι οι δραστηριότητες ενός δημόσιου φορέα ελέγχονται μόνο από την εποπτική αρχή της χώρας του. Προφανώς, οι δραστηριότητες ενός δημόσιου φορέα στην Ελλάδα ελέγχονται μόνο από την ΑΠΔΠΧ. Οι αποφάσεις της δεν μπορούν να επηρεαστούν από τις θέσεις άλλων εποπτικών αρχών σε άλλα Κ-Μ. Όσον αφορά όμως γνωμοδοτήσεις επί των διατάξεων του ΓΚΠΔ, οι εθνικές αρχές δεσμεύονται (και για το δημόσιο τομέα) από τις γνωμοδοτήσεις του ΕΣΠΔ.

### 12.3.1 Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Το όργανο που συντονίζει τη συνεργασία των εποπτικών αρχών της Ε.Ε. (και του Ε.Ο.Χ.) είναι το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ). Αποτελεί εξέλιξη της Ομάδας Εργασίας του άρθρου 29 της οδηγίας 95/46/ΕΚ το οποίο είναι καθαρά γνωμοδοτική αρμοδιότητα και δεν είχε νομική προσωπικότητα. Πλέον αποτελεί όργανο της Ευρωπαϊκής Ένωσης και διαθέτει νομική προσωπικότητα· οι αποφάσεις του μπορεί να προσβληθούν δικαστικά. Απαρτίζεται από τον Προϊστάμενο μιας εποπτικής αρχής από κάθε κράτος μέλος (όταν σε ένα Κ-Μ υπάρχουν παραπάνω από μια αρχές, ορίζεται ένας ως εκπρόσωπος) και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων (η εποπτική αρχή για τους Ευρωπαϊκούς Οργανισμούς) ή τους αντίστοιχους εκπροσώπους τους. Σε διάφορα γνωμοδοτικά θέματα συμμετέχει και εκπρόσωπος της Ευρωπαϊκής Επιτροπής, αλλά χωρίς ψήφο.

Οι αρμοδιότητές του είναι σε δύο βασικούς τομείς:

- **Συνεκτικότητα**: Με την έννοια της διασφάλισης ότι ο ΓΚΠΔ εφαρμόζεται με τον ίδιο τρόπο σε όλα τα Κ-Μ, ακόμα και σε περιπτώσεις που εποπτικές αρχές διαφωνούν για μια υπόθεση.
    - Εξετάζει, κάθε ζήτημα το οποίο αφορά στην εφαρμογή του κανονισμού και εκδίδει **κατευθυντήριες γραμμές**, **συστάσεις** και **βέλτιστες πρακτικές**, με σκοπό να ενθαρρύνει τη συνεκτική εφαρμογή του.
    - Εκδίδει γνώμες σε σχέδια αποφάσεων των εποπτικών αρχών και για ζητήματα γενικής εφαρμογής ή ζητήματος που παράγει αποτελέσματα σε περισσότερα από ένα κράτη μέλη και εκδίδει δεσμευτικές αποφάσεις.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Γνωμοδοτεί επί των κωδίκων δεοντολογίας που εκπονούνται σε επίπεδο Ένωσης

- **Συνεργασία**: με την έννοια ότι πρέπει να εξασφαλίζεται η εφαρμογή του ΓΚΠΔ σε όλη την Ε.Ε/Ε.Ο.Χ, τουλάχιστον για σημαντικά ζητήματα.
  - Προωθεί τη συνεργασία
  - Κοινά προγράμματα κατάρτισης, ανταλλαγή υπαλλήλων, ανταλλαγή γνώσεων και τεκμηρίωσης.

Συνεπώς, διαπιστώνουμε ότι η βασική πηγή νομολογίας και κατευθύνσεων σε σχέση με το ΓΚΠΔ αποτελεί το ΕΣΠΔ, οι αποφάσεις και γνώμες του οποίου δεσμεύουν τα μέλη του. Το ΕΣΠΔ παράγει πλειάδα γνωμοδοτήσεων και κατευθυντηρίων γραμμών κάθε χρόνο, στα οποία αξίζει να ανατρέχει κανείς[50]. Συνεδριάζει αρκετές φορές το χρόνο σε ολομέλεια (περί τις 10) ενώ διαθέτει πολλές υποομάδες, οι οποίες συνεδριάζουν τακτικά, για την επεξεργασία και την προετοιμασία των γνωμοδοτήσεων. Εκτιμάται ότι κάθε έτος πραγματοποιούνται πάνω από 100 συναντήσεις υποομάδων και ομάδων του ΕΣΠΔ, ώστε να επιτευχθεί ο στόχος του Κανονισμού.

### 12.3.2 Υπηρεσία μιας στάσης (One Stop Shop)

Στις περιπτώσεις που μια επεξεργασία είναι διασυνοριακή, όταν ένας υπεύθυνος επεξεργασίας ή ένας εκτελών έχει εγκαταστάσεις σε πολλά Κ-Μ ή επεξεργάζεται δεδομένα από υποκείμενα των δεδομένων που βρίσκονται σε πολλά Κ-Μ, εφαρμόζεται ένας μηχανισμός συνεργασίας των εποπτικών αρχών. Ο μηχανισμός αυτός δεν αφορά το δημόσιο τομέα, καθώς σε αυτόν έχει αποκλειστική αρμοδιότητα η εποπτική αρχή της χώρας του φορέα. Τον περιγράφουμε συνοπτικά για λόγους πληρότητας.

Σε περίπτωση διασυνοριακής επεξεργασίας, για τον υπεύθυνο επεξεργασίας ορίζεται ως επικεφαλής εποπτική αρχή (Lead Supervisory Authority - LSA) η αρχή της χώρας της βασικής του εγκατάστασης [73]. Καθώς όμως ο υπεύθυνος μπορεί να έχει πολλές εγκαταστάσεις ή να επεξεργάζεται δεδομένα υποκειμένων σε πολλά Κ-Μ, οι αρχές αυτών των χωρών αποτελούν ενδιαφερόμενες εποπτικές αρχές (Concerned Supervisory Authority -CSA). Η λειτουργία του μοντέλου αυτού έχει ως εξής:

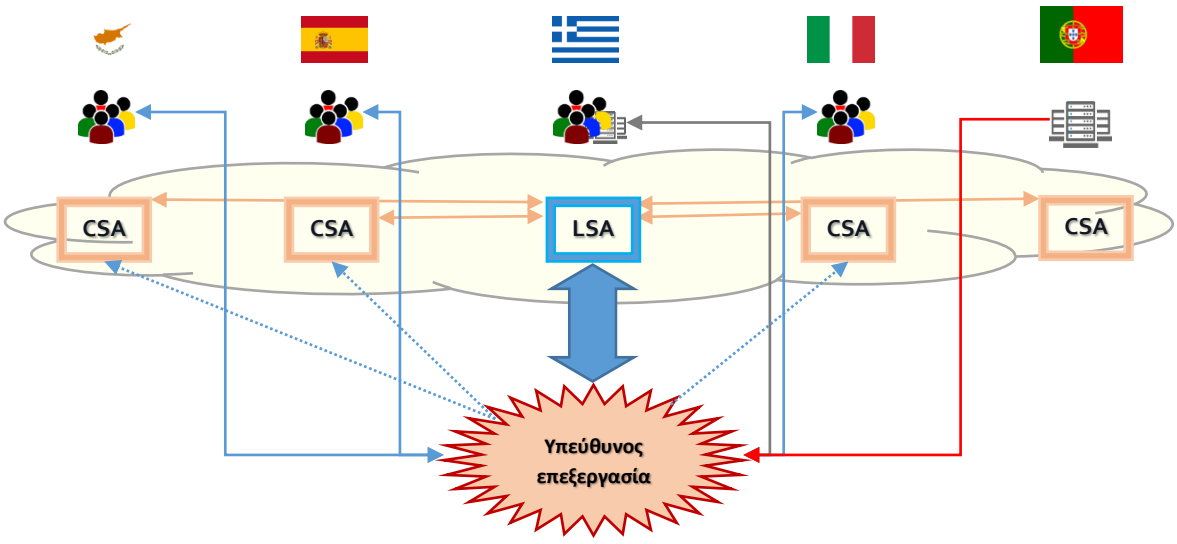
[50] Η ιστοσελίδα του ΕΣΠΔ είναι **https://edpb.europa.eu/edpb_en**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Ο υπεύθυνος επεξεργασίας συνεργάζεται ή ελέγχεται μόνο από μια εποπτική αρχή, την επικεφαλής εποπτική αρχή.
- Το υποκείμενο των δεδομένων μπορεί να απευθυνθεί για καταγγελίες σε όποια αρχή θέλει. Ιδανικά στην αρχή της χώρας του ή στην αρχή της χώρας του υπεύθυνου επεξεργασίας ή στην αρχή του κράτους στο οποίο διαμένει.
- Οι αρχές (επικεφαλής και ενδιαφερόμενες) συνεργάζονται μεταξύ τους, ώστε τελικά να εκδοθεί μια απόφαση για την υπόθεση.
    - Αν οι αρχές διαφωνούν, το ζήτημα παραπέμπεται στο ΕΣΠΔ, το οποίο, με πλειοψηφία, δίνει τη λύση.

Για κατανόηση δείτε το παρακάτω σχήμα.




**Εικόνα 8 - Παράδειγμα λειτουργίας του μηχανισμού συνεργασίας**

## 12.4 Διορθωτικές εξουσίες εποπτικών αρχών

Για την εφαρμογή του ΓΚΠΔ πρέπει να υπάρχουν και τρόποι με τους οποίους μια εποπτική αρχή να μπορεί να τον επιβάλλει. Γι' αυτό στο άρθρο 58 προβλέπεται μια σειρά «διορθωτικών» εξουσιών για τις αρχές. Συνοπτικά διακρίνεται στις εξής κατηγορίες:

- **Α. Προληπτικές:** Η εποπτική αρχή δεν έχει διαπιστώσει παράβαση, αλλά επισημάνει ότι ενδέχεται να υπάρξει παράβαση αν προχωρήσει μια επεξεργασία.
    - Προειδοποιήσεις



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- **Β. Κυρωτικές:** Η εποπτική αρχή διαπιστώνει παράβαση η οποία χρήζει διοικητικής κύρωσης.
    - Επιπλήξεις, για παραβάσεις ελάσσονος σημασίας
    - Διοικητικό πρόστιμο, επιπλέον ή αντί άλλων διορθωτικών μέτρων.
- **Γ. Περιορισμού επεξεργασίας:** Η αρχή διαπιστώνει παράβαση για την οποία κρίνει ότι πρέπει να παρέμβει ώστε να διακοπεί.
    - Προσωρινός ή οριστικός περιορισμός επεξεργασίας.
    - Απόσυρση πιστοποίησης
    - Αναστολή της κυκλοφορίας δεδομένων σε αποδέκτη σε τρίτη χώρα.
- **Δ. Εντολές Συμμόρφωσης:** Η εποπτική αρχή διαπιστώνει παράβαση για την οποία δίνει εντολή στον υπεύθυνο επεξεργασίας να προβεί σε διορθωτικές ενέργειες.
    - Εντολή ικανοποίησης δικαιωμάτων (π.χ. πρόσβασης).
    - Εντολή προσαρμογής στη νομιμότητα, με την εκτέλεσε συγκεκριμένων ενεργειών.
    - Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα σε επηρεαζόμενα υποκείμενα των δεδομένων.
    - Εντολή διόρθωσης ή διαγραφής δεδομένων ή περιορισμού της επεξεργασίας.

### 12.4.1 Πρόστιμα

Όπως είδαμε παραπάνω, τα πρόστιμα είναι μόνο ένα από τα εργαλεία κυρώσεων των εποπτικών αρχών. Ίσως είναι όμως αυτό για το οποίο έγινε «διάσημος» ο ΓΚΠΔ, καθώς πλέον μπορεί να είναι πολύ υψηλά. Αλλά ως γενική αρχή, τα πρόστιμα δεν πρέπει να είναι μεγάλα, αλλά: **αποτελεσματικά, αναλογικά και αποτρεπτικά**. Για τον υπολογισμό του ύψους του προστίμου λαμβάνονται υπόψη συγκεκριμένα κριτήρια που περιγράφονται στο άρθρο 83 παρ. 2 του ΓΚΠΔ. Συνοπτικά αναφέρουμε ότι εξετάζονται:

- Τα βασικά στοιχεία και τα περιστατικά της παραβίασης που οδηγεί στο πρόστιμο
- Αν ο υπεύθυνος ή εκτελών την επεξεργασία είχε τηρήσει τις υποχρεώσεις του (ιδίως τις υποχρεώσεις λογοδοσίας)



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Αν υπάρχει παράγοντες που μετριάζουν τις επιπτώσεις της παραβίασης και αν υπήρξε ορθή συνεργασία με την εποπτική Αρχή.

Ο ΓΚΠΔ προβλέπει δύο κατηγορίες ανωτάτων προστίμων, ανάλογα με το ποια διάταξη παραβιάζεται.

Το ανώτατο πρόστιμο μπορεί να έχει ύψος έως 10 (μικρή κατηγορία) ή έως 20 (μεγάλη κατηγορία) εκατ. €, ή σε περίπτωση επιχειρήσεων, έως 2 ή 4 % αντίστοιχα του συνολικού παγκόσμιου τζίρου του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

Στα **πρόστιμα με το χαμηλότερο άνω όριο** εντάσσονται:

α) υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία: άρθρα 8, 11, 25 έως 39 και 42 και 43

Συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών, Επεξεργασία η οποία δεν απαιτεί εξακρίβωση ταυτότητας, Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, Από κοινού υπεύθυνοι επεξεργασίας, Εκπρόσωποι υπευθύνων ή εκτελούντων μη εγκατεστημένων στην Ένωση, Εκτελών, Αρχεία δραστηριοτήτων, Συνεργασία με την εποπτική αρχή, Ασφάλεια επεξεργασίας, Παραβίαση δεδομένων προσωπικού χαρακτήρα, ΕΑΠΔ, ΥΠΔ

β) υποχρεώσεις του φορέα πιστοποίησης: άρθρα 42 και 43

γ) υποχρεώσεις του φορέα παρακολούθησης κωδίκων δεοντολογίας: άρθρο 41 παράγραφος 4

Στα **πρόστιμα με το υψηλότερο άνω όριο** εντάσσονται:

α) βασικές αρχές για την επεξεργασία, περιλαμβανομένων των όρων που ισχύουν για την έγκριση: άρθρα 5, 6, 7 και 9

Αρχές επεξεργασίας, Νομιμότητα, Συγκατάθεση, Επεξεργασία ειδικών κατηγοριών

β) δικαιώματα των υποκειμένων των δεδομένων: άρθρα 12 έως 22

Διαφάνεια, Ενημέρωση και πρόσβαση, Διόρθωση και διαγραφή, Δικαίωμα εναντίωσης και αυτοματοποιημένη ατομική λήψη αποφάσεων

γ) διαβίβαση δεδομένων σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό: άρθρα 44 έως 49

δ) υποχρεώσεις κεφαλαίου IX (δίκαιο Κ-Μ)

Ελευθερία έκφρασης και πληροφόρησης, Πρόσβαση σε επίσημα έγγραφα, Εθνικός αριθμός ταυτότητας, Απασχόληση, Αρχειοθέτηση προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς

ε) μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή δυνάμει του άρθρου 58 παράγραφος 2 ή μη παροχή πρόσβασης κατά παράβαση του άρθρου 58 παράγραφος 1.

Σε περίπτωση που ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, για τις ίδιες ή για συνδεδεμένες πράξεις επεξεργασίας, παραβιάζει αρκετές διατάξεις του κανονισμού, το συνολικό ύψος του διοικητικού προστίμου δεν μπορεί να υπερβαίνει το ανώτατο ποσό που ορίζεται για τη βαρύτερη παράβαση.

☞ Από τις κατηγορίες προστίμων αντιλαμβανόμαστε ότι ο ΓΚΠΔ προτάσσει τις βασικές αρχές, τη νομιμότητα, τα δικαιώματα, τις διαβιβάσεις και τη συμμόρφωση με τις εντολές των αρχών σε σχέση με τις υποχρεώσεις λογοδοσίας. Συνεπώς, ήδη ο ΓΚΠΔ «υποδεικνύει» σε ποιες ενέργειες πρέπει να δώσει προτεραιότητα ένας υπεύθυνος επεξεργασίας.

Τα Κ-Μ έχουν δυνατότητα να περιορίσουν τα πρόστιμα σε δημόσιους φορείς. Η Ελλάδα επέλεξε να περιορίσει το μέγιστο όριο για το δημόσιο στα 10.000.000 ευρώ, ανεξαρτήτως κατηγορίας παράβασης (άρθρο 39 ν. 4624/2019).

## 12.5 Προσφυγές υποκειμένων

Ο ΓΚΠΔ έχει ενδυναμώσει τα δικαιώματα των υποκειμένων των δεδομένων, καθώς και τη δυνατότητά τους να ασκήσουν νομικά μέτρα για την προστασία τους. Ένα υποκείμενο των δεδομένων μπορεί συνοπτικά να κάνει τις εξής ενέργειες:

- Να υποβάλλει καταγγελία σε εποπτική αρχή.
    - Οι εποπτικές αρχές οφείλουν να ενημερώνουν για τις ενέργειές τους εντός τριμήνου, αλλιώς οι πολίτες μπορούν να προσφύγουν δικαστικά κατά της αρχής.
    - Σε περίπτωση που το υποκείμενο των δεδομένων διαφωνεί με την



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

απόφαση της εποπτικής αρχής, μπορεί να προσφύγει σε δικαστήριο κατά της απόφασης αυτής.

- Το υποκείμενο των δεδομένων έχει το δικαίωμα να αναθέσει σε μη κερδοσκοπικό φορέα, οργάνωση ή ένωση (και υπό προϋποθέσεις) την εκπροσώπησή του στην εποπτική αρχή. Αυτό δίνει τη δυνατότητα καλύτερης εκπροσώπησης σε μεμονωμένους πολίτες, ιδίως αν σκεφτούμε ότι πολλές φορές έχουν να αντιμετωπίσουν μεγάλους οργανισμούς με «στρατιές» δικηγόρων και πολλούς πόρους.

- Να προσφύγει δικαστικά για την προστασία του κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, χωρίς να πρέπει να απευθυνθεί σε εποπτική αρχή.
- Να προσφύγει δικαστικά για αποζημιώσεις κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία.

Οι διατάξεις για τις δικαστικές προσφυγές εφαρμόζονται σύμφωνα με τα οριζόμενα στο δίκαιο κάθε Κ-Μ.

## 12.6 Η εποπτική αρχή της Ελλάδας

Με το ν. 4624/2019 επιβεβαιώθηκε ότι η εποπτική αρχή του ΓΚΠΔ για την Ελληνική Δημοκρατία είναι η αρχή που επέβλεπε το ν. 2472/1997, δηλαδή η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ, αν και η ίδια η Αρχή δεν χρησιμοποιεί κανένα αρκτικόλεξο, παρά μόνο την ονομασία «η Αρχή»). Στα Κεφ. Β του παραπάνω νόμου (άρθρα 9 -20), ορίζονται οι προϋποθέσεις για τη λειτουργία της ΑΠΔΠΧ. Προβλέπεται:

- 7 μελής σύνθεση.
    - Της Αρχής προΐσταται ο Πρόεδρος ενώ η ολομέλειά της αποτελείται από 6 μέλη. Για τον Πρόεδρο και τα μέλη έχουν οριστεί αναπληρωτές. Ως Πρόεδρος της Αρχής υπηρετεί πρώην δικαστικός
    - Για τα μέλη σύμφωνα με το νόμο, επιλέγονται πρόσωπα εγνωσμένου κύρους, τα οποία διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους εμπειρία σε τομείς που έχουν σχέση με την αποστολή και τις αρμοδιότητες της Αρχής. Παραδοσιακά επιλέγονται τουλάχιστον 3 μέλη ΔΕΠ νομικής και πληροφορικής



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

(αναλογία 2 προς 1) ενώ ο Πρόεδρος είναι πρώην ανώτατος δικαστικός (έχουν υπηρετήσει ως Πρόεδροι δύο πρώην πρόεδροι του ΣτΕ, καθώς και πρώην αντιπρόεδροι του ΣτΕ ή του Αρείου Πάγου).

- Η Αρχή αποτελεί πολυπρόσωπο όργανο και λειτουργεί ως επταμελής ολομέλεια για τις σημαντικές υποθέσεις, σε τριμελή τμήματα για τυπικές υποθέσεις και πρόσφατα και ως μονοπρόσωπο όργανο για απλές υποθέσεις (δηλαδή με απόφαση Προέδρου ή ενός μέλους).
- Η Αρχή λογοδοτεί προς το Κοινοβούλιο.
- Η ΑΠΔΠΧ δεν είναι αρμόδια για πράξεις επεξεργασίας από δικαστικές και εισαγγελικές αρχές στο πλαίσιο των δικαστικών τους καθηκόντων, ενώ δεν μπορεί να ελέγξει διαβαθμισμένα δεδομένα για δραστηριότητες εθνικής ασφάλειας.
- Στο ν. 4624/2019 της αποδίδονται καθήκοντα κι αρμοδιότητες επιπλέον του ΓΚΠΔ. Συγκεκριμένα:
    - Μπορεί να εκδίδει οδηγίες και συστάσεις για ζητήματα στα οποία δεν έχει αρμοδιότητα το ΕΣΠΔ, όπως σε επεξεργασίες που περιορίζονται εκτός Ελληνικής Επικράτειας.
    - Μπορεί να θέτει προτεραιότητα κατά την εξέταση υποθέσεων κατά την κρίση της
    - Μπορεί να συνάπτει μνημόνια συνεργασίας με ΑΕΙ και δημόσιους φορείς.
- Υπάρχει επίσης πρόβλεψη για έκδοση Π/Δτος με το οποίο εξειδικεύεται η λειτουργίας της οργανικής μονάδας της Γραμματείας της Αρχής, με ευρεία εξουσιοδότηση, ώστε να καλύπτονται οι προϋποθέσεις του ΓΚΠΔ. Το Π.Δ, αυτό δεν έχει ακόμα εκδοθεί.
- Τέλος, όπως και με το παλαιότερο θεσμικό πλαίσιο, δικαστική προσφυγή κατά αποφάσεων της ΑΠΔΠΧ μπορεί να γίνει μόνο στο ΣτΕ. Αυτό δείχνει την αυξημένη σημασία που ο Έλληνας νομοθέτης έδωσε στην κατοχύρωση των αποφάσεών της.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 12.7 Βιβλιογραφία για περισσότερη μελέτη

Ο.Ε. αρ. 29 - Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679 [74]



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 13. Προσωπικά δεδομένα στις ηλεκτρονικές επικοινωνίες και το Διαδίκτυο

Η προστασία των προσωπικών δεδομένων ειδικότερα στον τομέα των ηλεκτρονικών επικοινωνιών και στο Διαδίκτυο αποκτά μία ιδιάζουσα βαρύτητα, λόγω των αυξημένων κινδύνων που ελλοχεύουν για επέμβαση στην προσωπική σφαίρα των χρηστών. Πράγματι, η τεχνολογία – η οποία διαρκώς εξελίσσεται – παρέχει πολλές δυνατότητες για παρακολούθηση ηλεκτρονικών επικοινωνιών, όπως επίσης και για συλλογή μεγάλου όγκου δεδομένων από απλούς χρήστες τα οποία μπορούν να οδηγήσουν στην εξαγωγή ασφαλών συμπερασμάτων για αυτούς (π.χ. δημιουργία καταναλωτικού προφίλ, εξαγωγή συμπερασμάτων αναφορικά με τη συμπεριφορά τους, τα ενδιαφέροντά τους, τις πεποιθήσεις του κτλ.). Εξ αυτού, κρίθηκε αναγκαίο να θεσπιστούν ειδικότεροι κανόνες για την προστασία των προσωπικών δεδομένων στους εν λόγω τομείς.

## 13.1 Σχετική νομοθεσία σε ελληνικό και ευρωπαϊκό επίπεδο

Σε επίπεδο ΕΕ, ήδη δύο χρόνια μόλις μετά την Οδηγία 95/46/ΕΚ, είχε εκδοθεί η Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. Η εν λόγω Οδηγία είχε ενσωματωθεί στην εθνική έννομη τάξη με το ν. 2774/1999. Η εν λόγω Οδηγία ωστόσο καταργήθηκε το 2002, οπότε και αντικαταστάθηκε από την **Οδηγία 2002/58/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (γνωστή με τον όρο «**Οδηγία e-Privacy**») [11]. Η εν λόγω Οδηγία, όπως τροποποιήθηκε μεταγενέστερα με την *Οδηγία 2009/136/ΕΚ* [12], είναι σε ισχύ μέχρι και σήμερα.

Στην Ελλάδα, ο νόμος που ενσωματώνει στην εθνική έννομη τάξη την ως άνω Οδηγία είναι ο **ν. 3471/2006** (ο οποίος έχει τροποποιηθεί αναλόγως κατόπιν του ν. 4070/2012 και, βεβαίως, κατήργησε τον προηγούμενο ν. 2774/1999). Ο εν λόγω



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

νόμος εφαρμόζεται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών[51] σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών - περιλαμβανομένων αυτών που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης (βλ. άρθρο 3 παρ 1 του ν. 3471/2006). Ως εκ τούτου, ο εν λόγω νόμος προσδιορίζει, ιδίως, σύνολο υποχρεώσεων νόμιμης επεξεργασίας για την επεξεργασία δεδομένων συνδρομητών[52] ή/και χρηστών[53] υπηρεσιών ηλεκτρονικών επικοινωνιών που είναι διαθέσιμες στο κοινό, οπότε και θέτει πλήθος υποχρεώσεων για παρόχους τηλεπικοινωνιακών υπηρεσιών εντός της Ελλάδας. Οι εν λόγω υποχρεώσεις για τους τηλεπικοινωνιακούς παρόχους δεν αποτελούν αντικείμενο του παρόντος: εξάλλου, πρέπει επίσης να σημειωθεί ότι ο ν. 3471/2006 αφορά μόνο στις διαθέσιμες στο κοινό υπηρεσίες και δίκτυα ηλεκτρονικών επικοινωνιών και όχι ιδιωτικά δίκτυα όπως π.χ. νοσοκομείων και εταιρειών ή ειδικά δίκτυα του Δημοσίου όπως το δίκτυο ΣΥΖΕΥΞΙΣ ή σχολικά/πανεπιστημιακά δίκτυα (βλ. και άρθρο 3 παρ. 1 ν. 3471/2006 και αντίστοιχη διάταξη της Οδηγίας 2002/58/ΕΚ). Ωστόσο, ο ν. 3471/2006 ρυθμίζει και κάποια επιμέρους ζητήματα επεξεργασίας δεδομένων, τα οποία εμπίπτουν στο είδος επεξεργασιών που μπορεί να πραγματοποιεί φορέας του Δημοσίου Τομέα: αυτά θα είναι και το κύριο αντικείμενο της εν λόγω Ενότητας.

Συναφώς, πρέπει να επισημανθεί ότι σε επίπεδο Ευρωπαϊκής Επιτροπής συζητείται σχέδιο νέου «Κανονισμού e-Privacy», ο οποίος θα αντικαταστήσει την Οδηγία e-Privacy (κατ' αναλογία με το Γενικό Κανονισμό Προστασίας Δεδομένων, ο οποίος κατήργησε την Οδηγία 95/46/ΕΚ). Μία εκ των επιδιώξεων του νέου Κανονισμού φαίνεται να είναι και η ενσωμάτωση κατάλληλων προβλέψεων αναφορικά με τις

[51] Ως «υπηρεσίες ηλεκτρονικών επικοινωνιών» ορίζεται «*οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις*» (άρ. 2 παρ. 8 του ν. 3471/2006).

[52] Ως «συνδρομητής» ορίζεται «*κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών*» (άρ. 2 παρ. 1 του ν. 3471/2006).

[53] Ως «χρήστης» ορίζεται «*κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας*» (άρ. 2 παρ. 2 του ν. 3471/2006).

τεχνολογικές εξελίξεις (όπως το Διαδίκτυο των Πραγμάτων, τα «έξυπνα» δίκτυα κ.α.). Ωστόσο, το νέο αυτό σχέδιο δεν έχει ακόμα οριστικοποιηθεί – και ούτε βεβαίως ψηφιστεί. Ως εκ τούτου, η Οδηγία e-Privacy παραμένει σε εφαρμογή, κατά τη στιγμή που γράφονται αυτές οι γραμμές – και βεβαίως, το ίδιο ισχύει για το ν. 3471/2006.

## 13.2 Σχέση ΓΚΠΔ και νομοθεσίας e-Privacy

Σε πολλούς υπάρχει μία σύγχυση αναφορικά με το αν, για μία επεξεργασία δεδομένων προσωπικού χαρακτήρα, έχει εφαρμογή ο ΓΚΠΔ ή η νομοθεσία e-Privacy (για την Ελλάδα, ο ν. 3471/2006). Αυτό που πρέπει να αποσαφηνιστεί είναι ότι η νομοθεσία e-Privacy είναι ειδικότερη νομοθεσία του ΓΚΠΔ, εστιάζοντας σε κάποια εξειδικευμένα θέματα. Ως εκ τούτου, αν μία επεξεργασία εμπίπτει σε αυτές που ειδικώς ρυθμίζει η e-Privacy νομοθεσία, τότε εφαρμόζεται αυτή ως ειδικότερη (lex specialis) σε σχέση με τον Κανονισμό. Ουσιαστικά, ο ν. 3471/2006 πρέπει να εκλαμβάνεται ως συμπλήρωση και εξειδίκευση του θεσμικού πλαισίου της προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.

## 13.3 Ο ν. 3471/2006 στο Δημόσιο Τομέα

Στη συνέχεια, θα σταθούμε σε συγκεκριμένες διατάξεις του ν. 3471/2006 οι οποίες τυγχάνουν εφαρμογής από υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία που είναι φορείς του Δημοσίου Τομέα. Βέβαια, αυτονόητο είναι ότι οι εν λόγω διατάξεις ισχύουν αντιστοίχως και για μη δημόσιους φορείς.

### 13.3.1 Καταγραφές τηλεφωνικών συνδιαλέξεων

Όπως προβλέπεται στο άρθρο 4 παρ. 3 του ν. 3471/2006, *επιτρέπεται η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων εμπορικής συναλλαγής ή άλλης επικοινωνίας επαγγελματικού χαρακτήρα, υπό την προϋπόθεση ότι και τα δύο μέρη, μετά από προηγούμενη ενημέρωση*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*σχετικά με τον τρόπο καταγραφής, παρέχουν τη συγκατάθεσή τους*.

Η ανωτέρω διάταξη παρέχει τις προϋποθέσεις υπό τις οποίες μπορεί να υπάρξει εξαίρεση στον γενικότερο κανόνα που προσδιορίζεται νωρίτερα στην παρ. 2 του ιδίου άρθρου, ο οποίος είναι ο εξής: «*Απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται άλλως από το νόμο»*. Ως εκ τούτου, ως εξαίρεση, πρέπει να ερμηνεύεται περιοριστικά: δεν επιτρέπεται η καταγραφή τηλεφωνικών συνδιαλέξεων για οποιαδήποτε επικοινωνία επαγγελματικού χαρακτήρα, παρά μόνο για τις περιπτώσεις που ρητώς προσδιορίζονται στην ως άνω διάταξη. Για παράδειγμα, είναι νόμιμη η καταγραφή των συνδιαλέξεων για την παραγγελία προϊόντων και υπηρεσιών (βλ. Ετήσια Έκθεση της Αρχής για το 2006 [67], σελ. 78). Ωστόσο, αν συνδρομητής δεχτεί αζήτητη τηλεφωνική κλήση προωθητικού χαρακτήρα[54], τότε αυτή η κλήση δεν μπορεί να καταγράφεται εξ αρχής, αφού είναι πιθανό ο καλούμενος συνδρομητής να μην ενδιαφέρεται να συνομιλήσει και να ακούσει την προσφορά: η καταγραφή μπορεί να γίνει μόνο αν, κατά τη διάρκεια της συνομιλίας, συμφωνείται με τον καλούμενο συνδρομητή η σύμβαση, η οποία καταγραφή θα πρέπει να γίνεται για το διάστημα της συνομιλίας που αφορά αυτήν ακριβώς τη σύναψη και όχι για το προηγούμενο διάστημα (δηλαδή η καταγραφή δεν πρέπει να ξεκινά από την αρχή της κλήσης, όπου γίνεται ενημέρωση για την εκάστοτε προσφορά) – βλ. σχετικά την Απόφαση 73/2017 της Αρχής [68].

Περιπτώσεις για τις οποίες δεν είναι νόμιμη η καταγραφή τηλεφωνικών συνδιαλέξεων περιγράφονται στη συνέχεια.

**Παράδειγμα**: Σε μία Δημόσια Υπηρεσία, εμφανίζεται το φαινόμενο να καλούν τηλεφωνικά πολίτες οι οποίοι, στην πορεία της συνομιλίας, εκνευρισμένοι καθυβρίζουν ή/και απειλούν την/τον υπάλληλο. Η καταγραφή συνδιαλέξεων με απειλητικό περιεχόμενο δεν εντάσσεται στην εξαίρεση του άρθρου 4 παρ 3 του ν.

[54] Στην Ενότητα 13.3.2.2 θα συζητηθεί η νομιμότητα πραγματοποίησης τηλεφωνικών κλήσεων προωθητικού χαρακτήρα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

3471/2006 και ως εκ τούτου δεν είναι επιτρεπτή. Εξάλλου, σε κάθε περίπτωση μία τέτοια καταγραφή θα υπερέβαινε την αρχή της αναλογικότητας, αφού για την υλοποίησή της θα έπρεπε να καταγράφονται εξ αρχής όλες, ανεξαιρέτως, οι κλήσεις.

**Παράδειγμα**: Οργανισμός επιθυμεί να καταγράφει κλήσεις των υπαλλήλων του με πολίτες, με σκοπό την εκπαίδευση του προσωπικού που απαντά στις κλήσεις – δηλαδή, από μία ηχογραφημένη συνομιλία, να δοθούν ακολούθως κατευθύνσεις στο πώς θα έπρεπε ο υπάλληλος να ανταποκριθεί στις αιτιάσεις του πολίτη. Και αυτή η περίπτωση ωστόσο δεν εντάσσεται στην εξαίρεση του άρθρου 4 παρ 3 του ν. 3471/2006 και ως εκ τούτου δεν είναι επιτρεπτή.

Εφόσον βέβαια για την καταγραφή τηλεφωνικών συνδιαλέξεων σε συγκεκριμένες περιπτώσεις υπάρχει ειδικότερη νομοθεσία, τότε εφαρμόζονται αναλόγως τα όσα προβλέπονται σε αυτή (βλ., π.χ., ενδεικτικώς την Απόφαση 86/2015 της Αρχής [69] αναφορικά με καταγραφή τηλεφωνικών συνδιαλέξεων από υπαλλήλους τηλεπικοινωνιακών παρόχων, όπου η Αρχή έκρινε ότι η εν λόγω καταγραφή που εντάσσεται στο σκοπό διασφάλισης ποιότητας και εντάσσεται στις υποχρεώσεις του παρόχου λόγω σχετικών αποφάσεων της ΕΕΤΤ είναι νόμιμη).

Στο Δημόσιο τομέα, για να μπορεί να γίνει δεκτή η καταγραφή μιας τηλεφωνικής κλήσης απαιτείται η επικοινωνία να έχει σχέση με την αρμοδιότητα του φορέα που αποφασίζει να καταγράψει (κατ' αναλογία της αναφοράς σε επικοινωνία επαγγελματικού χαρακτήρα) και να προκύπτει ότι είναι απαραίτητη η απόδειξη ότι διενεργήθηκε η κλήση, όπως αν ενδεχομένως μπορεί να εγερθούν απαιτήσεις από την πλευρά του καλούντος χρήστη σε σχέση με την μη ανταπόκριση του δημοσίου φορέα.

**Παράδειγμα**: Κλήση προς δημόσιο φορέα ο οποίος έχει αρμοδιότητα να παρέχει τηλεφωνικά υπηρεσίες έκδοσης πιστοποιητικών, ενδέχεται να μπορεί να καταγραφεί, για την απόδειξη της ορθότητας της έκδοσης του πιστοποιητικού.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Τέλος, πρέπει να επισημανθεί, αναφορικά με τη συγκατάθεση και των δύο μελών η οποία είναι απαραίτητη προϋπόθεση για την καταγραφή τηλεφωνικής συνομιλίας (ακόμα και αν συντρέχει η εξαίρεση του άρθρου 4 παρ. 3 του ν. 3471/2006), ότι η Αρχή έχει κρίνει, υπό το φως και της Οδηγίας 2002/58/ΕΚ, ότι δεν απαιτείται προηγούμενη συγκατάθεση και των δύο μερών αλλά αρκεί προηγούμενη ενημέρωση του μέρους που δεν έχει την πρωτοβουλία της καταγραφής (βλέπε επίσης και ετήσια έκθεση της Αρχής για το 2006 [67], σελ. 78). Η απαιτούμενη ενημέρωση μπορεί να διενεργηθεί και με ηχογραφημένη ειδοποίηση πριν από την έναρξη της κρίσιμης τηλεφωνικής συνδιάλεξης. Ουσιαστικά, πρόκειται για μία οριακή «opt-out» συγκατάθεση, υπό την έννοια ότι αν δεν εκφράσει αντίρρηση ο συνδιαλεγόμενος ο οποίος ενημερώνεται ότι η κλήση θα καταγραφεί, η ενέργειά του να συνεχίσει τη συνομιλία του εκλαμβάνεται ως συγκατάθεσή του.

### 13.3.2 Προωθητικές ενέργειες με ηλεκτρονικά μέσα

Το άρθρο 11 του ν. 3471/2006 ρυθμίζει το ζήτημα των προωθητικών ενεργειών με ηλεκτρονικά μέσα. Αν και η πλειοψηφία των φορέων του Δημοσίου Τομέα δεν αναμένεται να πραγματοποιεί τέτοιες ενέργειες, εν τούτοις ως πιθανότητα δεν μπορεί να αποκλειστεί: για παράδειγμα, ένας Δήμος που παρέχει μέσα μεταφοράς για αστικές συγκοινωνίες στους δημότες, μπορεί να θέλει να κάνει προσφορές στους δημότες του για κάρτα απεριορίστων διαδρομών. Σε κάθε περίπτωση, είναι ένα ζήτημα που αφορά τον καθένα μας, ως υποκείμενο των δεδομένων, αφού όλοι μας αναμφίβολα έχουμε δεχτεί είτε τηλεφωνική κλήση είτε μήνυμα ηλεκτρονικού ταχυδρομείου με προωθητικό χαρακτήρα.

#### 13.3.2.1 Αυτοματοποιημένες προωθητικές ενέργειες

Η πραγματοποίηση αυτοματοποιημένων (χωρίς ανθρώπινη παρέμβαση) ηλεκτρονικών επικοινωνιών για προωθητική ενέργεια επιτρέπεται μόνο με προηγούμενη ειδική συγκατάθεση του καλούμενο συνδρομητή (“opt-in” συγκατάθεση). Αυτό προβλέπεται στο άρθρο 11 παρ. 1 του ν. 3471/2006, στο οποίο αναφέρονται τα εξής: «*Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με*

*χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς*».

**Παράδειγμα**: Φορέας επιθυμεί να πραγματοποιήσει τηλεφωνικές προωθητικές ενέργειες, καλώντας τυχαία τηλεφωνικούς αριθμούς. Η σχεδίαση της προωθητικής ενέργειας είναι προσανατολισμένη στο να ακούγεται ηχογραφημένο μήνυμα σε όσους απαντούν, το οποίο θα τους ενημερώνει για την προωθητική ενέργεια. Μία τέτοια επεξεργασία δεν επιτρέπεται. Η μόνη περίπτωση που θα ήταν επιτρεπτή μία τέτοια επεξεργασία είναι οι συνδρομητές των εν λόγω αριθμών να είχαν προηγουμένως δώσει ειδική προς τούτο συγκατάθεση στο φορέα (μέσω προηγούμενης επικοινωνίας/συναλλαγής μαζί του, όπου η συγκατάθεση θα αφορά ακριβώς στις αυτοματοποιημένες προωθητικές κλήσεις).

13.3.2.2 Τηλεφωνικές προωθητικές ενέργειες με ανθρώπινη παρέμβαση

Για τις τηλεφωνικές κλήσεις με ανθρώπινη παρέμβαση – ήτοι περιπτώσεις όπου ο καλούμενος θα συνομιλήσει, απαντώντας την κλήση, με άνθρωπο – το άρθρο 11 παρ. 2 του ν. 3471/2006 επιτρέπει την πραγματοποίησή τους ακόμα και χωρίς προηγούμενη ειδική συγκατάθεση: για την ακρίβεια, οι κλήσεις είναι επιτρεπτές με «opt-out» συγκατάθεση, δηλαδή επιτρέπονται εφόσον δεν έχει εκφράσει ειδική ή γενική αντίρρηση ο καλούμενος συνδρομητής.

Ειδικότερα, η ως άνω διάταξη αναφέρει τα εξής: *«Δεν επιτρέπεται η πραγματοποίηση μη ζητηθεισών επικοινωνιών με ανθρώπινη παρέμβαση (κλήσεων) για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής της διαθέσιμης στο κοινό υπηρεσίας, ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις. Ο φορέας υποχρεούται να καταχωρίζει δωρεάν τις δηλώσεις αυτές σε*

*ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερομένου*». Η εν λόγω διάταξη εισάγει την έννοια ενός καταλόγου (μητρώου) που οφείλει να τηρεί κάθε πάροχος τηλεπικοινωνιακών υπηρεσιών, στον οποίο εγγράφεται κάθε συνδρομητής ο οποίος επιθυμεί να μη δέχεται (από τον οποιονδήποτε πιθανό διαφημιζόμενο) τηλεφωνικές προωθητικές ενέργειες με ανθρώπινη παρέμβαση. Το μητρώο αυτό είθισται να αποκαλείται «*μητρώο του άρθρου 11*» ή «*μητρώο opt-out*» (για προφανείς λόγους). Ως εκ τούτου, αν ένας συνδρομητής δεν έχει εγγράψει, με δική του πρωτοβουλία, τον τηλεφωνικό του αριθμό στον εν λόγω κατάλογο του παρόχου της τηλεφωνικής του σύνδεσης (είτε σταθερής είτε κινητής τηλεφωνίας), τότε η πραγματοποίηση τηλεφωνικών προωθητικών ενεργειών με ανθρώπινη παρέμβαση στον εν λόγω τηλεφωνικό αριθμό δεν απαγορεύεται κατ' αρχήν. Αντίστροφα, αν κάποιος συνδρομητής δεν επιθυμεί να δέχεται τέτοιου τύπου κλήσεις, θα πρέπει να εγγράψει τον αριθμό του στο εν λόγω μητρώο του παρόχου του (σημειωτέο ότι η εγγραφή δεν γίνεται αυτόματα με το συμβόλαιό του, θα πρέπει να τη ζητήσει ειδικώς).

Ποιες είναι λοιπόν οι υποχρεώσεις ενός φορέα, ο οποίος ως υπεύθυνος επεξεργασίας σκοπεύει να πραγματοποιήσει προωθητικές τηλεφωνικές ενέργειες με ανθρώπινη παρέμβαση;

α) Πριν την πραγματοποίηση των κλήσεων, πρέπει να διασφαλίσει ότι κανείς καλούμενος τηλεφωνικός αριθμός που θα χρησιμοποιήσει δεν είναι καταχωρημένος στο μητρώο «opt-out» κανενός τηλεπικοινωνιακού παρόχου. Συνεπώς, οφείλει να ζητήσει αντίγραφα των εν λόγω μητρώων[55] από όλους τους παρόχους και να εξαιρέσει, από τις προωθητικές ενέργειες που θα πραγματοποιήσει, αριθμούς που εμφανίζονται σε κάποιο από αυτά τα μητρώα[56].

β) Ακόμα και αν ένας τηλεφωνικός αριθμός δεν είναι εγγεγραμμένος στο μητρώο «opt-out» κανενός τηλεπικοινωνιακού παρόχου, υπάρχει περίπτωση ο εν λόγω

[55] Τα εν λόγω μητρώα περιέχουν μόνο τηλεφωνικούς αριθμούς για συγκεκριμένη ημερομηνία για τον κάθε αριθμό: δεν περιέχουν ονοματεπώνυμα ή άλλα προσωπικά στοιχεία συνδρομητών

[56] Όπως έχει κρίνει η Αρχή (βλ., π.χ., ενδεικτικώς, την Απόφαση 65/2016 [103]), ο διαφημιζόμενος πρέπει να εξασφαλίζει, όταν καλεί έναν τηλεφωνικό αριθμό, ότι ο αριθμός αυτός δεν είναι εγγεγραμμένος στο μητρώο κανενός παρόχου για διάστημα μεγαλύτερο των 30 ημερών (δηλαδή μπορεί να ζητά αντίγραφα των μητρώων μία φορά το μήνα και όχι, π.χ., σε ημερήσια ή εβδομαδιαία βάση).

συνδρομητής να έχει ήδη ασκήσει, ειδικώς στον υπεύθυνο επεξεργασίας, το δικαίωμα εναντίωσης στην επεξεργασία κατά το άρθρο 21 του ΓΚΠΔ[57] – οπότε ο υπεύθυνος επεξεργασίας θα πρέπει επιπροσθέτως να εξαιρεί από τις προωθητικές ενέργειες τυχόν τηλεφωνικούς αριθμούς συνδρομητών οι οποίοι έχουν εναντιωθεί ειδικώς στον υπεύθυνο επεξεργασίας.

13.3.2.3 Προωθητικές ενέργειες μέσω ηλεκτρονικού ταχυδρομείου

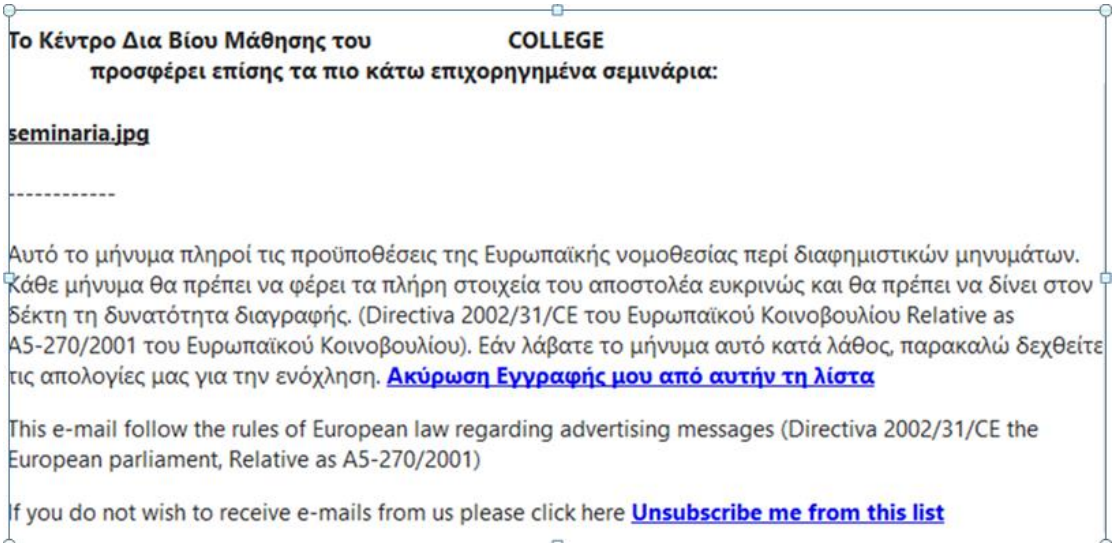
Η πραγματοποίηση προωθητικών ενεργειών μέσω ηλεκτρονικού ταχυδρομείου επιτρέπεται μόνο με προηγούμενη συγκατάθεση του λήπτη του μηνύματος, σύμφωνα με τα προαναφερόμενα στο άρθρο 11 παρ. 1 του ν. 3471/2006. Συνεπώς, κατά κανόνα, κάθε τέτοια λήψη αζήτητου μηνύματος («spam») είναι παράνομη.

Υπάρχει ωστόσο μία εξαίρεση, η οποία - εφόσον συντρέχει - καθιστά επιτρεπτή την αποστολή ενός τέτοιου μηνύματος με «opt-out» επιλογή. Ειδικότερα, σύμφωνα με το άρθρο 11 παρ 3 του ν. 3471/2006, «*τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεση του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων και αυτό κατά τη συλλογή των στοιχείων επαφής, καθώς και σε κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση*».

[57] Τούτο διότι η εγγραφή στο μητρώο «opt-out» εξαιρεί τον τηλεφωνικό αριθμό από κάθε προωθητική ενέργεια, οποιουδήποτε εν δυνάμει διαφημιζόμενου: συνεπώς, εάν κάποιος συνδρομητής δεν θέλει να «αποκόψει» γενικώς τις προωθητικές ενέργειες προς τον ίδιο αλλά θέλει να εναντιωθεί σε συγκεκριμένο υπεύθυνο επεξεργασίας, τότε δεν θα πρέπει να εγγράψει τον αριθμό του στο μητρώο «opt-out» αλλά να ασκήσει ειδικό δικαίωμα εναντίωσης, κατά το άρθρο 21 του ΓΚΠΔ, στον υπεύθυνο επεξεργασίας



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης


Το Κέντρο Δια Βίου Μάθησης του COLLEGE
προσφέρει επίσης τα πιο κάτω επιχορηγημένα σεμινάρια:

seminaria.jpg

---

Αυτό το μήνυμα πληροί τις προϋποθέσεις της Ευρωπαϊκής νομοθεσίας περί διαφημιστικών μηνυμάτων. Κάθε μήνυμα θα πρέπει να φέρει τα πλήρη στοιχεία του αποστολέα ευκρινώς και θα πρέπει να δίνει στον δέκτη τη δυνατότητα διαγραφής. (Directiva 2002/31/CE του Ευρωπαϊκού Κοινοβουλίου Relative as A5-270/2001 του Ευρωπαϊκού Κοινοβουλίου). Εάν λάβατε το μήνυμα αυτό κατά λάθος, παρακαλώ δεχθείτε τις απολογίες μας για την ενόχληση. Ακύρωση Εγγραφής μου από αυτήν τη λίστα

This e-mail follow the rules of European law regarding advertising messages (Directiva 2002/31/CE the European parliament, Relative as A5-270/2001)

If you do not wish to receive e-mails from us please click here Unsubscribe me from this list

**Εικόνα 9 - Παράδειγμα αζήτητου προωθητικού ηλεκτρονικού μηνύματος**

Συνεπώς, σε περιπτώσεις προηγούμενης αντίστοιχης συναλλαγής, μπορεί ο υπεύθυνος επεξεργασίας να ενημερώσει ότι θα χρησιμοποιήσει την ηλεκτρονική διεύθυνση για αντίστοιχες προωθητικές ενέργειες: εφόσον δεν υπάρξει αντίρρηση/εναντίωση, αυτές θα είναι επιτρεπτές (περίπτωση «opt-out» συγκατάθεσης). Βέβαια, κάθε τέτοιο μήνυμα πρέπει να παρέχει με ευχερή τρόπο τη δυνατότητα έκφρασης αντίρρησης στη λήψη αντίστοιχων μηνυμάτων στο μέλλον. Σε όρους ΓΚΠΔ, η χρήση της δυνατότητας «opt-out» λόγω προηγούμενης σχετικής συναλλαγής ισοδυναμεί με τη χρήση της νομικής βάσης του υπέρτερου εννόμου συμφέροντος, με αυστηρά καθορισμένους όρους για το πότε εφαρμόζεται. Στην πράξη, καθώς η διαφήμιση είναι μια νόμιμη δραστηριότητα, αναγνωρίζεται το προβάδισμα των εταιρειών να διαφημίζουν προϊόντα σε υφιστάμενους πελάτες τους.

**Παράδειγμα**: Κέντρο Δια Βίου Μάθησης επιθυμεί να διαφημίσει σεμινάριά του. Αποστέλλει ηλεκτρονικά μηνύματα όπως αυτό που απεικονίζεται στην Εικόνα 9 σε διάφορες ηλεκτρονικές διευθύνσεις χρηστών, από τους οποίους δεν έχει λάβει τη συγκατάθεσή τους, ούτε είχε κάποια προηγούμενη συναλλαγή μαζί τους[58]. Το εν λόγω μήνυμα είναι σαφώς παράνομο με βάση τις διατάξεις του άρθρου 11 του ν.

[58] Προσοχή: Εγείρεται και ζήτημα ως προς τη νομιμότητα αυτής καθ' αυτής της συλλογής των διευθύνσεων ηλεκτρονικού ταχυδρομείου για τον εν λόγω σκοπό, εφόσον η αποστολή των ηλεκτρονικών μηνυμάτων δεν είναι επιτρεπτή.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

3471/2006 (παρά το ότι δίνει τη δυνατότητα έκφρασης αντίρρησης). Σημειωτέο δε ότι επιπροσθέτως παρέχει και λανθασμένη/παραπλανητική ενημέρωση[59] ως προς το νομικό πλαίσιο (αφού η αναφερόμενη Οδηγία 2002/31/ΕΚ δεν έχει καμία σχέση με το νομικό πλαίσιο που διέπει την αποστολή προωθητικών ηλεκτρονικών μηνυμάτων).

**Ερώτηση δραστηριότητας**: Υπό ποιες προϋποθέσεις το ανωτέρω Κολλέγιο (Εικόνα 9) μπορεί να στείλει νομίμως προωθητικά ηλεκτρονικά μηνύματα σε ηλεκτρονικές διευθύνσεις προσώπων από τους οποίους δεν έχει λάβει την προηγούμενη ειδική και ρητή («opt-in») συγκατάθεσή τους; Εξηγείστε αναλυτικά, ενώ επίσης, προτείνετε και αλλαγές που πρέπει να έχει το μήνυμα που εμφανίζεται στην Εικόνα 9.

☞ Αν και δεν διατυπώνεται ρητά στην εν λόγω διάταξη, το ζήτημα των σύντομων γραπτών μηνυμάτων (SMS) εμπίπτει επίσης στην ως άνω διάταξη, οπότε και συντρέχουν οι ίδιες ακριβώς προϋποθέσεις για τη νόμιμη αποστολή τους για προωθητικούς σκοπούς (αυτό πλέον προκύπτει ευθέως από την αιτιολογική σκέψη 67 της οδηγίας 2009/136/ΕΚ η οποία τροποποίησε την οδηγία 2002/58/ΕΚ).

☞ Στην Ελλάδα, οι ρυθμίσεις του άρθρου 11 συνολικά ισχύουν και για συνδρομητές που είναι νομικά πρόσωπα. Για παράδειγμα, δεν επιτρέπεται να σταλεί αζήτητο προωθητικό μήνυμα ηλεκτρονικού ταχυδρομείου σε μία κεντρική ηλεκτρονική διεύθυνση του Φορέα Α (π.χ στην **info@foreasA.gr**).

### 13.3.3 Η περίπτωση των cookies

Ο ν. 3471/2006 περιλαμβάνει μία διάταξη που αφορά γενικά τη δυνατότητα

[59] Γενικά, τέτοιου τύπου «λάθη» σε μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να υποδηλώνουν ότι το μήνυμα δεν είναι απλά κάποιο «spam» αλλά κακόβουλο, οπότε χρήζει ιδιαίτερης προσοχής (όπως να μην «ανοιχτεί» σε καμία περίπτωση το συνημμένο αρχείο)



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αποθήκευσης πληροφορίας, η/και πρόσβασης σε ήδη αποθηκευμένη πληροφορία, στη συσκευή του χρήστη (Η/Υ, κινητό τηλέφωνο, tablet κτλ.). Ειδικότερα, στο άρθρο 4 παρ. 5 του ν. 3471/2006 αναφέρεται το εξής:

«*Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεση του μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει*[60]. *Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής. Τα παραπάνω δεν εμποδίζουν την οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής (…)*»

Στην παραπάνω διάταξη εντάσσεται και το ζήτημα των «cookies», όπως αυτά ορίζονται στο RFC 6265[61]. Με απλά λόγια, τα cookies είναι μικρά αρχεία κειμένου που τοποθετούνται στο χώρο αποθήκευσης (π.χ. σκληρό δίσκο) της συσκευής του χρήστη από τον διακομιστή (server) μιας ιστοσελίδας. Τα cookies μπορούν να εξυπηρετήσουν διάφορους σκοπούς. Για παράδειγμα, δεν θα μπορούσαμε να πραγματοποιήσουμε ηλεκτρονικές αγορές αν δεν χρησιμοποιούνταν κατάλληλα cookies από την ιστοσελίδα του ηλεκτρονικού καταστήματος, τα οποία επιτρέπουν να «αναγνωρίζουν» ότι, μέχρι την ολοκλήρωση της αγοράς, όλες οι ενέργειες (επιλογή προϊόντων, επιλογή τρόπου πληρωμής κτλ.) γίνονται από τον ίδιο χρήστη στην ίδια σύνοδο (session). Τα cookies μπορούν να εξυπηρετήσουν και άλλους σκοπούς, όπως στατιστικούς ή διαφημιστικούς.

Η νομοθεσία μάλιστα για τα cookies εφαρμόζεται **ανεξάρτητα από το αν αυτά συνδέονται με προσωπικά δεδομένα ή όχι**. Καθώς η ePrivacy νομοθεσία δεν αφορά

[60] Προφανώς, η διάταξη αυτή ως προς το σκέλος της ενημέρωσης του συνδρομητή ή χρήστη ερμηνεύεται πλέον υπό τις απαιτήσεις διαφάνειας του ΓΚΠΔ.
[61] Βλ. https://datatracker.ietf.org/doc/html/rfc6265



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μόνο προσωπικά δεδομένα, αλλά ρυθμίζει και ζητήματα απορρήτου, η διάταξη του άρθρου 4 παρ. 5 του ν. 3471/2006 αφορά την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες που βρίσκονται στον τερματικό εξοπλισμό. Ως ειδικότερη νομοθεσία (lex spexialis) εφαρμόζεται πρώτα η νομοθεσία ePrivacy και κατόπιν, εφαρμόζεται ο ΓΚΠΔ κατά το μέρος που κάποια ζητήματα δεν ρυθμίζονται ειδικά.

Τα cookies μπορούν να εγκαθίστανται και από υπευθύνους επεξεργασίας οι οποίοι δεν χειρίζονται τον δικτυακό τόπο στον οποίον βρίσκεται ο χρήστης: για παράδειγμα, ο χρήστης μπορεί να βρίσκεται στην ιστοσελίδα **www.exampleA.gr** και να εγκατασταθεί cookie στον υπολογιστή του, λόγω της επίσκεψής του στην εν λόγω ιστοσελίδα, από άλλη υπηρεσία κοινωνικής δικτύωσης. Αυτά τα cookies ονομάζονται «cookies τρίτου μέρους» (third-party cookies). Διαφορετικά, εφόσον τα cookies εγκαθίσταται από τον υπεύθυνο επεξεργασίας (ή από κάποιον δικό του εκτελούντα επεξεργασία) ο οποίος χειρίζεται τον δικτυακό τόπο που επισκέπτεται ο χρήστης, τότε αναφερόμαστε σε «cookies πρώτου μέρους» (first-party cookies). Στο προηγούμενο παράδειγμα, κάθε cookie που εγκαθίσταται στη συσκευή του χρήστη από τον πάροχο της ιστοσελίδας **www.exampleA.gr**, κατά την επίσκεψη του χρήστη σε αυτή, εμπίπτει σε αυτήν την κατηγορία.

Με βάση την ως άνω διάταξη, και όπως έχει κρίνει ερμηνευτικά και η ελληνική Αρχή υπό το φως και της Γνώμης 4/2012 της Ο.Ε. του Άρθρου 29 [70], τα cookies θα πρέπει να διακρίνονται - με απλά λόγια - σε δύο κατηγορίες (ανεξαρτήτως του αν πρόκειται για πρώτου μέρους ή τρίτου μέρους cookies):

1) Απαραίτητα cookies: πρόκειται για τα cookies εκείνα τα οποία είναι απολύτως αναγκαία για την παροχή της υπηρεσίας της κοινωνίας της πληροφορίας που ζήτησε ρητώς ο χρήστης, υπό την έννοια ότι σε περίπτωση απενεργοποίησης των εν λόγω cookies, η παροχή της υπηρεσίας καθίσταται αδύνατη.
2) Μη απαραίτητα cookies: πρόκειται για τα cookies εκείνα για τα οποία, ακόμα και αν εκλείψουν, η υπηρεσίας της κοινωνίας της πληροφορίας που ζήτησε ρητώς ο χρήστης μπορεί να παρασχεθεί.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Για τα απαραίτητα cookies, η εγκατάστασή τους επιτρέπεται και χωρίς συγκατάθεση του χρήστη. Για τα μη απαραίτητα cookies όμως, η εγκατάστασή τους επιτρέπεται μόνο με σαφή και ειδική συγκατάθεση του χρήστη. Πρόκειται για μία περίπτωση «opt-in συγκατάθεσης», η οποία πρέπει να πληροί το σύνολο των προϋποθέσεων της συγκατάθεσης του ορισμού στο άρθρο 4 περ. 11 και των προϋποθέσεων του άρθρου 7 του ΓΚΠΔ (βλ. ενότητα 5.6), δηλαδή ο χρήστης πρέπει να δηλώσει τη συναίνεσή του με σαφή θετική ενέργεια – το οποίο σημαίνει, για παράδειγμα, ότι δεν πρέπει να υπάρχουν προ-επιλεγμένα εικονίδια συγκατάθεσης για τα συγκεκριμένα cookies (αφού τυχόν μη ενέργεια του χρήστη επί της προ-επιλογής δεν θα πρέπει να εκλαμβάνεται ως συγκατάθεσή του).

☞ Ανεξαρτήτως του αν τα cookies είναι απαραίτητα (οπότε δεν χρειάζεται συγκατάθεση του χρήστη) ή όχι (οπότε είναι απαραίτητη η "opt-in" συγκατάθεση του χρήστη), θα πρέπει να παρέχεται στους χρήστες πλήρης ενημέρωση για τα cookies και τους σκοπούς τους.

**Παράδειγμα**: Ιστοσελίδα Δημόσιου Φορέα δίνει τη δυνατότητα στους πολίτες να συνδέονται με τα διαπιστευτήριά τους προκειμένου να αξιοποιούν τις ηλεκτρονικές υπηρεσίες του, όπως να βλέπουν την κατάσταση των αιτήσεων που έχουν υποβάλει, να μπορούν να υποβάλουν νέες αιτήσεις κ.α. Για τις εν λόγω υπηρεσίες απαιτείται η χρήση cookies για τη διατήρηση της συνόδου του χρήστη μετά τη σύνδεση του χρήστη στις ηλεκτρονικές υπηρεσίες του φορέα (session cookies). Για αυτά τα cookies δεν απαιτείται η συγκατάθεση του χρήστη προκειμένου να εγκατασταθούν στην τερματική του συσκευή. Θα πρέπει βέβαια να παρέχεται ενημέρωση για αυτήν την εγκατάσταση.

**Παράδειγμα**: Κάποιες ιστοσελίδες επιθυμούν την εγκατάσταση cookies για σκοπούς συμπεριφορικής διαφήμισης (behavioral advertising). Η συμπεριφορική διαφήμιση βασίζεται στην ιχνηλάτηση των ιστοσελίδων που επισκέπτεται ο χρήστης στο διαδίκτυο αλλά και των ενεργειών που πραγματοποιεί ηλεκτρονικά (π.χ. τα «click» που κάνει σε συγκεκριμένα προϊόντα) με σκοπό την εξαγωγή συμπερασμάτων για τις



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προτιμήσεις του και το γενικότερο καταναλωτικό του προφίλ. Από την πληροφορία αυτή, δύνανται οι διαφημιζόμενοι να προβάλλουν στοχευμένες διαφημίσεις στο χρήστη σε μελλοντικές πλοηγήσεις του, βάσει του προφίλ του (για αυτό και μπορεί σε διαφορετικούς χρήστες που θα επισκεφτούν ταυτόχρονα, από τις συσκευές τους, την ίδια ιστοσελίδα, να προβληθούν διαφορετικές διαφημίσεις).

Τα cookies αποτελούν μία τεχνολογική προσέγγιση που μπορεί να επιτρέψει την ως άνω ιχνηλάτηση του χρήστη (κατά κύριο λόγο, αν και όχι αποκλειστικώς, είναι cookies τρίτου μέλους για τις διάφορες ιστοσελίδες στις οποίες πλοηγείται ο χρήστης). Η εγκατάσταση τέτοιων cookies απαιτεί, με βάση τα προαναφερόμενα, τη ρητή και ειδική συγκατάθεση του χρήστη, κατόπιν πλήρους ενημέρωσής του.

**Παράδειγμα**: Δημόσιος φορέας θέλει να αξιοποιήσει cookies στην ιστοσελίδα του προκειμένου να εξάγει στατιστικά αναφορικά με την επισκεψιμότητά της. Για το σκοπό αυτό, επιθυμεί να αξιοποιήσει τη σχετική υπηρεσία Google Analytics. Η περίπτωση αυτή των «cookies» όμως δεν εμπίπτει στην εξαίρεση της παρ. 5 του άρθρου 4 ν. 3471/2006, ακόμα και όταν αφορά αποκλειστικά τη στατιστική ανάλυση της επισκεψιμότητας σε μια ιστοσελίδα. Και τούτο γιατί η υπηρεσία μπορεί να παρασχεθεί και χωρίς τη μέτρηση στατιστικών. Συνεπώς, για να εγκαθίσταται ένα τέτοιο cookie χρειάζεται η ρητή και ειδική συγκατάθεση του χρήστη (opt-in).

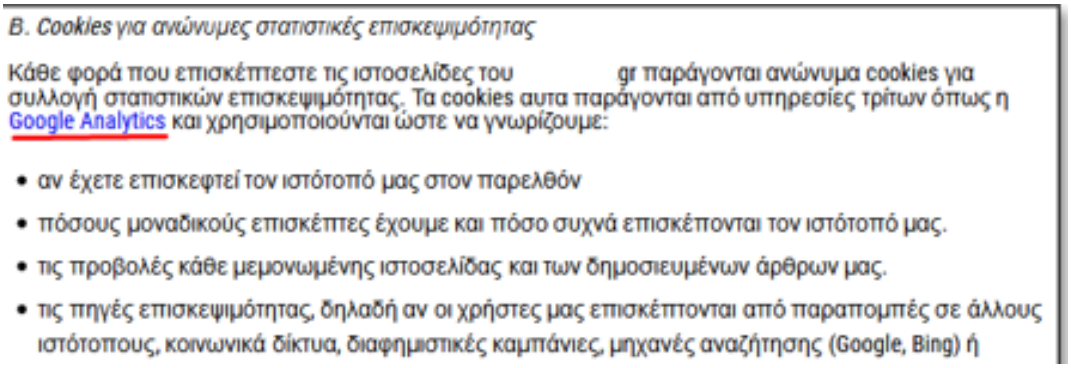
Σημειώνεται ότι, αν και βάσει της διάταξης του άρθρου 4 παρ. 5 του ν. 3471/2006 τα cookies επισκεψιμότητας, είτε είναι πρώτου μέρους είτε τρίτου μέρους (όπως είναι η περίπτωση των Google Analytics), δεν θεωρούνται απαραίτητα και συνεπώς απαιτείται, για την εγκατάστασή τους, η opt-in συγκατάθεση του χρήστη, εν τούτοις το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) αναγνωρίζει την ιδιαιτερότητα αυτού του είδους των cookies και τους χαμηλούς κινδύνους ως προς την ιδιωτικότητα όταν γίνεται εγκατάσταση cookies πρώτου μέρους από την ίδια την ιστοσελίδα. Στην περίπτωση αυτή, έχει προταθεί και από το ΕΣΠΔ και από άλλους φορείς, για τον Κανονισμό e-Privacy, να είναι επιτρεπτή η εγκατάσταση αρκεί να



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

δίνεται η δυνατότητα ανάκλησης της συγκατάθεσης («opt-out» συγκατάθεση)[62].

**Ερώτηση δραστηριότητας**: Στο ενημερωτικό κείμενο μίας ιστοσελίδας εμφανίζεται το απόσπασμα που φαίνεται στην Εικόνα 10 αναφορικά με την υπηρεσία Google Analytics. Σχολιάστε τόσο την πληρότητα της ενημέρωσης, όσο και τη νομιμότητα της εγκατάστασης των εν λόγω cookies που περιγράφονται στο κείμενο αυτό.



*B. Cookies για ανώνυμες στατιστικές επισκεψιμότητας*

Κάθε φορά που επισκέπτεστε τις ιστοσελίδες του gr παράγονται ανώνυμα cookies για συλλογή στατιστικών επισκεψιμότητας. Τα cookies αυτα παράγονται από υπηρεσίες τρίτων όπως η Google Analytics και χρησιμοποιούνται ώστε να γνωρίζουμε:

- αν έχετε επισκεφτεί τον ιστότοπό μας στον παρελθόν
- πόσους μοναδικούς επισκέπτες έχουμε και πόσο συχνά επισκέπτονται τον ιστότοπό μας.
- τις προβολές κάθε μεμονωμένης ιστοσελίδας και των δημοσιευμένων άρθρων μας.
- τις πηγές επισκεψιμότητας, δηλαδή αν οι χρήστες μας επισκέπτονται από παραπομπές σε άλλους ιστότοπους, κοινωνικά δίκτυα, διαφημιστικές καμπάνιες, μηχανές αναζήτησης (Google, Bing) ή

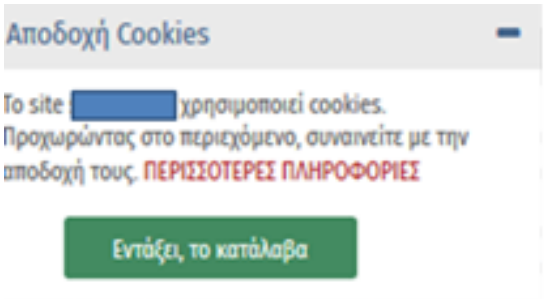
**Εικόνα 10 - Ενημερωτικό κείμενο σχετικά με την υπηρεσία Google Analytics**

**Ερώτηση δραστηριότητας**: Με την επίσκεψη χρήστη σε μία ιστοσελίδα, εμφανίζεται αμέσως, στην κάτω δεξιά γωνία του παραθύρου, το αναδυόμενο παράθυρο που εμφανίζεται στην Εικόνα 11. Σχολιάστε την παρεχόμενη ενημέρωση, αλλά και τη νομιμότητα εγκατάστασης των cookies. (Θεωρείστε ότι αν ο χρήστης επιλέξει «ΠΕΡΙΣΣΟΤΕΡΕΣ ΠΛΗΡΟΦΟΡΙΕΣ» θα λάβει αναλυτική και πλήρη ενημέρωση για όλα τα cookies που εγκαθίστανται, τόσο τα απαραίτητα όσο και τα μη απαραίτητα, χωρίς δυνατότητα επιλογής ή από-επιλογής).

[62] Βλ. σχετικώς την ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, **https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/electronikesepikoinwnies/cookies/statistikh_cookies**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης




**Εικόνα 11 - Αναδυόμενο παράθυρο ενημέρωσης για εγκατάσταση cookies**

Τέλος, επισημαίνουμε ότι εκτός από τα cookies οι παραπάνω ρυθμίσεις εφαρμόζονται σε HTTP/S cookies, σε flash cookies, στον "τοπικό αποθηκευτικό χώρο" (local storage) που εφαρμόζεται στην HTML 5, σε αναγνώριση με τον υπολογισμό του ψηφιακού αποτυπώματος της τερματικής συσκευής ή του χρησιμοποιούμενου φυλλομετρητή (browser), σε αναγνωριστικά που δημιουργούνται από τα λειτουργικά συστήματα (είτε προορίζονται για σκοπό διαφήμισης είτε όχι: IDFA, IDFV, Android ID κ.λπ.), σε αναγνωριστικά υλικού (διεύθυνση MAC, σειριακό αριθμό ή άλλο αναγνωριστικό συσκευής) κ.λπ. Δηλαδή σε κάθε πληροφορία που πρόκειται να αποθηκευτεί ή προέρχεται από την τερματική συσκευή[63] ενός χρήστη. Στην επόμενη ενότητα μπορείτε να βρείτε παραπομπή στις αναλυτικές συστάσεις που έχει εκδώσει η Ελληνική εποπτική αρχή για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες στο ζήτημα της χρήσης ιχνηλατών συμπεριλαμβανομένων των cookies.

## 13.4 Βιβλιογραφία για περισσότερη μελέτη


1. Working Party 29, “Opinion 4/2012 on cookie consent exemption”. Διαθέσιμο στο **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_el.pdf** (η εκδοχή στα ελληνικά)
2. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «Συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες». Διαθέσιμο στο **https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-**


[63] Μπορεί να είναι σταθερός υπολογιστής ή κινητό τηλέφωνο.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**ypeythynon-epexergasias-dedomenon-me-tin-eidiki**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 14. Ειδικά θέματα συμμόρφωσης με το ΓΚΠΔ

Στη συγκεκριμένη Ενότητα, θα αναπτύξουμε κάποια ειδικότερα ζητήματα περιπτώσεων επεξεργασίας, για τα οποία ο ΓΚΠΔ «αφιερώνει» ειδικό Κεφάλαιο (βλ Κεφάλαιο IX αυτού). Συγκεκριμένα, θα σταθούμε σε ζητήματα του Κεφαλαίου IX που άπτονται ιδίως επεξεργασιών του Δημοσίου Τομέα, όπως η ελευθερία έκφρασης και πληροφόρησης (άρθρο 85 του ΓΚΠΔ), η πρόσβαση στα δημόσια έγγραφα (άρθρο 86 του ΓΚΠΔ), η επεξεργασία εθνικού αριθμού ταυτότητας (άρθρο 87 του ΓΚΠΔ), η επεξεργασία στο πλαίσιο της απασχόλησης (άρθρο 88 του ΓΚΠΔ), καθώς και η επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς (άρθρο 89 του ΓΚΠΔ). Για τις εν λόγω περιπτώσεις, ο ΓΚΠΔ δίνει στον εθνικό νομοθέτη την ευχέρεια ρύθμισης ειδικότερων ζητημάτων. Επιπροσθέτως, θα δοθεί έμφαση σε άλλες δύο ειδικές περιπτώσεις οι οποίες παρουσιάζουν ενδιαφέρον: η χρήση συστημάτων βιντεοεπιτήρησης και η χρήση βιομετρικών συστημάτων για την αυθεντικοποίηση προσώπου.

## 14.1 Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης

Στο άρθρο 85 του ΓΚΠΔ, αναφέρεται ότι ο εθνικός νομοθέτης μπορεί να εξισορροπήσει κατάλληλα το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς και για σκοπούς πανεπιστημιακής, καλλιτεχνικής ή λογοτεχνικής έκφρασης: πράγματι, το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης ενδέχεται σε ορισμένες περιπτώσεις να «συγκρούεται» με το δικαίωμα στην προστασία προσωπικών δεδομένων και θα πρέπει να προκύπτει μία δίκαιη εξισορρόπηση στο πλαίσιο της εκάστοτε περίπτωσης. Μάλιστα, στην παράγραφο 2 του εν λόγω άρθρου, ο ΓΚΠΔ προβλέπει τη δυνατότητα, στα Κράτη-Μέλη, να προβλέπουν εξαιρέσεις ή παρεκκλίσεις από «*το κεφάλαιο II (αρχές), το κεφάλαιο III (δικαιώματα του υποκειμένου των δεδομένων), το κεφάλαιο IV (υπεύθυνος επεξεργασίας και εκτελών*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*την επεξεργασία), το κεφάλαιο V (διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς), το κεφάλαιο VI (ανεξάρτητες εποπτικές αρχές), το κεφάλαιο VII (συνεργασία και συνεκτικότητα) και το κεφάλαιο IX (ειδικές περιπτώσεις επεξεργασίας δεδομένων), εφόσον αυτές είναι αναγκαίες για να συμβιβαστεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με την ελευθερία της έκφρασης και πληροφόρησης».*

Ο εθνικός νομοθέτης, με το άρθρο 28 του ν. 4624/2019, ουσιαστικά ορίζει ρητώς ότι, στον βαθμό που είναι αναγκαίο να συμβιβαστεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς, και για σκοπούς ακαδημαϊκής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, δεν εφαρμόζονται: α) το Κεφάλαιο ΙΙ του ΓΚΠΔ «Αρχές», εκτός από το άρθρο 5, β) το Κεφάλαιο ΙΙΙ του ΓΚΠΔ «Δικαιώματα του Υποκειμένου», γ) το Κεφάλαιο IV του ΓΚΠΔ «Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία», εκτός από τα άρθρα 28, 29 και 32, δ) το Κεφάλαιο V του ΓΚΠΔ «Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς», ε) το Κεφάλαιο VII του ΓΚΠΔ «Συνεργασία και συνεκτικότητα και στ) το Κεφάλαιο IX του ΓΚΠΔ «Διατάξεις που αφορούν ειδικές περιπτώσεις επεξεργασίας». Χρήζει όμως ιδιαίτερης επισήμανσης ότι η Αρχή, με την Γνωμοδότηση 1/2020, έκρινε ως προς την εν λόγω διάταξη του ν. 4624/2019 ότι *η ευρύτητα των εν λόγω εξαιρέσεων θέτει υπό διακινδύνευση τον πυρήνα της προστασίας των δεδομένων προσωπικού χαρακτήρα* - ιδίως η εξαίρεση από ορισμένα δικαιώματα, όπως το δικαίωμα εναντίωσης ή ενημέρωσης. Όπως σημειώνεται ειδικότερα στην εν λόγω Γνωμοδότηση:

«*Σημειωτέον ότι η προβλεπόμενη από τον ΓΚΠΔ δυνατότητα θέσπισης των εξαιρέσεων μέσω νομοθετικών μέτρων πρέπει να αιτιολογείται ως αναγκαία (βλ. αρ. 85 παρ. 2 ΓΚΠΔ), τέτοια δε αιτιολογία ελλείπει από την αιτιολογική έκθεση. Επιπλέον, οι εν λόγω εξαιρέσεις πρέπει να αποσκοπούν στην εξισορρόπηση των θεμελιωδών δικαιωμάτων (αιτ.σκ. 153)*[64] *και όχι στην μονομερή απάλειψη ή αποκλεισμό εφαρμογής των*

[64] Σύμφωνα με τη Σκέψη 153 του ΓΚΠΔ, «Το δίκαιο των κρατών μελών θα πρέπει να συμφιλιώνει τους κανόνες που διέπουν την ελευθερία της έκφρασης και της πληροφόρησης, περιλαμβανομένης της



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*δικαιωμάτων στην προστασία των δεδομένων προσωπικού χαρακτήρα».* Στην πράξη, η εξαίρεση του άρθρου 28 του ν. 4624/2019 θα ερμηνευτεί σε συγκεκριμένες περιπτώσεις από την Αρχή. Αναμένεται να μπορεί να χρησιμοποιηθεί ιδίως από δημοσιογράφους, τουλάχιστον έως ένα βαθμό. Άλλωστε η ίδια η διάταξη προϋποθέτει μια στάθμιση δικαιωμάτων και μόνο εάν η στάθμιση αποβαίνει υπέρ της ελευθερίας της έκφρασης και πληροφόρησης θα μπορεί να γίνει επίκλησή της. Είναι μια διάταξη που δεν φαίνεται να αφορά το δημόσιο τομέα.

## 14.2 Πρόσβαση σε δημόσια έγγραφα

### 14.2.1 «Συνδυάζοντας» ΓΚΠΔ και Κώδικα Διοικητικής Διαδικασίας

Σύμφωνα με το άρθρο 86 του ΓΚΠΔ, «*τα δεδομένα προσωπικού χαρακτήρα σε επίσημα έγγραφα που κατέχει δημόσια αρχή ή δημόσιος ή ιδιωτικός φορέας για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον μπορούν να κοινοποιούνται από την εν λόγω αρχή ή φορέα σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται η δημόσια αρχή ή ο φορέας, προκειμένου να συμβιβάζεται η πρόσβαση του κοινού σε επίσημα έγγραφα με το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού*». Ο ν. 4624/2019, με το άρθρο 42, ουσιαστικά αναφέρει ότι εξακολουθούν να ισχύουν και να εφαρμόζονται ως έχουν οι υπάρχουσες εθνικές διατάξεις – ήτοι οι διατάξεις του άρθρου 5 του Κώδικα Διοικητικής Διαδικασίας

δημοσιογραφικής, πανεπιστημιακής, καλλιτεχνικής ή και λογοτεχνικής έκφρασης, με το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα (…). Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνο για δημοσιογραφικούς σκοπούς ή για σκοπούς πανεπιστημιακής, καλλιτεχνικής ή λογοτεχνικής έκφρασης θα πρέπει να υπόκειται σε παρεκκλίσεις ή εξαιρέσεις από ορισμένες διατάξεις του παρόντος κανονισμού, εφόσον είναι αναγκαίο για να συμβιβασθεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης, όπως κατοχυρώνεται στο άρθρο 11 του Χάρτη (…) Επομένως, τα κράτη μέλη θα πρέπει να θεσπίσουν νομοθετικά μέτρα που να προβλέπουν τις αναγκαίες εξαιρέσεις και παρεκκλίσεις για την εξισορρόπηση των εν λόγω θεμελιωδών δικαιωμάτων. Τα κράτη μέλη θα πρέπει να θεσπίσουν τέτοιες εξαιρέσεις και παρεκκλίσεις σχετικά με τις γενικές αρχές, τα δικαιώματα του υποκειμένου των δεδομένων, του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς, τις ανεξάρτητες εποπτικές αρχές, τη συνεργασία και τη συνεκτικότητα και ειδικές περιπτώσεις επεξεργασίας δεδομένων (…) Για να ληφθεί υπόψη η σημασία του δικαιώματος της ελευθερίας της έκφρασης σε κάθε δημοκρατική κοινωνία, είναι απαραίτητο να ερμηνεύονται διασταλτικά οι έννοιες που σχετίζονται με την εν λόγω ελευθερία, όπως η δημοσιογραφία.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

(ΚΔΔιαδ) που αφορούν στη χορήγηση εγγράφων από φορείς του δημόσιου τομέα που εμπίπτουν στο πεδίο εφαρμογής του άρθρου 1 του ανωτέρω Κώδικα, καθώς και οι λοιπές διατάξεις που αφορούν στη χορήγηση εγγράφων από τον εκάστοτε φορέα ή αρχή ή υπηρεσία, εφόσον το περιεχόμενο των εγγράφων αυτών αποτελούν δεδομένα προσωπικού χαρακτήρα. Συνεπώς, με το ΓΚΠΔ δεν διαφοροποιήθηκε ουσιαστικά[65] αυτό που ήδη ίσχυε, αναφορικά με την πρόσβαση του κοινού σε δημόσια έγγραφα, και πριν τη θέση του ΓΚΠΔ σε εφαρμογή.

Τι ίσχυε λοιπόν πριν τον ΓΚΠΔ και εξακολουθεί να ισχύει και σήμερα;

Κατ' αρχάς, εφόσον το αίτημα πρόσβασης φυσικού προσώπου σε δημόσια έγγραφα αφορά σε έγγραφα που αναφέρονται στο πρόσωπό του, τότε το εν λόγω αίτημα υπέχει θέση άσκησης δικαιώματος πρόσβασης κατά την έννοια του άρθρου 15 του ΓΚΠΔ και, ως εκ τούτου, ισχύουν όλα όσα σχετικώς περιγράφηκαν νωρίτερα στην Ενότητα 6: το αίτημα συνεπώς μπορεί να αφορά και πρόσθετες πληροφορίες όπως την προέλευση των δεδομένων, τους αποδέκτες κ.α. (βλ. δικαίωμα πρόσβασης στην Ενότητα 6), ενώ θα πρέπει να ικανοποιείται αμελλητί και, σε κάθε περίπτωση, εντός τριάντα ημερών. Σημειώνεται και εδώ ότι δεν χρειάζεται ο αιτών να εξηγήσει, με το αίτημά του, τους λόγους για τους οποίους το υποβάλει.

Η πιο «δύσκολη» περίπτωση είναι αυτή για την οποία το αίτημα για πρόσβαση σε δημόσια έγγραφα που περιέχουν προσωπικά δεδομένα υποβάλλεται από τρίτο – και όχι από το υποκείμενο των δεδομένων. Κατ' αρχάς, το άρθρο 5 του ν. 2690/1999 (Κώδικας Διοικητικής Διαδικασίας) αναφέρει τα εξής:

*«1. Κάθε ενδιαφερόμενος έχει το δικαίωμα, ύστερα από γραπτή αίτησή του, να λαμβάνει γνώση των διοικητικών εγγράφων. Ως διοικητικά έγγραφα νοούνται όσα*

[65] Μη διαφοροποίηση, υπό την έννοια ότι εξακολουθεί να είναι σε ισχύ ο ΚΔΔιαδ. Βέβαια, πριν την έναρξη εφαρμογής του ΓΚΠΔ, για τη διαβίβαση δημοσίων εγγράφων με προσωπικά δεδομένα σε τρίτους απαιτούνταν άδεια της Αρχής, εφόσον το έγγραφο περιείχε ευαίσθητα δεδομένα. Η υποχρέωση λήψης άδειας από την Αρχή έχει πλέον καταργηθεί με το ΓΚΠΔ, αλλά αυτό μεταφράζεται, όπως θα εξηγηθεί στη συνέχεια, ότι ο κάθε υπεύθυνος επεξεργασίας οφείλει να ελέγχει, στο πλαίσιο της αρχής της λογοδοσίας, ότι συντρέχουν οι προϋποθέσεις για χορήγηση δημοσίου εγγράφου με προσωπικά δεδομένα (ευαίσθητα ή μη) σε τρίτο.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*συντάσσονται από τις δημόσιες υπηρεσίες, όπως εκθέσεις, μελέτες, πρακτικά, στατιστικά στοιχεία, εγκύκλιες οδηγίες, απαντήσεις της Διοίκησης, γνωμοδοτήσεις και αποφάσεις.*

*2. Όποιος έχει ειδικό έννομο συμφέρον δικαιούται, ύστερα από γραπτή αίτησή του, να λαμβάνει γνώση των ιδιωτικών εγγράφων που φυλάσσονται στις δημόσιες υπηρεσίες και είναι σχετικά με υπόθεσή του η οποία εκκρεμεί σε αυτές ή έχει διεκπεραιωθεί από αυτές.*

*3. Το κατά τις προηγούμενες παραγράφους δικαίωμα δεν υφίσταται στις περιπτώσεις που το έγγραφο αφορά την ιδιωτική ή οικογενειακή ζωή τρίτου, ή αν παραβλάπτεται απόρρητο το οποίο προβλέπεται από ειδικές διατάξεις. Η αρμόδια διοικητική αρχή μπορεί να αρνηθεί την ικανοποίηση του δικαιώματος τούτου αν το έγγραφο αναφέρεται στις συζητήσεις του Υπουργικού Συμβουλίου, ή αν η ικανοποίηση του δικαιώματος αυτού είναι δυνατόν να δυσχεράνει ουσιωδώς την έρευνα δικαστικών, διοικητικών, αστυνομικών ή στρατιωτικών αρχών σχετικώς με την τέλεση εγκλήματος ή διοικητικής παράβασης.*

*(…)*

*5. Η άσκηση του κατά της παρ. 1 και 2 δικαιώματος γίνεται με την επιφύλαξη της ύπαρξης τυχόν δικαιωμάτων πνευματικής ή βιομηχανικής ιδιοκτησίας.*

*6. Η χρονική προθεσμία για τη χορήγηση εγγράφων κατά τις παραγράφους 1 και 2 ή την αιτιολογημένη απόρριψη της σχετικής αίτησης του πολίτη είναι είκοσι (20) ημέρες.»*

Συνεπώς, από τα ανωτέρω, προκύπτει ότι, στη γενική περίπτωση, για την πρόσβαση σε διοικητικά έγγραφα μπορεί κάποιος τρίτος να έχει πρόσβαση επικαλούμενος εύλογο ενδιαφέρον, όμως για ιδιωτικά έγγραφα δεν αρκεί το εύλογο ενδιαφέρον αλλά θα πρέπει να έχει ειδικό έννομο συμφέρον (εφόσον τα έγγραφα αυτά δεν αναφέρονται στην ιδιωτική ή οικογενειακή ζωή τρίτου και δεν παραβλάπτεται απόρρητο προβλεπόμενο από ειδικές διατάξεις, κατά τα ανωτέρω). Ειδικότερα:

**<u>Πρόσβαση σε διοικητικά έγγραφα: Εύλογο ενδιαφέρον</u>**

Κατ’ αρχάς, η αναφορά των ειδών διοικητικών εγγράφων της παρ. 1 του άρθρου 5 είναι



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ενδεικτική[66]: ως διοικητικά έγγραφα πρέπει επίσης να θεωρούνται, λαμβάνοντας υπόψη τη νομολογία του Συμβουλίου της Επικρατείας (Σ.τ.Ε.) και του Νομικού Συμβουλίου του Κράτους (Ν.Σ.Κ.)[67], και όσα έγγραφα δεν προέρχονται μεν από δημόσιες υπηρεσίες αλλά χρησιμοποιήθηκαν ή ελήφθησαν υπόψη για τον καθορισμό της διοικητικής δράσης ή τη διαμόρφωση γνώμης ή κρίσης διοικητικού οργάνου. Επίσης, με τον όρο διοικητικά έγγραφα νοούνται όχι μόνο τα έγγραφα με τη στενή έννοια του όρου, αλλά και "*ό,τι υπάρχει μέσα στα αρχεία της διοίκησης*"[68].

Αναφορικά με την επίκληση του εύλογου ενδιαφέροντος, σύμφωνα με τη νομολογία, όπως αυτή εκφράζεται με αποφάσεις του Συμβουλίου της Επικρατείας και των διοικητικών δικαστηρίων, ο όρος «*εύλογο ενδιαφέρον*» αναφέρεται στη συνδρομή προσωπικής έννομης σχέσης που συνδέει τον αιτούντα με το περιεχόμενο των εγγράφων – δηλαδή *ως εύλογο ενδιαφέρον δεν μπορεί να νοηθεί το ενδιαφέρον κάθε πολίτη για την εύρυθμη άσκηση των γενικών καθηκόντων μίας υπηρεσίας και την τήρηση των νόμων, αλλά εκείνο το οποίο προκύπτει, κατά τρόπο αντικειμενικό, από την ύπαρξη μιας συγκεκριμένης, προσωπικής έννομης σχέσης συνδεομένης με το περιεχόμενο των διοικητικών στοιχείων στα οποία ζητείται η πρόσβαση* [71].

**<u>Πρόσβαση σε ιδιωτικά έγγραφα: Ειδικό έννομο συμφέρον</u>**

Ιδιωτικά έγγραφα είναι όλα τα έγγραφα τα οποία δεν είναι δημόσια (άρθρο 167 του ν. 2717/1999 – Κώδικας Διοικητικής Δικονομίας). Ενδεικτικά, ιδιωτικά έγγραφα είναι τα τιμολόγια, τα ιδιωτικά συμφωνητικά, τα τοπογραφικά σχεδιαγράμματα ιδιωτών μηχανικών, επιστολές ιδιωτών κ.α. (βλ. και [72]). Ως ιδιωτικά έγγραφα νοούνται όσα κατατίθενται στις υπηρεσίες του Δημοσίου αλλά δεν λαμβάνονται υπόψη για την έκδοση μίας διοικητικής πράξης.

Σύμφωνα με την αριθ. 620/1999 γνωμοδότηση του Ε΄ Τμήματος του Ν.Σ.Κ., η έννοια του ειδικού έννομου συμφέροντος είναι αυτή του άρθρου 902 του Αστικού Κώδικα, στο οποίο ορίζεται ότι: «*Οποιος έχει έννομο συμφέρον να πληροφορηθεί το*

[66] Βλ., π.χ, Γνωμ. 189/2015 του Β' Τμήματος Διακοπών του Νομικού Συμβουλίου του Κράτους (Ν.Σ.Κ.)
[67] Βλ., π.χ., Γνωμ. 620/1999 του Ε' Τμήματος του Ν.Σ.Κ
[68] Βλ. σχετικώς ΣτΕ 3855/2010.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*περιεχόμενο ενός εγγράφου που βρίσκεται στην κατοχή άλλου έχει δικαίωμα να απαιτήσει την επίδειξη ή και αντίγραφό του, αν το έγγραφο συντάχθηκε για το συμφέρον αυτού που το ζητεί ή πιστοποιεί έννομη σχέση που αφορά και αυτόν ή σχετίζεται με διαπραγματεύσεις που έγιναν σχετικά με τέτοια έννομη σχέση είτε απευθείας από τον ίδιο είτε για το συμφέρον του, με τη μεσολάβηση τρίτου*». Σημειώνεται ότι δεν αρκεί η αόριστη επίκληση ότι θα γίνει νόμιμη χρήση των αιτουμένων στοιχείων χωρίς αναφορά ειδικότερου λόγου που θα θεμελίωνε αντίστοιχα έννομο συμφέρον (βλ. ενδεικτικώς Ολ. Ν.Σ.Κ. 63/2008, 589/2005) [72].

**«Συνδυάζοντας» ΚΔΔιαδ με ΓΚΠΔ**

Η νομιμότητα επεξεργασίας προσωπικών δεδομένων που έγκειται στην ανακοίνωση δεδομένων κάποιου προσώπου σε τρίτους μέσω της πρόσβασης στα δημόσια έγγραφα, πρέπει να βασίζεται σε συνδυαστική εφαρμογή του ΓΚΠΔ και του άρθρου 5 ΚΔΔιαδ. Όπως έχει κρίνει και η Αρχή[69], μία τέτοια επεξεργασία επιτρέπεται και χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων, εάν είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπευθύνου επεξεργασίας η οποία επιβάλλεται από το νόμο (δηλαδή με τη νομική βάση του άρ. 6 παρ. 1 γ' του ΓΚΠΔ) και, στις συγκεκριμένες περιπτώσεις, τέτοια υποχρέωση του υπευθύνου επεξεργασίας είναι και το προαναφερόμενο, όπως προβλέπεται στο άρθρο 5 ΚΔΔιαδ, δικαίωμα πρόσβασης στα δημόσια έγγραφα («διοικητικά» κατά το άρθρο 5 παρ. 1 και «ιδιωτικά» που φυλάσσονται από δημόσιες αρχές κατά το άρθρο 5 παρ. 2), όταν τα έγγραφα αυτά δεν αναφέρονται στην ιδιωτική ή οικογενειακή ζωή τρίτου και δεν παραβλάπτεται απόρρητο προβλεπόμενο από ειδικές διατάξεις (άρθρο 5 παρ. 3 ΚΔΔιαδ). Μάλιστα, ως προς την έννοια της «ιδιωτικής ή οικογενειακής ζωής», η Αρχή δέχεται ότι δεν είναι ικανά εκ της φύσεώς τους όλα τα προσωπικά δεδομένα να θίξουν την ιδιωτική ζωή κάποιου προσώπου, ενώ ως δυνάμενα να επιφέρουν τέτοιο αποτέλεσμα θα πρέπει να αντιμετωπίζονται κυρίως οι ειδικές κατηγορίες δεδομένων, όπως εκείνα που σχετίζονται με τη φυλετική ή εθνική προέλευση, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τα σχετικά με την υγεία και τη σεξουαλική ζωή ενός προσώπου δεδομένα.

[69] Βλ. σχετικώς το σύνδεσμο **https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/dimosiostomeas/dimosiadioikhsh/xorigisi_dimosiwn_eggrafwn_se_tritous**

Συνεπώς, στην περίπτωση που στα δημόσια έγγραφα περιέχονται προσωπικά δεδομένα τρίτων προσώπων, τα οποία σχετίζονται με την ιδιωτική ή οικογενειακή τους ζωή (είτε πρόκειται για «απλά» δεδομένα είτε για ειδικές κατηγορίες δεδομένων), εφαρμόζονται ως επί το πλείστον οι διατάξεις των άρθρων 6 παρ. 1 παρ. γ΄ ή στ΄ του ΓΚΠΔ («απλά» δεδομένα) και 9 παρ. 2 στ΄ του ΓΚΠΔ (ειδικές κατηγορίες δεδομένων), λαμβανομένων υπόψη και των σχετικών διατάξεων του ν. 4624/2019. Με άλλα λόγια, εφόσον συντρέχουν οι κατά περίπτωση προϋποθέσεις (την εκπλήρωση των οποίων ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να την αποδείξει, σύμφωνα με την αρχή της λογοδοσίας), μία τέτοια διαβίβαση είναι επιτρεπτή και χωρίς συγκατάθεση του προσώπου το οποίο αφορά το δημόσιο έγγραφο.

**Πώς οφείλει να ενεργεί ο υπεύθυνος επεξεργασίας**

Εφόσον τρίτος υποβάλει αίτημα προς Δημόσιο φορέα για να αποκτήσει πρόσβαση σε δημόσια έγγραφα που περιέχουν προσωπικά δεδομένα, τότε είναι ευθύνη του φορέα, ως υπεύθυνος επεξεργασίας, να κρίνει αν συντρέχουν οι νόμιμες προϋποθέσεις για να επιτρέψει πρόσβαση / χορηγήσει αντίγραφο του εγγράφου – ήτοι: α) αν πρόκειται για περίπτωση διοικητικού εγγράφου που αρκεί η επίκληση εύλογου ενδιαφέροντος, να ελέγξει ότι πράγματι τεκμαίρεται εύλογο ενδιαφέρον, ενώ β) αν πρόκειται για περίπτωση ιδιωτικού εγγράφου που απαιτεί την ύπαρξη ειδικού έννομου συμφέροντος του αιτούντος, να επιβεβαιώσει ότι ο αιτών τεκμηριώνει το ειδικό έννομο συμφέρον που έχει, το οποίο θα πρέπει να υπερτερεί προφανώς των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων στα οποία αναφέρονται τα δεδομένα. Η εν λόγω υποχρέωση των φορέων είχε ήδη προδιαγραφεί από την Αρχή με τη Γνωμοδότηση 6/2013 [71], προ του ΓΚΠΔ, στη βάση της νομολογίας του Ν.Σ.Κ. και του Σ.τ.Ε., αλλά είναι πλέον και άμεση απόρροια της αρχής της λογοδοσίας που εισάγει ο ΓΚΠΔ. Συνεπώς, ο φορέας δεν μπορεί να ζητά και να αναμένει τη γνώμη της Αρχής ως προς το πώς θα διαχειρίζεται τέτοια αιτήματα.

**Παράδειγμα**: Πολίτης Α υποβάλει αίτημα σε δημόσιο φορέα Χ προκειμένου να



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αποκτήσει πρόσβαση σε ιδιωτικό έγγραφο που έχει υποβάλει ο πολίτης Β προς το φορέα Χ, για υπόθεσή του. Ο Α στο αίτημά του σημειώνει «*αιτούμαι το εν λόγω έγγραφο διότι έχω ειδικό έννομο συμφέρον να λάβω γνώση αυτού*».

Ο φορέας Χ δεν επιτρέπεται να χορηγήσει το έγγραφο, αφού ο Α δεν τεκμηρίωσε το ειδικό έννομο συμφέρον που έχει.

Εάν ο Α επανέλθει με νεότερο αίτημα, στο οποίο θα τεκμηριώνει τους λόγους για τους οποίους έχει ειδικό έννομο συμφέρον, τότε ο φορέας Χ θα πρέπει να σταθμίσει και να αξιολογήσει αν πράγματι το έννομο συμφέρον του Α υπερτερεί των δικαιωμάτων και ελευθεριών του Β (εφόσον βέβαια δεν προσκρούει σε άλλο απόρρητο ή δεν είναι η περίπτωση που το έγγραφο αφορά την ιδιωτική ή οικογενειακή ζωή του Β, οπότε η απάντηση ως προς το αίτημα θα είναι αρνητική). Εάν ο φορέας Χ κρίνει ότι πράγματι υπερτερεί, τότε μπορεί να χορηγήσει το έγγραφο (υπό την πρόσθετη προϋπόθεση ενημέρωσης που περιγράφεται αμέσως μετά) – διαφορετικά, δεν το διαβιβάζει και εξηγεί τους λόγους. Σε περίπτωση που το εν λόγω έγγραφο περιέχει πλήθος προσωπικών δεδομένων του Β αλλά μόνο για κάποια εξ αυτών τεκμηριώνεται υπέρτερο έννομο συμφέρον του Α να τα λάβει, τότε τα δεδομένα που δεν εμπίπτουν σε αυτά για τα οποία επιτρέπεται η χορήγηση (π.χ. μία συνηθισμένη τέτοια περίπτωση είναι η διεύθυνση ή ο τηλεφωνικός αριθμός επικοινωνίας του Β), απαλείφονται πριν τη διαβίβαση.

Επισημαίνεται ότι, ακόμα και στην περίπτωση που συντρέχουν οι προϋποθέσεις και είναι επιτρεπτή η χορήγηση εγγράφου με προσωπικά δεδομένα σε τρίτο και χωρίς τη συγκατάθεση του προσώπου του οποίου τα δεδομένα εμπεριέχονται στο έγγραφο, δεν αίρεται η υποχρέωση ενημέρωσης του εν λόγω προσώπου (υποκειμένου των δεδομένων) κατά τα άρθρα 13 και 14 του ΓΚΠΔ[70]. Η υποχρέωση ενημέρωσης εξάλλου αποτελεί έκφανση της θεμελιώδους αρχής της διαφάνειας για κάθε επεξεργασία (άρθρο 5 παρ. 1 του ΓΚΠΔ), η οποία θα πρέπει να πληρούται και για κάθε τέτοια επεξεργασία.

☞ Εφόσον φορέας κρίνει ότι είναι επιτρεπτή η χορήγηση δημοσίου εγγράφου (είτε

[70] Εκτός βέβαια αν συντρέχουν οι εξαιρέσεις ως προς την ενημέρωση του άρθρου 13 παρ. 4 και του άρθρου 14 παρ. 5 του ΓΚΠΔ, όπως και του άρθρου 33 παρ. 4 του ν. 4624/2019.

διοικητικού είτε ιδιωτικού, κατά τα ανωτέρω), το οποίο περιέχει προσωπικά δεδομένα, σε τρίτο πρόσωπο, τότε πριν τη χορήγηση οφείλει να ενημερώσει σχετικώς το πρόσωπο του οποίου τα δεδομένα πρόκειται να διαβιβαστούν στο τρίτο πρόσωπο.

**Παράδειγμα**: Σε συνέχεια του προηγούμενου παραδείγματος, ο φορέας Χ πρέπει να ενημερώσει τον Β ότι ο Α υπέβαλε στον Χ αίτημα λήψης συγκεκριμένου εγγράφου (θα πρέπει η ενημέρωση να προσδιορίζει σαφώς περί ποιου εγγράφου πρόκειται), ότι τεκμηρίωσε ειδικό έννομο συμφέρον και ότι ο Χ αξιολόγησε ότι πράγματι το εν λόγω συμφέρον υπερτερεί της προσβολής δικαιωμάτων του Β που ενδεχομένως επιφέρει η επικείμενη διαβίβαση του εγγράφου στον Α και, άρα, είναι επιτρεπτή η εν λόγω χορήγηση σύμφωνα με το άρθρο 5 του ΚΔΔιαδ, συνδυαστικά με τις διατάξεις του ΓΚΠΔ. Η εν λόγω ενημέρωση του Β πρέπει να γίνει πριν τη χορήγηση του εγγράφου στον Α.

Σημειώνεται ότι ακόμα και αν ο Β εκφράσει, μόλις ενημερωθεί, την αντίρρησή του για την εν λόγω χορήγηση, η έκφραση αντίρρησης αυτή είναι πρακτικά αλυσιτελής εφόσον είναι σαφές και αδιαμφισβήτητο το υπέρτερο έννομο συμφέρον του Α: και τούτο διότι δεν απαιτείται συγκατάθεση του Β για την εν λόγω επεξεργασία.

Η ως άνω ενημέρωση από τον Χ προς τον πολίτη Β θα πρέπει να γίνει με τρόπο τέτοιο που να επιτρέπει στον Χ, αν χρειαστεί, να αποδείξει ότι πράγματι την έκανε.

☞ Εφόσον συντρέχουν οι ως άνω αναφερόμενες προϋποθέσεις, δεν απαιτείται εισαγγελική παραγγελία για τη χορήγηση δημοσίου εγγράφου με προσωπικά δεδομένα σε τρίτο. Μάλιστα, όπως εξηγείται στη συνέχεια στην Ενότητα 14.2.1.2, μία εισαγγελική παραγγελία δεν πρέπει πάντοτε να «μεταφράζεται» ως εντολή χορήγησης των αρχείων χωρίς έλεγχο της συνδρομής των προϋποθέσεων νόμιμης επεξεργασίας.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Συναφής νομολογία της Αρχής**

Δεδομένου ότι, όπως προαναφέρθηκε, αφενός δεν επήλθαν μεγάλες αλλαγές από το ΓΚΠΔ αναφορικά με την πρόσβαση σε δημόσια έγγραφα, και αφετέρου το εν λόγω ζήτημα ουσιαστικά σχετίζεται με τη «σύγκρουση» δύο συνταγματικά κατοχυρωμένων δικαιωμάτων, ήτοι του δικαιώματος της πληροφοριακής αυτοδιάθεσης του ατόμου (άρθρο $9^{A}$ Σ.) και της αρχής της διαφάνειας (με τις ειδικότερες εκφάνσεις του δικαιώματος στην πληροφόρηση, άρθρο $5^{A}$ Σ. και του δικαιώματος πρόσβασης στα διοικητικά έγγραφα, άρθρο 10 παρ. 3 Σ.) για τα οποία δεν υπάρχει ιεραρχική σειρά [71], παρατίθενται στη συνέχεια κάποια ενδεικτικά παραδείγματα από την υπάρχουσα νομολογία της Αρχής. Τα εν λόγω παραδείγματα, αν και πολλά εξ αυτών αναφέρονται σε προ του ΓΚΠΔ χρονικές περιόδους[71], παραμένουν επίκαιρα για τους λόγους που εξηγήθηκαν ανωτέρω και μπορούν να αποτελέσουν «οδηγό» για υπευθύνους επεξεργασίας οι οποίοι πλέον καλούνται να κάνουν οι ίδιοι, και να είναι σε θέση να τεκμηριώσουν σχετικά, την ως άνω στάθμιση για κάθε τέτοιο αίτημα που λαμβάνουν.

1. Επιτρέπεται η πρόσβαση τρίτου στα δικαιολογητικά έγγραφα που κατέθεσε το υποκείμενο των δεδομένων σε Περιφέρεια, βάσει των οποίων εκδόθηκε παραχωρητήριο συμβόλαιο, με το σκεπτικό ότι τα έγγραφα αυτά, μολονότι δεν έχουν συνταχθεί από δημόσια υπηρεσία, εμπίπτουν στην έννοια των διοικητικών εγγράφων, λόγω του ότι ελήφθησαν υπόψη προκειμένου να εκδοθεί το παραχωρητήριο, και επιπλέον δεν σχετίζονται με την ιδιωτική ή οικογενειακή ζωή κάποιου προσώπου (εκτός από τα πιστοποιητικά οικογενειακής κατάστασης) [73].
2. Επιτρέπεται η πρόσβαση στους κτηματολογικούς πίνακες, εφόσον αυτοί συντάσσονται από τους δήμους και ως εκ τούτου αποτελούν δημόσια έγγραφα. Εξάλλου, τα προσωπικά δεδομένα, που περιλαμβάνονται σε αυτούς δεν σχετίζονται με την ιδιωτική ή οικογενειακή ζωή κάποιου προσώπου) [73].
3. Επιτρέπεται η χορήγηση από τη Διοίκηση σε τρίτο αντιγράφων της άδειας ίδρυσης και λειτουργίας καταστήματος, καθώς και της έκθεσης αυτοψίας αυθαίρετης κατασκευής, καθώς πρόκειται για διοικητικά έγγραφα που δεν

[71] Υπάρχει νομολογία της Αρχής ως προς το εν λόγω ζήτημα, ιδίως πριν την Γνωμοδότηση 6/2013

σχετίζονται με την ιδιωτική ή οικογενειακή ζωή κάποιου προσώπου [73].

4. Επιτρέπεται η χορήγηση από το Σώμα Επιθεωρητών Ελεγκτών Δημόσιας Διοίκησης αντιγράφου της έκθεσης επιθεώρησης ελέγχου σε τρίτο, βάσει καταγγελίας του οποίου κινήθηκε ο συγκεκριμένος έλεγχος, καθώς δεν προβλέπεται κάποιου είδους απόρρητο για την έκθεση που συντάσσει το συγκεκριμένο Σώμα [73].
5. Επιτρέπεται σε Δήμο να χορηγήσει σε δημότη αρχεία προσωπικών δεδομένων που τηρεί, για τα οποία ο δημότης τεκμηρίωσε ότι τα χρειάζεται για το σκοπό της αναγνώρισης, άσκησης ή υπεράσπισης των νομίμων δικαιωμάτων του ενώπιον των αρμόδιων δικαστηρίων ή διοικητικών αρχών [74].
6. Επιτρέπεται η χορήγηση, από τον ΟΑΕΔ, αιτήσεων και δικαιολογητικών επιλεγέντος σε διαγωνισμό για πλήρωση θέσεων ΑΜΕΑ σε έτερο, μη επιλεγέντα, υποψήφιο, προκειμένου να ασκήσει τα εκ του νόμου δικαιώματά του υποβολής ενστάσεως κατά του πίνακα κατάταξης. Εφόσον και δεδομένα ειδικών κατηγοριών (δεδομένα υγείας) ελήφθησαν υπόψη με τα υπόλοιπα δικαιολογητικά και αποτέλεσαν με αυτά τη βάση αξιολόγησης για την κατάληψη των θέσεων που προκηρύχθηκαν, η χορήγηση κρίνεται αναγκαία προκειμένου ο αιτών να υποβάλει αίτηση ακυρώσεως κατά των τελικών πινάκων επιτυχόντων/επιλαχόντων ενώπιον του αρμόδιου Διοικητικού Δικαστηρίου [75].
7. Επιτρέπεται σε δημόσια υπηρεσία η χορήγηση δεδομένων υπαλλήλου της σε τρίτο για δικαστική χρήση (περίπτωση αγωγής διατροφής ανήλικου τέκνου), εφόσον α) τα αιτούμενα στοιχεία είναι συναφή με την εκκρεμή αστική δίκη (αγωγή διατροφής) και αναγκαία στον τρίτο για την αντίκρουση της αγωγής ως εναγομένου, και β) η εν λόγω χορήγηση προβλέπεται σε ρητή διάταξη νόμου (για την εν λόγω περίπτωση συντρέχουν τα άρθρα 1445 του ΑΚ και 17 παρ. 1 περ. ζ' του ν. 4174/2013). Αυτονόητη βέβαια είναι η προηγούμενη ενημέρωση του υπαλλήλου (βλ. [76], όπου στην εν λόγω περίπτωση δεν είχε προηγηθεί ενημέρωση).
8. Αιτών μπορεί να λάβει, για διαγωνισμό Υπουργείου αναφορικά με επιλογή Προϊσταμένου στον οποίο συμμετείχε, πλήρη πληροφόρηση ως προς την αναλυτική του μοριοδότηση, στο πλαίσιο άσκησης δικαιώματος πρόσβασης.

Ωστόσο, αναφορικά με τη διαδικασία υποβολής ενστάσεων, το δικαίωμα διόρθωσης των δεδομένων δεν ταυτίζεται με το δικαίωμα υποβολής ένστασης ή αίτησης θεραπείας που τυχόν επιφυλάσσει ο νόμος για την επαναξιολόγηση της μοριοδότησης της και, κατά τούτο, η τυχόν αμφισβήτηση της ληφθείσας μοριοδότησης δεν μπορεί να ζητηθεί με την άσκηση του δικαιώματος διόρθωσης (βλ. [77]).

#### 14.2.1.1 Η περίπτωση πρόσβασης σε φάκελο συνυποψηφίου ΑΣΕΠ

Για το ειδικότερο ζήτημα της πρόσβασης υποψηφίου διαγωνισμού του ΑΣΕΠ σε φάκελο συνυποψηφίου του, σύμφωνα και με τα όσα έχει προδιαγράψει σχετικώς η Αρχή[72], η ανακοίνωση των στοιχείων των επιλεγέντων συνυποψηφίων σε άλλον υποψήφιο είναι νόμιμη, και χωρίς τη συγκατάθεσή τους, υπό τις εξής σωρευτικά εξεταζόμενες προϋποθέσεις:

1. Τα δεδομένα ζητούνται με τη νόμιμη διαδικασία (έγγραφη αίτηση, τεκμηρίωση υπέρτερου έννομου συμφέροντος). Το έννομο συμφέρον του αιτούντος προκύπτει από το δικαίωμα του αιτούντος να ασκήσει τα εκ του νόμου δικαιώματά του προσβολής των σχετικών αποφάσεων και πινάκων (π.χ. υποβολή ένστασης, άσκηση αιτήσεως ακυρώσεως, κ.λπ.).
2. Η ανακοίνωση στοιχείων των συνυποψηφίων περιορίζεται στη χορήγηση μόνο εκείνων των στοιχείων που αποτέλεσαν τη βάση της αξιολόγησης των υποψηφίων για την κατάληψη των προς πλήρωση θέσεων. Συνεπώς, δεν χορηγούνται στοιχεία τα οποία δεν προσμετρήθηκαν στην αξιολόγηση (π.χ. διεύθυνση κατοικίας, ηλεκτρονική διεύθυνση, τηλεφωνικός αριθμός κτλ.). Στην περίπτωση που οι υποψήφιοι επικαλέστηκαν και πρόσθετα προσόντα, μπορούν να χορηγηθούν και αυτά τα δικαιολογητικά στον συνυποψήφιο που απορρίφθηκε, μόνο εφόσον τα πρόσθετα αυτά προσόντα τελικά προσμετρήθηκαν και έγινε σύγκριση των υποψηφίων και επί των πρόσθετων αυτών προσόντων.
3. Τα στοιχεία που ανακοινώνονται δεν περιλαμβάνουν ειδικές κατηγορίες,

[72] Βλ. το διαδικτυακό τόπο
**https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/dimosiostomeas/dimosia dioikhsh/prosvasi_se_stoixeia_sunupopsifiwn**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εκτός εάν αυτά ελήφθησαν υπόψη κατά την επιλογή. Αν, δηλαδή, και τέτοια στοιχεία αποτέλεσαν τη βάση αξιολόγησης των υποψηφίων και υπήρξε σύγκριση των υποψηφίων και επί των στοιχείων αυτών, ο υπεύθυνος επεξεργασίας δύναται να επιτρέψει την πρόσβαση στα στοιχεία αυτά σε κάθε υποψήφιο που δεν επιλέχθηκε, προκειμένου να ασκήσει το δικαίωμά του προσβολής της επιλογής άλλου συνυποψηφίου ενώπιον δικαστηρίου (βλ. την υπ' αριθμ. 40/2005 Απόφαση της Αρχής [78]).

4. Πριν από την ανακοίνωση των στοιχείων συνυποψηφίων στον αιτούντα, πρέπει να ενημερώσει ο υπεύθυνος επεξεργασίας τα υποκείμενα των δεδομένων με κάθε πρόσφορο τρόπο.

#### 14.2.1.2 Η περίπτωση εισαγγελικής παραγγελίας

Αναφορικά με τις περιπτώσεις για τις οποίες το αίτημα τρίτου προς Δημόσια Υπηρεσία για απόκτηση πρόσβαση σε δημόσια έγγραφα με προσωπικά δεδομένα συνοδεύεται από εισαγγελική παραγγελία, η Αρχή έχει εκδώσει τη Γνωμοδότηση 3/2009 [79]. Σύμφωνα με αυτή:

1. Η εισαγγελική παραγγελία είναι δεσμευτική για τη Διοίκηση, μόνον όταν ο εισαγγελέας ζητά τα στοιχεία στο πλαίσιο άσκησης ποινικής δίωξης (προκαταρκτική εξέταση, προανάκριση, κύρια ανάκριση). Σε αυτή την περίπτωση, η νομιμότητα της χορήγησης κρίνεται με βάση τις διατάξεις του Κώδικα Ποινικής Δικονομίας.
2. Η τυποποιημένη εισαγγελική παραγγελία με την ένδειξη «δια τα καθ' υμάς περαιτέρω» ή «για τις περαιτέρω ενέργειες» δεσμεύει τη Διοίκηση ως προς το ότι αποτελεί επιτακτική εντολή προς διερεύνηση του αιτήματος. Αυτό δεν σημαίνει ότι η Διοίκηση υποχρεούται να χορηγήσει το δημόσιο έγγραφο χωρίς να εξετάσει τη συνδρομή των προϋποθέσεων νόμιμης χορήγησής του, υποχρεούται όμως να δώσει σαφή και τεκμηριωμένη απάντηση στον αιτούντα (είτε αυτή είναι θετική είτε αρνητική), αφού διερευνήσει το αίτημα με βάση κυρίως το άρθρο 5 του ν. 2690/1999 (ΚΔΔιαδ) και τα άρθρα 6 παρ. 1 στοιχ. γ΄ ή στ΄ ΓΚΠΔ («απλά» δεδομένα) και 9 παρ. 2 στοιχ. στ΄ ΓΚΠΔ (ειδικές κατηγορίες δεδομένων) λαμβανομένων υπόψη και των διατάξεων των άρθρων

26 και 30 του ν. 4624/2019.

Και σε αυτή την περίπτωση βέβαια, εφόσον η Διοίκηση κρίνει ότι επιτρέπεται να χορηγήσει το αιτούμενο έγγραφο, πρέπει προηγουμένως να ενημερώσει τα υποκείμενα των δεδομένων (δηλαδή τα πρόσωπα, τα στοιχεία των οποίων αναφέρονται στο έγγραφο) κατά τα προβλεπόμενα στα άρθρα 13 και 14 του ΓΚΠΔ**,** όπως αναφέρθηκε και ανωτέρω.

**Ερώτηση δραστηριότητας**: Ο πολίτης Α υποβάλει αίτημα σε δημόσιο φορέα Χ για να λάβει δημόσιο έγγραφο με προσωπικά δεδομένα του Β. Δεν επικαλείται τους λόγους για τους οποίους θέλει το έγγραφο, αλλά φέρει εισαγγελική παραγγελία η οποία αναφέρει: «*Σας διαβιβάζουμε τη συνημμένη αίτηση του Α και παρακαλούμε για την κατά το νόμο εκτίμηση των διαλαμβανομένων σε αυτή και τις εντεύθεν επιβαλλόμενες ενέργειές σας*». Πώς θα πρέπει να ανταποκριθεί ο φορέας Χ;

### 14.2.2 Διαβίβαση προσωπικών δεδομένων στον καθ΄ ου η καταγγελία

Ένα ειδικό ζήτημα της πρόσβασης σε δημόσια έγγραφα είναι αυτό όπου πολίτης, για τον οποίο έχει υποβληθεί καταγγελία σε Δημόσια Υπηρεσία από άλλο πολίτη, ζητάει να του χορηγηθεί η πλήρης καταγγελία, συμπεριλαμβανομένων των στοιχείων του καταγγέλλοντα (ονοματεπώνυμο, διεύθυνση κ.α.). Ως προς το ζήτημα αυτό, έχει ήδη αποφανθεί σχετικώς η Αρχή με την Απόφαση 73/2010[73] [80], σύμφωνα με την οποία ο καταγγελλόμενος, ως υποκείμενο των δεδομένων που τον αφορούν, έχει δικαίωμα πρόσβασης όχι μόνο στο κείμενο της καταγγελίας αλλά και σε κάθε πληροφορία σχετική με την προέλευση (πηγή) των δεδομένων αυτών – στην οποία έννοια της προέλευσης συμπεριλαμβάνονται στοιχεία όπως το όνομα και η διεύθυνση του καταγγέλλοντα.

Στο ανωτέρω δικαίωμα υπάρχουν περιορισμοί, όπως αυτοί προσδιορίζονται στην εν

[73] Καίτοι η εν λόγω Απόφαση εκδόθηκε προ του ΓΚΠΔ, εν τούτοις πρακτικά δεν διαφοροποιείται κάτι μετά τη θέση του ΓΚΠΔ σε εφαρμογή.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

λόγω Απόφαση: κατ' αρχάς, ισχύουν οι περιορισμοί του άρθρο 5 παρ. 3 του ΚΔΔιαδ αναφορικά με περιπτώσεις που το έγγραφο αφορά ιδιωτική ή οικογενειακή ζωή τρίτου ή παραβλέπεται απόρρητο, προβλεπόμενο από ειδικές διατάξεις, καθώς επίσης και όταν η συγκεκριμένη πρόσβαση είναι δυνατόν να δυσχεράνει ουσιωδώς την έρευνα της υπόθεσης σχετικά με την τέλεση εγκλήματος ή διοικητικής παράβασης. Επιπλέον περιορισμοί που παρατίθενται στην εν λόγω Απόφαση αναφέρονται στην ύπαρξη ειδικών διατάξεων που επιβάλλουν ή επιτρέπουν ενδεχομένως απόλυτη ή μερική τήρηση μυστικότητας καθώς και στην περίπτωση που η γνωστοποίηση των στοιχείων του καταγγέλλοντος δύναται να απειλήσει/απειλεί το υπέρτατο έννομο αγαθό της ζωής του.

Όπως έχει επισημάνει η Αρχή με την ως άνω Απόφαση, ο καταγγέλλων οφείλει να γνωρίζει ότι ο καταγγελλόμενος έχει, πλην εξαιρέσεων, δικαίωμα πρόσβασης στην καταγγελία που τον αφορά και στα στοιχεία του καταγγέλλοντος και, άρα, σκόπιμο είναι να ενημερώνεται προς τούτο ο καταγγέλλων κατά το χρόνο υποβολής της καταγγελίας. Εφόσον ο καταγγέλλων δεν επιθυμεί να αποκαλυφθεί η ταυτότητά του, θα πρέπει εξαρχής να τεκμηριώσει εγγράφως τους λόγους, ώστε να εξετάζονται από τη Δημόσια Υπηρεσία.

## 14.3 Επιστημονική έρευνα, στατιστικοί σκοποί, αρχειοθέτηση προς το δημόσιο συμφέρον

Οι σκοποί της επιστημονικής έρευνας, οι στατιστικοί σκοποί, αλλά και οι σκοποί αρχειοθέτησης προς το δημόσιο συμφέρον ενδέχεται, εκ της φύσης τους, να προσκρούουν σε θεμελιώδη δικαιώματα αν δεν ληφθούν κατάλληλες εγγυήσεις για την αντίστοιχη επεξεργασία που θα πραγματοποιηθεί. Ιδίως ως προς την προστασία των προσωπικών δεδομένων, ο ΓΚΠΔ δεν επιδιώκει να θέσει «εμπόδια» στις επεξεργασίες εν όψει των ανωτέρω σκοπών – δίνει όμως έμφαση στην ανάγκη ύπαρξης κατάλληλων εγγυήσεων. Πράγματι, στο άρθρο 89 παρ. 1 του ΓΚΠΔ αναφέρονται τα εξής (η υπογράμμιση που ακολουθεί είναι του γράφοντος):

*«Η επεξεργασία για σκοπούς αρχειοθέτησης για το δημόσιο συμφέρον ή για σκοπούς*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς υπόκειται σε κατάλληλες εγγυήσεις, σύμφωνα με τον παρόντα κανονισμό, ως προς τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, σύμφωνα με τον παρόντα κανονισμό. Οι εν λόγω εγγυήσεις διασφαλίζουν ότι έχουν θεσπιστεί τα τεχνικά και οργανωτικά μέτρα, ιδίως για να διασφαλίζουν την τήρηση της αρχής της ελαχιστοποίησης των δεδομένων. Τα εν λόγω μέτρα μπορούν να περιλαμβάνουν τη χρήση ψευδωνύμων, εφόσον οι εν λόγω σκοποί μπορούν να εκπληρωθούν κατ' αυτόν τον τρόπο. Εφόσον οι εν λόγω σκοποί μπορούν να εκπληρωθούν από περαιτέρω επεξεργασία η οποία δεν επιτρέπει ή δεν επιτρέπει πλέον την ταυτοποίηση των υποκειμένων των δεδομένων, οι εν λόγω σκοποί εκπληρώνονται κατ' αυτόν τον τρόπο».*

Συνεπώς, δίνεται ιδιαίτερη βαρύτητα στην ύπαρξη εγγυήσεων, κάποιες εκ των οποίων εξειδικεύονται στην εν λόγω διάταξη. Συγκεκριμένα:

1) Έμφαση δίνεται στην αρχή της ελαχιστοποίησης των δεδομένων, το οποίο συνεπάγεται ότι τα προσωπικά δεδομένα τα οποία θα υποστούν επεξεργασίας εν όψει των ανωτέρω σκοπών πρέπει να είναι τα απολύτως απαραίτητα και όχι περισσότερα από ό,τι απαιτείται για την επίτευξή τους.
2) Ειδική αναφορά γίνεται στη χρήση ψευδωνύμων, εφόσον με αυτά επιτυγχάνονται οι επιδιωκόμενοι σκοποί.
3) Εάν οι εν λόγω σκοποί μπορούν να επιτευχθούν από δεδομένα τα οποία, μετά από κατάλληλη επεξεργασία, δεν επιτρέπουν την αναγνώριση των προσώπων, τότε αυτή είναι η προσέγγιση που πρέπει να ακολουθείται.

Οι εγγυήσεις 2 και 3 ανωτέρω ενδεχομένως να γεννούν προβληματισμό ως προς το ποια είναι η ειδοποιός διαφορά τους. Ουσιαστικά, η υπό στοιχείο 3 εγγύηση υπονοεί τη λεγόμενη *ανωνυμοποίηση* των δεδομένων, η οποία είναι διαφορετική από την ψευδωνυμοποίηση που περιγράφεται στην υπό στοιχείο 2 εγγύηση: περισσότερη συζήτηση επ' αυτού θα γίνει στην Ενότητα 15.

☞ Η εν λόγω διάταξη, με την απαίτηση για τις κατάλληλες εγγυήσεις, μπορεί να αφορά δημόσιους τομείς σε δύο διαφορετικές περιπτώσεις: είτε αν οι ίδιοι πραγματοποιούν επεξεργασίες για τους σκοπούς που αφορά η εν λόγω διάταξη



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

είτε αν οι φορείς αυτοί δίνουν πρόσβαση, για δεδομένα που τηρούν, σε τρίτους οι οποίοι νομίμως πραγματοποιούν επεξεργασίες για τους εν λόγω σκοπούς (π.χ. εξωτερικοί ερευνητές, Πανεπιστήμια, ερευνητικά κέντρα κτλ.)

☞ Σε κάθε περίπτωση, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για επιστημονικούς σκοπούς θα πρέπει να είναι σύμφωνη και με τυχόν ειδικότερες νομοθεσίες - για παράδειγμα, όπως αυτή για τις κλινικές δοκιμές (Κανονισμός (ΕΕ) αριθ. 536/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου). Βλ. σχετικώς και αιτιολογική Σκέψη 156 του ΓΚΠΔ.

Η σημασία που αποδίδει ο ΓΚΠΔ στην έρευνα – υπό τις κατάλληλες βέβαια εγγυήσεις – αποτυπώνεται και στην αιτιολογική σκέψη 157 αυτού, στην οποία αναφέρονται τα εξής: «*Συνδυάζοντας πληροφορίες από μητρώα, οι ερευνητές μπορούν να αποκτούν νέες γνώσεις μεγάλης σημασίας όσον αφορά διαδεδομένες παθολογικές καταστάσεις όπως καρδιαγγειακά νοσήματα, καρκίνος και κατάθλιψη. Βάσει των μητρώων, τα αποτελέσματα των ερευνών μπορούν να ενισχύονται, δεδομένου ότι στηρίζονται σε ευρύτερη πληθυσμιακή βάση. Στις κοινωνικές επιστήμες, η έρευνα βάσει μητρώων δίνει στους ερευνητές τη δυνατότητα να αποκτούν ουσιαστικές γνώσεις για τον μακροπρόθεσμο συσχετισμό ορισμένων κοινωνικών καταστάσεων, όπως η ανεργία και η εκπαίδευση με άλλες συνθήκες διαβίωσης. Τα αποτελέσματα των ερευνών που αποκτώνται μέσω μητρώων παρέχουν αξιόπιστες και ποιοτικές γνώσεις οι οποίες μπορούν να αποτελέσουν τη βάση για την εκπόνηση και εφαρμογή πολιτικής βασισμένης στη γνώση, να βελτιώσουν την ποιότητα ζωής ορισμένων ανθρώπων και να βελτιώσουν την αποτελεσματικότητα των κοινωνικών υπηρεσιών. Με στόχο τη διευκόλυνση της επιστημονικής έρευνας, τα δεδομένα προσωπικού χαρακτήρα μπορούν να υφίστανται επεξεργασία για σκοπούς επιστημονικής έρευνας, υπό τις κατάλληλες προϋποθέσεις και εγγυήσεις που θεσπίζονται στο ενωσιακό δίκαιο ή στο δίκαιο κράτους μέλους*».

Περαιτέρω, άξια αναφοράς είναι και η αιτιολογική Σκέψη 159, αναφορικά με τον ευρύ χαρακτήρα της έννοιας «επιστημονική έρευνα». Συγκεκριμένα, σύμφωνα με τη Σκέψη αυτή, «*όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς επιστημονικής έρευνας, ο παρών κανονισμός θα πρέπει να ισχύει και για την*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*επεξεργασία αυτή. Για τους σκοπούς του παρόντος κανονισμού, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας θα πρέπει να ερμηνεύεται διασταλτικά, δηλαδή να περιλαμβάνει παραδείγματος χάριν τεχνολογική ανάπτυξη και επίδειξη, βασική έρευνα, εφαρμοσμένη έρευνα και ιδιωτικά χρηματοδοτούμενη έρευνα. Επιπλέον, θα πρέπει να λαμβάνει υπόψη τον στόχο της Ένωσης δυνάμει του άρθρου 179 παράγραφος 1 ΣΛΕΕ για την επίτευξη ενός ευρωπαϊκού χώρου έρευνας. Στους σκοπούς επιστημονικής έρευνας θα πρέπει να περιλαμβάνονται και μελέτες που πραγματοποιούνται για το δημόσιο συμφέρον στον τομέα της δημόσιας υγείας (...)»*

☞ Για την πραγματοποίηση μίας επιστημονικής έρευνας, η συγκατάθεση των προσώπων μπορεί να αποτελεί νομική βάση αυτής εφόσον βέβαια πληροί τα κριτήρια για να είναι έγκυρη (βλ. Ενότητα 5). Ωστόσο, σαφώς μία τέτοια επεξεργασία μπορεί να είναι επιτρεπτή και χωρίς τη συγκατάθεση – και αυτό αφορά επίσης και τους σκοπούς της αρχειοθέτησης προς το δημόσιο συμφέρον. Οι πιθανές νομικές βάσεις, πλην της συγκατάθεσης, μπορεί να είναι είτε η έννομη υποχρέωση του υπευθύνου επεξεργασίας (άρ. 6 παρ. 1 στοιχ. γ΄) είτε η εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον που του έχει ανατεθεί (άρ. 6 παρ. 1 στοιχ. ε΄) είτε – για περίπτωση όπου ο υπεύθυνος επεξεργασίας δεν είναι δημόσιος φορέας – το υπέρτερο έννομο συμφέρον αυτού (συμφέρον (άρ. 6 παρ. 1 στοιχ. στ΄). Αυτές είναι και οι περιπτώσεις που πρέπει να ληφθεί ιδιαίτερη μέριμνα στην παροχή εγγυήσεων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ακριβώς διότι εκλείπει η συγκατάθεσή τους.

Στο ν. 4624/2019 γίνεται επίσης ειδική αναφορά σε διασφαλίσεις για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων εν όψει των ανωτέρω σκοπών. Συγκεκριμένα, στο άρθρο 30 παρ. 1 του ν. 4624/2019 αναφέρεται ότι επιτρέπεται η επεξεργασία χωρίς τη συγκατάθεση του υποκειμένου, όταν η επεξεργασία είναι απαραίτητη για σκοπούς επιστημονικής ή ιστορικής έρευνας ή συλλογής και τήρησης στατιστικών στοιχείων και το συμφέρον του υπεύθυνου επεξεργασίας είναι υπέρτερο του συμφέροντος του υποκειμένου να μην τύχουν επεξεργασίας τα δεδομένα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προσωπικού του χαρακτήρα. Στην ίδια διάταξη αναφέρεται ότι ο υπεύθυνος επεξεργασίας υποχρεούται να λαμβάνει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των εννόμων συμφερόντων του υποκειμένου των δεδομένων. Στα μέτρα αυτά μπορούν να περιλαμβάνονται ιδίως: α) περιορισμοί πρόσβασης των υπεύθυνων επεξεργασίας και εκτελούντων την επεξεργασία, β) ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα, γ) κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα, δ) ορισμός ΥΠΔ. Σημειωτέο ότι η εν λόγω διάταξη κάνει ρητή αναφορά σε δεδομένα ειδικών κατηγοριών του άρθρου 9 του ΓΚΠΔ, αναφέροντας ότι επιτρέπεται η επεξεργασία τους για τους εν λόγω σκοπούς υπό τις προαναφερθείσες υποχρεώσεις[74]. Περαιτέρω, στην παράγραφο 4 του ιδίου άρθρου, ορίζεται ότι «*ο υπεύθυνος επεξεργασίας μπορεί να δημοσιεύει δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται στο πλαίσιο της έρευνας, εφόσον τα υποκείμενα των δεδομένων έχουν συγκατατεθεί εγγράφως ή η δημοσίευση είναι απαραίτητη για την παρουσίαση των αποτελεσμάτων της έρευνας. Στην τελευταία αυτή περίπτωση η δημοσίευση γίνεται με ψευδωνυμοποίηση*». Τέλος, στην παράγραφο 3 του ιδίου άρθρου αναφέρεται ότι «*οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα όταν υποβάλλονται σε επεξεργασία για τους σκοπούς της παραγράφου 1, θα πρέπει να ανωνυμοποιούνται αμέσως μόλις το επιτρέψουν οι επιστημονικοί ή στατιστικοί σκοποί, εκτός εάν αυτό είναι αντίθετο προς το έννομο συμφέρον του υποκειμένου των δεδομένων. Μέχρι τότε, τα χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για την αντιστοίχιση μεμονωμένων λεπτομερειών σχετικά με προσωπικές ή πραγματικές καταστάσεις ενός ταυτοποιημένου ή ταυτοποιήσιμου προσώπου πρέπει να αποθηκευτούν χωριστά. Τα χαρακτηριστικά αυτά μπορεί να συνδυαστούν με τις μεμονωμένες λεπτομέρειες, μόνο εάν το απαιτεί η έρευνα ή ο στατιστικός σκοπός*».

Οι ως άνω αναφερόμενες προβλέψεις του άρθρου 30 παρ. 1 του ν. 4624/2019 που αφορούν την επεξεργασία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή συλλογής και τήρησης στατιστικών στοιχείων επαναλαμβάνονται αυτούσιες και στο

[74] Υπενθυμίζεται ότι σύμφωνα με το άρθρο 9 παρ. 2 στοιχ. ι' του ΓΚΠΔ, επιτρέπεται κατ' εξαίρεση η επεξεργασία δεδομένων ειδικών κατηγοριών εφόσον «*η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων*».



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

άρθρο 29 παρ. 1 του ν. 4624/2019 που αφορά επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον.

**Παράδειγμα**: Δημόσιο ερευνητικό κέντρο/φορέας επιθυμεί να αποκτήσει πρόσβαση σε στοιχεία νοσηλειών νοσοκομείων σε όλη την Ελλάδα με σκοπό τη διεξαγωγή επιστημονικής έρευνας για συγκεκριμένη ασθένεια. Τα στοιχεία που το ερευνητικό κέντρο χρειάζεται να γνωρίζει για τους σκοπούς της έρευνας[75] είναι η ημερομηνία εισαγωγής του κάθε ασθενούς που διαγνώστηκε με την εν λόγω ασθένεια, η ηλικία, το φύλο του, καθώς και στοιχεία ως προς τη διάγνωση, τη θεραπεία και την έκβαση, σε συνδυασμό με τυχόν υποκείμενα νοσήματα.

Από την αρχή της ελαχιστοποίησης των δεδομένων συνάγεται ότι μπορεί να δοθεί πρόσβαση στο κέντρο/φορέα μόνο για τα απολύτως απαραίτητα δεδομένα για τους σκοπούς της ειδικής έρευνας που επιθυμεί (και την οποία οφείλει να καταδεικνύει και να τεκμηριώνει προς τα νοσοκομεία από τα οποία αιτείται πρόσβαση). Ως εκ τούτου, δεν μπορεί το εν λόγω ερευνητικό κέντρο/φορέας να αποκτήσει πρόσβαση, π.χ., σε άλλα δεδομένα νοσηλειών που τηρούν τα νοσοκομεία. Επίσης, μετά τη συλλογή των δεδομένων και πριν τη δημοσίευση ή καθ' οιονδήποτε άλλον τρόπο χρήση των αποτελεσμάτων της έρευνας, το κέντρο/φορέας θα πρέπει να προβαίνει στη μετατροπή των δεδομένων σε μορφή τέτοια ώστε να μην είναι εφικτή η αναγνώριση των προσώπων, καθώς επίσης και να καταστρέψει το τυχόν υπάρχον ονομαστικό αρχείο που έχει συλλεγεί.

Δημόσιες αρχές και δημόσιοι (ή ιδιωτικοί) φορείς που τηρούν αρχεία δημόσιου συμφέροντος θα πρέπει να είναι υπηρεσίες οι οποίες, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο, υπέχουν εκ του νόμου υποχρέωση να αποκτούν, να διατηρούν, να αξιολογούν, να ταξινομούν, να περιγράφουν, να ανακοινώνουν, να προωθούν, να διαδίδουν και να παρέχουν πρόσβαση σε αρχεία για το γενικό δημόσιο συμφέρον. Σε αυτό το πλαίσιο εντάσσεται και κάθε περαιτέρω επεξεργασία για σκοπούς

[75] Επισημαίνεται ότι το ποια είναι τα στοιχεία που θεωρούνται απολύτως απαραίτητα για τους σκοπούς της έρευνας θα μπορούσε να προσδιοριστεί επακριβώς, με κατάλληλη τεκμηρίωση της αναγκαιότητάς τους, μέσω εκπόνησης ΕΑΠΔ (η οποία εξάλλου, εφόσον πρόκειται για επεξεργασία μεγάλης κλίμακας, θα ήταν σε μία τέτοια περίπτωση υποχρεωτική – βλ. Ενότητα 10).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αρχειοθέτησης, λόγου χάρη με στόχο την παροχή συγκεκριμένων πληροφοριών σχετικών με πολιτική συμπεριφορά σε πρώην απολυταρχικά καθεστώτα, γενοκτονία, εγκλήματα κατά της ανθρωπότητας, ιδίως το Ολοκαύτωμα, ή εγκλήματα πολέμου (βλ. αιτιολογική Σκέψη 158 του ΓΚΠΔ). Τα ανωτέρω εμπίπτουν στο ΓΚΠΔ, όπως άλλωστε εμπίπτει και η ιστορική έρευνα αλλά και η έρευνα για γενεαλογικούς σκοπούς και, άρα, τυγχάνουν εφαρμογής οι προβλέψεις του άρθρου 89. Σημειωτέο βέβαια ότι, όπως αναφέρθηκε και στην Ενότητα 3, ο ΓΚΠΔ δεν ισχύει για όσους δεν βρίσκονται στη ζωή.

**Παρεκκλίσεις από δικαιώματα**

Η σημασία που δίνει ο ΓΚΠΔ στην έρευνα αλλά και στην αρχειοθέτηση προς το δημόσιο συμφέρον απορρέει και από τις λοιπές προβλέψεις του άρθρου 89. Συγκεκριμένα στην παράγραφο 2 ορίζεται ότι είτε ο ενωσιακός είτε ο εθνικός νομοθέτης μπορεί, για επεξεργασία προσωπικών δεδομένων για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, να προβλέπει παρεκκλίσεις από τα δικαιώματα που αναφέρονται στα άρθρα 15 (δικαίωμα πρόβασης), 16 (δικαίωμα διόρθωσης), 18 (δικαίωμα περιορισμού της επεξεργασίας) και 21 (δικαίωμα εναντίωσης), με την επιφύλαξη των προαναφερθέντων προϋποθέσεων και των εγγυήσεων, εφόσον τα εν λόγω δικαιώματα είναι πιθανό να καταστήσουν αδύνατη ή να παρακωλύσουν σοβαρά την επίτευξη των ειδικών σκοπών και εφόσον οι εν λόγω παρεκκλίσεις είναι απαραίτητες για την εκπλήρωση των εν λόγω σκοπών. Με άλλα λόγια, αν η ικανοποίηση των ως άνω δικαιωμάτων δεν επιτρέπει την επίτευξη των ως άνω σκοπών – και εφόσον βέβαια έχει ληφθεί μέριμνα για τις εγγυήσεις ως προς τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων από την εν λόγω επεξεργασία – τότε δύναται νόμος να ορίζει ότι, κατ' εξαίρεση, δεν υπάρχει υποχρέωση για την ικανοποίησή τους.

Ο εθνικός νομοθέτης πράγματι αξιοποίησε τη δυνατότητα που δίνει ο ΓΚΠΔ και προβλέπει παρεκκλίσεις από τα δικαιώματα εν όψει των ανωτέρω σκοπών. Συγκεκριμένα, στο άρθρο 30 παρ. 2 του ν. 4624/2019 αναφέρεται: «*Κατά παρέκκλιση των οριζόμενων στα άρθρα 15, 16, 18 και 21 του ΓΚΠΔ, τα δικαιώματα του*

*υποκειμένου των δεδομένων προσωπικού χαρακτήρα περιορίζονται, εφόσον η άσκησή τους είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την εκπλήρωση των σκοπών της παραγράφου 1 (σσ. σκοποί επιστημονικής ή ιστορικής έρευνας ή συλλογής και τήρησης στατιστικών στοιχείων) και εφόσον οι περιορισμοί αυτοί κρίνονται απαραίτητοι για την εκπλήρωσή τους. Για τον ίδιο λόγο δεν εφαρμόζεται και το προβλεπόμενο στο άρθρο 15 του ΓΚΠΔ δικαίωμα πρόσβασης του υποκειμένου, όταν τα δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα για επιστημονικούς σκοπούς και η παροχή πληροφοριών απαιτεί δυσανάλογη προσπάθεια».*

Αντιστοίχως, στην παράγραφο 3 του άρθρου 89 του ΓΚΠΔ ορίζεται ο ενωσιακός ή εθνικός νομοθέτης μπορεί, όταν πρόκειται για επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, να προβλέπει παρεκκλίσεις από τα δικαιώματα που αναφέρονται στα άρθρα 15 (δικαίωμα πρόσβασης), 16 (δικαίωμα διόρθωσης, 18 (δικαίωμα περιορισμού της επεξεργασίας), 19 (γνωστοποίηση όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας), 20 (δικαίωμα φορητότητας) και 21 (δικαίωμα εναντίωσης), με την επιφύλαξη των προαναφερθέντων προϋποθέσεων και εγγυήσεων, εφόσον τα εν λόγω δικαιώματα είναι πιθανό να καταστήσουν αδύνατη ή να παρακωλύσουν σοβαρά την επίτευξη των ειδικών σκοπών και εφόσον οι εν λόγω παρεκκλίσεις είναι απαραίτητες για την εκπλήρωση των εν λόγω σκοπών.

Και σε αυτήν την περίπτωση, ο εθνικός νομοθέτης αξιοποίησε τη δυνατότητα που δίνει ο ΓΚΠΔ και προβλέπει παρεκκλίσεις από τα δικαιώματα εν όψει του ανωτέρω σκοπού. Συγκεκριμένα, στο άρθρο 29 παρ. 2-4 του ν. 4624/2019 αναφέρονται τα εξής:

*«2. Κατά παρέκκλιση από το άρθρο 15 του ΓΚΠΔ, το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων σε δεδομένα που το αφορούν μπορεί να περιοριστεί, εφόσον η άσκησή του είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την επίτευξη των σκοπών της παραγράφου 1 (σσ. αρχειοθέτηση προς το δημόσιο συμφέρον), και η άσκηση του δικαιώματος θα απαιτούσε δυσανάλογη προσπάθεια.*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*3. Κατά παρέκκλιση από το άρθρο 16 του ΓΚΠΔ, το υποκείμενο των δεδομένων δεν έχει δικαίωμα διόρθωσης των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον η άσκησή του είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την επίτευξη των σκοπών της παραγράφου 1 (σσ. (σσ. αρχειοθέτηση προς το δημόσιο συμφέρον), ή την άσκηση δικαιωμάτων τρίτων.*

*4. Κατά παρέκκλιση των οριζόμενων στα άρθρα 18 παράγραφος 1 εδάφια α΄, β΄ και δ΄ και στα άρθρα 20 και 21 του ΓΚΠΔ, τα δικαιώματα του υποκειμένου των δεδομένων περιορίζονται, εφόσον η άσκησή τους είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την εκπλήρωση των σκοπών της παραγράφου 1 (σσ. αρχειοθέτηση προς το δημόσιο συμφέρον) και εφόσον οι περιορισμοί αυτοί κρίνονται απαραίτητοι για την επίτευξη των σκοπών αυτών.».*

☞ Πρέπει να επισημανθεί ότι, αν και είναι επιτρεπτή η - υπό προϋποθέσεις – παρέκκλιση από σύνολο δικαιωμάτων για περιπτώσεις επεξεργασίας για σκοπούς επιστημονικής έρευνας, στατιστικούς ή αρχειοθέτησης προς το δημόσιο συμφέρον, εν τούτοις υπάρχει ένα σημαντικό δικαίωμα για το οποίο δεν προβλέπεται ουσιαστικά παρέκκλιση: η ενημέρωση των υποκειμένων των δεδομένων (άρθρα 13 και 14 του ΓΚΠΔ). Συνεπώς, ο εκάστοτε υπεύθυνος επεξεργασίας οφείλει να λαμβάνει υπόψη τις σχετικές υποχρεώσεις για τη διαφάνεια της επεξεργασίας, ανεξαρτήτως του ότι πιθανώς να ισχύουν παρεκκλίσεις για άλλα δικαιώματα, όπως εκτέθηκε ανωτέρω.

**Παράδειγμα**: Δημόσιος φορέας θέλει να δημοσιοποιεί στατιστικά στοιχεία αναφορικά με τα αιτήματα των πολιτών που υποβλήθηκαν σε αυτόν, προκειμένου να καθίστανται διαθέσιμες πληροφορίες όπως πόσα αιτήματα υποβλήθηκαν, τι αφορούσαν, εάν και με ποιον τρόπο διεκπεραιώθηκαν κτλ. Σημειώνεται ότι η εν λόγω επεξεργασία, εφόσον προκύπτουν πράγματι δεδομένα στατιστικής φύσης από τα οποία δεν είναι εφικτό να αντιστοιχηθεί καμία πληροφορία σε ταυτοποιήσιμο πρόσωπο, θεωρείται συμβατή με τον αρχικό σκοπό για τον οποίο συνελέγησαν και υπέστησαν επεξεργασία τα δεδομένα, σύμφωνα με το άρθρο 5 παρ. 1 στοιχ. β’ του



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΓΚΠΔ (βλ. και Ενότητα 4). Εφόσον πολίτης, υποβάλλοντας αίτημα στον εν λόγω φορέα, ασκήσει δικαίωμα εναντίωσης για τη συγκεκριμένη επεξεργασία, συντρέχουν οι προϋποθέσεις του άρθρου 30 παρ. 2 του ν. 4624/2019 για τη μη ικανοποίησή του. Ωστόσο, ο φορέας πρέπει να παρέχει ενημέρωση για την εν λόγω επεξεργασία, σύμφωνα με το άρθρο 13 του ΓΚΠΔ.

Η παρέκκλιση από τα δικαιώματα στις παραπάνω περιπτώσεις δεν είναι παράλογη. Αν ο φορέας έχει εξασφαλίσει με μέτρα, όπως η ψευδωνυμοποίηση στην πηγή προέλευσής τους, ότι τα δεδομένα δεν είναι δυνατό να αντιστοιχηθούν σε συγκεκριμένο πρόσωπο, οι ενέργειες για την άρση της ψευδωνυμοποίησης θα είναι δυσχερείς και επιπλέον ενδέχεται να αποθαρρύνουν τη χρήση της.

**Ερώτηση δραστηριότητας**: Πολίτης διαπιστώνει ότι ερευνητικό κέντρο δημοσιεύει ερευνητικά αποτελέσματα τα οποία προκύπτουν από ανάλυση η οποία πραγματοποιείται σε αναρτήσεις χρηστών κοινωνικών δικτύων που είναι ελεύθερα προσβάσιμες σε όλους (ήτοι «δημόσια» προφίλ χρηστών). Ο πολίτης αντιλαμβάνεται, εκ της φύσης της έρευνας και όντας χρήστης κοινωνικού δικτύου, ότι τα δεδομένα του υπόκεινται σε επεξεργασία για τους εν λόγω επιστημονικούς σκοπούς του κέντρου, ενώ επίσης διαπιστώνει, μελετώντας τα ερευνητικά αποτελέσματα που αναρτώνται σε εβδομαδιαία βάση, ότι παρουσιάζονται με τρόπο τέτοιο ώστε να είναι εφικτή, σε όσους τα διαβάζουν, η αναγνώρισή του ως χρήστη του κοινωνικού δικτύου – χωρίς αυτό να προκύπτει ότι είναι αναγκαίο για το σκοπό της έρευνας, όπως αυτός προβάλλεται. Συνεπώς, υποβάλλει προς το ερευνητικό κέντρο τόσο δικαίωμα πρόσβασης, προκειμένου να μάθει επακριβώς ποια δεδομένα του υπέστησαν επεξεργασία (υποδηλώνοντας ποιος χρήστης του κοινωνικού δικτύου είναι, χρησιμοποιώντας για το αίτημά του την ίδια ηλεκτρονική διεύθυνση με αυτή με την οποία έχει εγγραφεί στο κοινωνικό δίκτυο και θεωρεί ευλόγως ότι είναι εις γνώσιν του ερευνητικού κέντρου που τη συνέλεξε) όσο και δικαίωμα εναντίωσης στην επεξεργασία. Το ερευνητικό κέντρο απαντά ότι βάσει των παρεκκλίσεων που προβλέπονται στο άρθρο 30 παρ. 2 του ν. 4624/2019, τα δικαιώματά του δεν μπορούν να ικανοποιηθούν. Σχολιάστε σχετικά.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 14.4 Προστασία δεδομένων εργαζομένων

Η επεξεργασία προσωπικών δεδομένων εργαζομένων από τον εργοδότη τους, στο πλαίσιο της σχέσης απασχόλησης, αποτελεί μία ιδιαίτερη κατηγορία επεξεργασίας, λαμβάνοντας υπόψη την εγγενώς ανισοβαρή σχέση μεταξύ εργοδότη και εργαζόμενου. Κατ' αρχάς, θα πρέπει να λαμβάνεται υπόψη ότι, όπως έχει κρίνει και το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου, η προστασία της ιδιωτικής ζωής, που θεμελιώνεται στο άρθρο 8 της ΕΣΔΑ, δεν εξαιρεί την επαγγελματική ζωή των εργαζομένων και δεν περιορίζεται στη ζωή εντός του χώρου κατοικίας. Επιπροσθέτως, όπως αναφέρεται και στο Έγγραφο Εργασίας WP55 για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας της Ομάδας Εργασίας του Άρθρου 29 [81], οι ηλεκτρονικές επικοινωνίες που γίνονται από επιχειρηματικούς χώρους μπορούν να καλύπτονται από τις έννοιες της ιδιωτικής ζωής και της αλληλογραφίας υπό την έννοια του άρθρου 8 της ΕΣΔΑ[76]. Με άλλα λόγια, οι εργαζόμενοι πρέπει να έχουν προσδοκία ιδιωτικότητας και στο χώρο εργασίας τους. Συναφής, και ακόμα επίκαιρη σε μεγάλο βαθμό, είναι και η 115/2001 Οδηγία της Αρχής [82].

Ο ΓΚΠΔ, στο άρθρο 88 παρ. 1, ορίζει ότι «*τα κράτη μέλη, μέσω της νομοθεσίας ή μέσω των συλλογικών συμβάσεων, μπορούν να θεσπίζουν ειδικούς κανόνες προκειμένου να διασφαλίζουν την προστασία των δικαιωμάτων και των ελευθεριών έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο της απασχόλησης, ιδίως για σκοπούς πρόσληψης, εκτέλεσης της σύμβασης απασχόλησης, συμπεριλαμβανομένης της εκτέλεσης των υποχρεώσεων που προβλέπονται από τον νόμο ή από συλλογικές συμβάσεις, διαχείρισης, προγραμματισμού και οργάνωσης εργασίας, ισότητας και πολυμορφίας στον χώρο εργασίας, υγείας και ασφάλειας στην εργασία, προστασίας της περιουσίας εργοδοτών και πελατών και για σκοπούς άσκησης και απόλαυσης, σε ατομική ή συλλογική βάση, δικαιωμάτων και παροχών που σχετίζονται με την απασχόληση και για σκοπούς*

[76] Στο ίδιο Έγγραφο Εργασίας η Ομάδα Εργασίας έκρινε ότι η έννοια του απορρήτου της αλληλογραφίας περιλαμβάνει την έννοια του απορρήτου των επικοινωνιών, με σκοπό να εξασφαλίσει στην ηλεκτρονική επικοινωνία τον ίδιο βαθμό προστασίας με αυτόν της παραδοσιακής αλληλογραφίας. Σημειώνεται ότι το άρθρο 8 παρ. 1 της Ευρωπαϊκής Σύμβασης για την Προστασία των Ανθρωπίνων Δικαιωμάτων και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ) ορίζει τα εξής: *«Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του»* (*βλ. και Ενότητα 2*).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*καταγγελίας της σχέσης απασχόλησης».* Συνεπώς, αναγνωρίζοντας τον ειδικό χαρακτήρα αυτής της επεξεργασίας, ο ΓΚΠΔ επιτρέπει στον εθνικό νομοθέτη να ρυθμίσει ειδικότερα το ζήτημα, θέτοντας εξειδικευμένους κανόνες με στόχο την προστασία των δικαιωμάτων και ελευθεριών των εργαζομένων. Περαιτέρω, στην παρ. 2 του ιδίου άρθρου, αναφέρεται «*οι εν λόγω κανόνες περιλαμβάνουν κατάλληλα και ειδικά μέτρα για τη διαφύλαξη της ανθρώπινης αξιοπρέπειας, των έννομων συμφερόντων και των θεμελιωδών δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα, με ιδιαίτερη έμφαση στη διαφάνεια της επεξεργασίας, τη διαβίβαση δεδομένων προσωπικού χαρακτήρα εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκούν κοινή οικονομική δραστηριότητα και τα συστήματα παρακολούθησης στο χώρο εργασίας*».

Πριν παραθέσουμε τις σχετικές προβλέψεις του ν. 4624/2019 αναφορικά με την επεξεργασία δεδομένων στο πλαίσιο της απασχόλησης, είναι σημαντικό να εστιάσουμε σε κάποια βασικά χαρακτηριστικά που διέπουν μία τέτοια επεξεργασία όταν ενέχει, κατά ένα τρόπο, την έννοια της «επιτήρησης» εργαζομένου. Κατ' αρχάς, μία τέτοια επεξεργασία δεν μπορεί, κατά κανόνα, να έχει ως νομική βάση τη συγκατάθεση του εργαζομένου – και αυτό γιατί, λόγω της προαναφερθείσας ανισοβαρούς σχέσης μεταξύ εργοδότη και εργαζόμενου, η συγκατάθεση δεν μπορεί να είναι ελεύθερη (και, άρα, δεν μπορεί να είναι έγκυρη), εκτός από ειδικές εξαιρέσεις. Μάλιστα, και ο ν. 4624/2019 έχει εμμέσως μία τέτοια αναφορά, αφού στο άρθρο 27 παρ. 2 αυτού ορίζεται ότι «*στην περίπτωση που η επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένου έχει κατ' εξαίρεση ως νομική βάση τη συγκατάθεσή του, για την κρίση ότι αυτή ήταν αποτέλεσμα ελεύθερης επιλογής, πρέπει να λαμβάνονται υπόψη κυρίως: α) η υφιστάμενη στη σύμβαση εργασίας εξάρτηση του εργαζομένου και β) οι περιστάσεις κάτω από τις οποίες χορηγήθηκε η συγκατάθεση. Η συγκατάθεση παρέχεται είτε σε έγγραφη είτε σε ηλεκτρονική μορφή και πρέπει να διακρίνεται σαφώς από τη σύμβαση εργασίας. Ο εργοδότης πρέπει να ενημερώνει τον εργαζόμενο είτε σε έγγραφη είτε σε ηλεκτρονική μορφή σχετικά με τον σκοπό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και το δικαίωμά του να ανακαλέσει τη συγκατάθεση σύμφωνα με το άρθρο 7 παράγραφος 3 του ΓΚΠΔ*». Ουσιαστικά λοιπόν, ο ν. 4624/2019 αναφέρει ότι η νομική βάση της συγκατάθεσης

μπορεί να υφίσταται μόνο κατ' εξαίρεση, για την οποία μάλιστα πρέπει να μπορεί να τεκμηριωθεί ότι δόθηκε ελευθέρως. Η αιτιολογική έκθεση του ν. 4624/2019 δίνει μία κατεύθυνση ως προς τις περιπτώσεις για τις οποίες θα μπορούσε η συγκατάθεση του εργαζομένου να αποτελεί πράγματι έγκυρη νομική βάση – π.χ. *όταν καθιερώνεται ένα σύστημα διαχείρισης της υγείας στο χώρο της απασχόλησης που σκοπό έχει την προαγωγή της υγείας των εργαζομένων ή όταν τα συμφέρονται εργοδότη και εργαζομένου συγκλίνουν (όπως λ.χ. η χρήση φωτογραφιών στο ενδοδίκτυο -intranet- με την έννοια ότι εργαζόμενοι και εργοδότες αλληλεπιδρούν στο χώρο της επιχείρησης).* Εφόσον όμως η επεξεργασία ενέχει, όπως προαναφέρθηκε, την έννοια της «επιτήρησης», η συγκατάθεση δεν μπορεί κατά κανόνα να είναι νομική βάση.

Στη γενική περίπτωση αυτή, και ιδίως για τον ιδιωτικό τομέα, η πιθανότερη νομική βάση που δύναται να έχει εφαρμογή - εάν πράγματι η επεξεργασία μπορεί να είναι επιτρεπτή - είναι αυτή του άρθρου 6 παρ. 1 στοιχ. στ': για παράδειγμα, αν η επεξεργασία αφορά στην ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού και για την επίτευξη του εν λόγω σκοπού γίνεται επεξεργασία δεδομένων εργαζομένων η οποία δεν προσβάλλει όμως τα θεμελιώδη δικαιώματα και ελευθερίες των εργαζομένων. Όμως, για να είναι πράγματι έγκυρη η εν λόγω νομική βάση, πρέπει να καθίσταται σαφές - και ο υπεύθυνος επεξεργασίας να μπορεί να το αποδείξει, με βάση την αρχή της λογοδοσίας - ότι δεν προσβάλλονται τα δικαιώματα των εργαζομένων σε σχέση με τον επιδιωκόμενο σκοπό. Ειδικά δε για δημόσιο φορέα, δεδομένου ότι εναπόκειται στον νομοθέτη να παρέχει διά νόμου τη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις δημόσιες αρχές, οπότε και η εν λόγω νομική βάση δεν εφαρμόζεται στην επεξεργασία από τις δημόσιες αρχές κατά την εκπλήρωση των καθηκόντων τους (βλ. και αιτιολογική σκέψη 47 του ΓΚΠΔ), μία τέτοια επεξεργασία θα πρέπει να έχει ως νομική βάση αυτή του άρθρου 6 παρ. 1 στοιχ. ε΄ (απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας): και σε αυτήν την περίπτωση βέβαια, η επεξεργασία θα πρέπει να σέβεται την ουσία του θεμελιώδους δικαιώματος της προστασίας δεδομένων των εργαζομένων.

**Παράδειγμα [βασισμένο στο** [83]**]:** Φορέας ο οποίος επεξεργάζεται υψηλής

σπουδαιότητας προσωπικά δεδομένα – η διαρροή των οποίων θα επέφερε εξαιρετικά δυσμενείς συνέπειες στα θιγόμενα πρόσωπα – αποφασίζει, κατόπιν διαχείρισης κινδύνων που εκπονεί, να ενσωματώσει ένα εργαλείο αποτροπής απώλειας δεδομένων (Data Loss Prevention tool). Μεταξύ των δυνατοτήτων που κρίνεται σκόπιμο από το φορέα να διαθέτει ένα τέτοιο εργαλείο είναι ο αυτοματοποιημένος έλεγχος της εξερχόμενης αλληλογραφίας, προκειμένου να ελέγχεται αν ένα μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει περιεχόμενο τέτοιο, το οποίο υποδηλώνει ότι η αποστολή του δεν πρέπει να γίνει γιατί πιθανότατα συνιστά διαρροή δεδομένων (π.χ. αν περιέχει δεδομένα υγείας). Αν ένα τέτοιο μήνυμα αναγνωριστεί ως «ύποπτο» για διαρροή (είτε εκ παραδρομής είτε όχι) προσωπικών δεδομένων, τότε γίνεται περαιτέρω έλεγχος αυτού από άνθρωπο (εντεταλμένο προς τούτο αρμόδιο στέλεχος του φορέα).

Ένα τέτοιο εργαλείο εγκυμονεί στη γενική περίπτωση σοβαρούς κινδύνους για τα δικαιώματα και τις ελευθερίες των εργαζομένων – για παράδειγμα, εάν προσωπικό μήνυμα εργαζομένου που αποστέλλει από το ηλεκτρονικό του ταχυδρομείο αναγνωριστεί, εσφαλμένα, ως «ύποπτο» διαρροής δεδομένων. Συνεπώς, εφόσον δεν υπάρξουν κατάλληλα εχέγγυα, δεν μπορεί να θεωρηθεί ότι μία τέτοια επεξεργασία από δημόσιο φορέα είναι απαραίτητη για την εκπλήρωση του δημόσιου καθήκοντός του (ενώ, και για ιδιωτικό φορέα, δεν προκύπτει ότι έχει εφαρμογή η διάταξη του άρθρου 6 παρ. 1 στοιχ. στ΄).

Μία τέτοια επεξεργασία θα μπορούσε ενδεχομένως να είναι επιτρεπτή αν ληφθούν, στο πλαίσιο αυτής, κατάλληλες διασφαλίσεις για τα δικαιώματα των εργαζομένων, με έμφαση στη διαφάνεια της επεξεργασίας. Για παράδειγμα, εφόσον πράγματι δεν υπάρχουν αποτελεσματικότερα μέτρα σε σχέση με την επιδιωκόμενη προστασία από αθέμιτη ή εκ παραδρομής διαρροή δεδομένων, θα πρέπει να ελεγχθεί με ποιον τρόπο μία τέτοια επεξεργασία δεν θα προσβάλλει τις ελευθερίες των εργαζομένων. Π.χ. ένα τέτοιο μέτρο θα ήταν το εξής: κάθε «ύποπτο» μήνυμα δεν θα ελέγχεται περαιτέρω αλλά θα έχει ως αποτέλεσμα, προτού σταλεί, την εμφάνιση αναδυόμενου μηνύματος στον αποστολέα αυτού υποδηλώνοντάς του τον κίνδυνο που διαφαίνεται από την αποστολή του (οπότε και ο εργαζόμενος θα έχει την ευχέρεια να μην προχωρήσει

στην αποστολή του, διασφαλίζοντας κατ' αυτόν τον τρόπο ότι – σε περίπτωση που πρόκειται για προσωπικό μήνυμα – δεν θα αναγνωστεί από άλλον και ούτε η Διοίκηση του φορέα θα αποκτήσει κάποια πληροφορία επ' αυτού). Σε κάθε δε περίπτωση, οι κανόνες «φιλτραρίσματος» του εργαλείου DLP θα πρέπει να είναι απόλυτα διαφανείς σε όλους τους εργαζόμενους.

Σημειώνεται ότι μία τέτοια επεξεργασία θεωρείται υψηλού ρίσκου και εμπίπτει σε αυτές για τις οποίες η Αρχή έχει κρίνει ότι είναι υποχρεωτική η εκπόνηση ΕΑΠΔ (βλ. Ενότητα 10)

**Παράδειγμα [βασισμένο στο** [83]**]:** Φορέας θέλει να διασφαλίσει την ελεγχόμενη πρόσβαση, για αυστηρά εξουσιοδοτημένο προς τούτο προσωπικό, σε χώρο που βρίσκεται και λειτουργεί κρίσιμος ηλεκτρομηχανολογικός και δικτυακός εξοπλισμός (server and network security operation room). Συνεπώς, η πρόσβαση στο χώρο επιτρέπεται μόνο με κατάλληλη ηλεκτρομαγνητική κάρτα και με εισαγωγή σωστού PIN – ενώ οι κάρτες πρέπει να επιδεικνύονται στη συσκευή-αναγνώστη (reader) και κατά την έξοδο του εργαζόμενου, επίσης εισάγοντας το σωστό PIN. Οι είσοδοι και έξοδοι του εξουσιοδοτημένου προσωπικού στο χώρο αυτό καταγράφονται, με βάση τις πληροφορίες που στέλνει ο «αναγνώστης» των καρτών σε βάση δεδομένων, προκειμένου αν συμβεί απώλεια εξοπλισμού ή γίνει κάποια ενέργεια κατά παράβαση του εσωτερικού κανονισμού ασφαλείας, να μπορεί να διαπιστωθεί ποιος εργαζόμενος βρισκόταν στο χώρο κατά το επίμαχο χρονικό διάστημα έτσι ώστε να μπορεί να διερευνηθεί το περιστατικό.

Μία τέτοια επεξεργασία, εφόσον είναι απόλυτα διαφανής προς τους εργαζόμενους (συμπεριλαμβανομένης της πληροφόρησης ως προς το χρόνο τήρησης των σχετικών δεδομένων που καταγράφονται, ο οποίος πρέπει να είναι τεκμηριωμένα ο απολύτως απαραίτητος) και εφόσον η κρισιμότητα του να διασφαλιστεί απολύτως ελεγχόμενη πρόσβαση στο χώρο είναι μεγάλη, δεν προσκρούει στις θεμελιώδεις προϋποθέσεις νομιμότητας επεξεργασίας δεδομένων και μπορεί να έχει εφαρμογή, εφόσον πρόκειται για δημόσιο φορέα, η νομική βάση του άρθρου 6 παρ. 1 στοιχ. ε΄). Είναι



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σημαντικό ωστόσο να τονιστεί ότι κάθε άλλη επεξεργασία επί των εν λόγω δεδομένων για διαφορετικό σκοπό είναι μη επιτρεπτή – όπως, για παράδειγμα, για την αξιολόγηση των υπαλλήλων ή/και τον έλεγχο της αποδοτικότητάς τους.

Επισημαίνεται ότι οι εργαζόμενοι, όπως προαναφέρθηκε, έχουν μια νόμιμη προσδοκία προστασίας της ιδιωτικής ζωής τους στον τόπο εργασίας, η οποία δεν αίρεται από το γεγονός ότι χρησιμοποιούν εξοπλισμό, συσκευές επικοινωνιών ή οποιεσδήποτε άλλες επαγγελματικές εγκαταστάσεις και υποδομές (π.χ. δίκτυο ηλεκτρονικών επικοινωνιών, wifi κ.λπ) του εργοδότη (βλ. και Απόφαση 34/2018 [84] της Αρχής). Συναφώς, το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου με απόφαση της 05-9-2017[77] έκρινε ότι παραβιάζεται το δικαίωμα του εργαζομένου στην προστασία του ιδιωτικού βίου κατά το άρθρο 8 της ΕΣΔΑ σε περίπτωση κατά την οποία λαμβάνει χώρα επιτήρηση των ηλεκτρονικών επικοινωνιών του από τον εργοδότη, χωρίς να έχει προηγουμένως ενημερωθεί τόσο για το ενδεχόμενο αυτό, όσο και για τις περιστάσεις διενέργειας μιας τέτοιας παρακολούθησης (σκοπός, φύση, έκταση, βαθμός περιορισμού του ατομικού δικαιώματος), η οποία μάλιστα θα πρέπει να αποτελεί το έσχατο μέσο επίτευξης του επιδιωκόμενου σκοπού. Συνεπώς, μία τέτοια πρόσβαση δεν απαγορεύεται μεν a priori, αλλά μπορεί κατ' εξαίρεση να επιτρέπεται μόνο εφόσον συντρέχει σύνολο προϋποθέσεων – και, βεβαίως, να μην αντίκειται σε ισχύουσα ειδικότερη νομοθεσία.

**Ερώτηση δραστηριότητας**: Η Διοίκηση ενός φορέα, προκειμένου να διαπιστώσει αν ένας εργαζόμενος δαπανά πολλές ώρες της εργασίας του «σερφάροντας» σε κοινωνικά δίκτυα κτλ. χωρίς αυτό να χρειάζεται για τους εργασιακούς σκοπούς, ζητά, κατά την απουσία με κανονική άδεια του υπαλλήλου, να γίνει έλεγχος στον Η/Υ του χωρίς την παρουσία του και χωρίς να ενημερωθεί, προκειμένου να εξαχθούν πληροφορίες για τις προσωπικές του δραστηριότητες πλοήγησης. Ο φορέας διαθέτει εσωτερική πολιτική ορθής χρήσης εξοπλισμού και δικτύων, από την οποία δεν προβλέπεται απαγόρευση χρήσης Η/Υ για προσωπικούς σκοπούς. Σχολιάστε σχετικά ως προς τη νομιμότητα της συγκεκριμένης επεξεργασίας από την πλευρά του φορέα.

[77] Υπόθεση Barbulescu v. Romania



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ο ν. 4624/2019 ρυθμίζει, στο άρθρο 27, το ζήτημα της επεξεργασία δεδομένων στο πλαίσιο της απασχόλησης, σύμφωνα με το περιθώριο που δίνει το άρθρο 88 του ΓΚΠΔ στον εθνικό νομοθέτη. Κατ' αρχάς, σύμφωνα με την παράγραφο 8 του εν λόγω άρθρου του ν. 4624/2019, ως εργαζόμενοι νοούνται οι απασχολούμενοι με οποιαδήποτε σχέση εργασίας ή σύμβαση έργου ή παροχής υπηρεσιών στο δημόσιο και στον ιδιωτικό φορέα, ανεξαρτήτως του κύρους της σύμβασης, οι υποψήφιοι για εργασία και οι πρώην απασχολούμενοι. Με άλλα λόγια, η έννοια του εργαζόμενου πρέπει να ερμηνεύεται με ευρεία έννοια. Από εκεί και ύστερα, ήδη αναλύθηκε νωρίτερα η παράγραφος 2 του εν λόγω άρθρου αναφορικά με τις προϋποθέσεις υπό τις οποίες η συγκατάθεση εργαζομένου θα μπορούσε, κατ' εξαίρεση, να είναι νομική βάση της επεξεργασίας. Περαιτέρω, στην παράγραφο 1 του άρθρου 27[78] εξειδικεύονται οι όροι νομιμότητας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων όταν αυτή έχει ως νομική βάση το άρθρο 6 παρ. 1 στοιχ. β' του ΓΚΠΔ («εκτέλεση σύμβασης»), ενώ με την παράγραφο 3 του ιδίου άρθρου[79] επαναλαμβάνεται η προβλεπόμενη στο άρθρο 9 παρ. 2 στοιχ. β' του ΓΚΠΔ εξαίρεση από την απαγόρευση που εισάγεται με την παρ. 1 του ίδιου άρθρου.

Ωστόσο, η Αρχή με τη Γνωμοδότηση 1/2020 έχει διατυπώσει την άποψη ότι οι εν λόγω διατάξεις του ν. 4624/2019 εμπεριέχουν σημεία που χρήζουν βελτίωσης/αλλαγής και ως εκ τούτου δεν θα αναλυθούν περαιτέρω στο παρόν ως προς το πώς «μεταφράζονται» στην πράξη. Συγκεκριμένα:

Ι) Για την παράγραφο 1, λαμβάνοντας υπόψη την αιτιολογική έκθεση του ν. 4624/2019 στην οποία παρατίθενται, ως παραδείγματα επεξεργασίας προσωπικών δεδομένων για την περίπτωση αυτή, η επεξεργασία βιομετρικών δεδομένων, η χρήση

[78] Σύμφωνα με το άρθρο 27 παρ. 1 του ν. 4624/2019, «*Δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορούν να υποβάλλονται σε επεξεργασία για σκοπούς της σύμβασης εργασίας, εφόσον είναι απολύτως απαραίτητο για την απόφαση σύναψης σύμβασης εργασίας ή μετά τη σύναψη της σύμβασης εργασίας για την εκτέλεσή της*».

[79] Σύμφωνα με το άρθρο 27 παρ. 3 του ν. 4624/2019, «*Κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με την έννοια του άρθρου 9 παράγραφος 1 του ΓΚΠΔ για τους σκοπούς της σύμβασης εργασίας επιτρέπεται, εάν είναι απαραίτητη για την άσκηση των δικαιωμάτων ή την εκπλήρωση νόμιμων υποχρεώσεων που απορρέουν από το εργατικό δίκαιο, το δίκαιο της κοινωνικής ασφάλισης και της κοινωνικής προστασίας και δεν υπάρχει κανένας λόγος να θεωρηθεί ότι το έννομο συμφέρον του υποκειμένου των δεδομένων σε σχέση με την επεξεργασία υπερτερεί. Η παράγραφος 2 ισχύει επίσης για τη συγκατάθεση στηνεπεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Η συγκατάθεση πρέπει να αναφέρεται ρητά στα δεδομένα αυτά (...)*»



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

συστημάτων γεωεντοπισμού, η κατάρτιση ενός κανονισμού χρήσης επικοινωνιακών μέσων και μέσων ηλεκτρονικής παρακολούθησης, αλλά και τα συστήματα καταγγελίας (whistleblowing), για τα οποία δεν μπορεί η νομική βάση να είναι η εκτέλεση σύμβασης κατά το άρθρο 6 παρ. 1 στοιχ. β' ΓΚΠΔ τότε, κατά τη Γνωμοδότηση 1/2020 της Αρχής, εφόσον ο σκοπός της εν λόγω διάταξης είναι να «*εισάγει μοναδική νομική βάση επεξεργασίας για κάθε σκοπό επεξεργασίας στο πλαίσιο των εργασιακών σχέσεων, στην οποία κατ' ουσία «συγχωνεύονται» οι νομικές βάσεις του άρθρου 6 παρ. 1 ΓΚΠΔ και άρα αποκλείεται η αυτοτελής εφαρμογή τους (πλην της συγκατάθεσης, που προβλέπεται ρητά στην παράγραφο 2 του άρθρου 27 του νόμου), η ρύθμιση έρχεται σε αντίθεση με τις διατάξεις του άρθρου 88 παρ. 1 ΓΚΠΔ με βάση τις οποίες επιτρέπεται η «θέσπιση ειδικών κανόνων» για την εξειδίκευση κανόνων επεξεργασίας που βασίζονται στις νομικές βάσεις του άρθρου 6 παρ. 1 ΓΚΠΔ και όχι για την δημιουργία νέων νομικών βάσεων ή τον αποκλεισμό εφαρμογής των νομικών βάσεων του ΓΚΠΔ*».

ΙΙ) Ως προς τη δε παράγραφο 3 του άρθρου 27, η Αρχή με την ως άνω Γνωμοδότηση κρίνει ότι η στην εν λόγω διάταξη δεν προβλέπονται αφενός, οι απαιτούμενες «*κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων*» κατά το άρθρο 9 παρ. 2 στοιχ. β' ΓΚΠΔ και αφετέρου τα «*κατάλληλα και ειδικά μέτρα για τη διαφύλαξη της ανθρώπινης αξιοπρέπειας, των έννομων συμφερόντων και των θεμελιωδών δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα, με ιδιαίτερη έμφαση στη διαφάνεια της επεξεργασίας, τη διαβίβασης δεδομένων προσωπικού χαρακτήρα εντός ομίλου επιχειρήσεων, ή ομίλου εταιριών που ασκούν κοινή οικονομική δραστηριότητα*» κατά το άρθρο 88 παρ. 2 του ΓΚΠΔ – ενώ μία γενική σχετική αναφορά που υπάρχει στο άρθρο 27 παρ. 4 του ν. 4624/2019[80] δεν μπορεί να χαρακτηριστεί ως αρκετή ως προς τον προσδιορισμό των εν λόγω μέτρων.

Πέραν των ανωτέρω σημείων, στο άρθρο 27 του ν. 4624/2019 γίνεται ειδική αναφορά ως προς το ότι οι σχετικές προβλέψεις του άρθρου ισχύουν για κάθε επεξεργασία, ακόμα και ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα των εργαζομένων,

[80] Σύμφωνα με το τελευταίο εδάφιο της εν λόγω παραγράφου, «*Τα διαπραγματευόμενα μέρη συμμορφώνονται με το άρθρο 88 παράγραφος 2 του ΓΚΠΔ*»



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ανεξάρτητα του αν αποθηκεύονται ή προορίζονται να αποθηκευτούν σε ένα σύστημα αρχειοθέτησης (βλ. άρθρο 27 παρ. 6 του ν. 4624/2019). Τέλος υπάρχει ειδική πρόβλεψη, στην παράγραφο 7 του εν λόγω άρθρου, στα κλειστά κυκλώματα οπτικής καταγραφής σε χώρους εργασίας. Συγκεκριμένα, σύμφωνα με την εν λόγω διάταξη:

«*Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω κλειστού κυκλώματος οπτικής καταγραφής εντός των χώρων εργασίας, είτε είναι δημοσίως προσβάσιμοι είτε μη, επιτρέπεται μόνο εάν είναι απαραίτητη για την προστασία προσώπων και αγαθών. Τα δεδομένα που συλλέγονται μέσω κλειστού κυκλώματος οπτικής καταγραφής δεν επιτρέπεται να χρησιμοποιηθούν ως κριτήριο για την αξιολόγηση της αποδοτικότητας των εργαζομένων. Οι εργαζόμενοι ενημερώνονται εγγράφως, είτε σε γραπτή είτε σε ηλεκτρονική μορφή για την εγκατάσταση και λειτουργία κλειστού κυκλώματος οπτικής καταγραφής εντός των χώρων εργασίας*».

Η εν λόγω πρόβλεψη του άρθρου 27 του ν. 4624/2019 είναι σε πλήρη συνάφεια και με την πρότερη νομολογία της Αρχής αναφορικά με την επεξεργασία δεδομένων μέσω συστημάτων βιντεοεπιτήρησης (βλ. και επόμενη υπο-ενότητα 14.5, όπου εξειδικεύονται οι προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων μέσω τέτοιων συστημάτων).

**Παράδειγμα:** Δημόσιος φορέας έχει τοποθετήσει κάμερα στην είσοδο του κτιρίου του, για το σκοπό της ασφάλειας (προστασία προσώπων και αγαθών)[81]. Δεν επιτρέπεται στη Διοίκηση του φορέα να χρησιμοποιήσει το τυχόν καταγεγραμμένο υλικό από την κάμερα προκειμένου να διαπιστώσει αν οι εργαζόμενοι τηρούν το ωράριο ή αν αποχωρούν αδικαιολογήτως από την Υπηρεσία: μία τέτοια επεξεργασία γίνεται για άλλο σκοπό, ο οποίος όχι μόνο δεν είναι συμβατός με τον αρχικό, αλλά είναι και μη επιτρεπτός σύμφωνα με τη διάταξη του άρθρου 27 παρ. 7 του ν. 4624/2019.

[81] Η νομιμότητα της επεξεργασίας δεδομένων μέσω μίας τέτοιας κάμερας αναλύεται στην υπο-ενότητα 14.5.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 14.5 Επεξεργασία δεδομένων μέσω συστημάτων βιντεοεπιτήρησης

Λαμβάνοντας υπόψη ότι τα συστήματα βιντεοεπιτήρησης χρησιμοποιούνται ευρέως σε διάφορους τομείς, συμπεριλαμβανομένης της Δημόσιας Διοίκησης, στην παρούσα ενότητα θα εστιάσουμε στις προϋποθέσεις νόμιμης επεξεργασίας δεδομένων μέσω αυτών, παρά το ότι ο ΓΚΠΔ δεν αφιερώνει κάποιο ειδικό άρθρο στα συστήματα βιντεοεπιτήρησης (οπότε οι προϋποθέσεις νόμιμης επεξεργασίας μέσω αυτών συνάγονται από τις γενικές προϋποθέσεις νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα).

### 14.5.1 Προστασία προσώπων και αγαθών

Κατ' αρχάς, θα εστιάσουμε στην μάλλον πιο συνηθισμένη περίπτωση χρήσης συστημάτων βιντεοεπιτήρησης, που είναι αυτή για την προστασία προσώπων και αγαθών (δηλαδή για την ασφάλεια ενός χώρου). Είναι μία περίπτωση όπου η νομική βάση της επεξεργασίας, στη γενική περίπτωση και ιδίως για υπευθύνους επεξεργασίας του ιδιωτικού τομέα, είναι το άρθρο 6 παρ. 1 στοιχ. στ' (έννομο συμφέρον του υπευθύνου επεξεργασίας): όμως, για να έχει πράγματι εφαρμογή η εν λόγω νομική βάση, θα πρέπει να καθίσταται σαφές ότι το έννομο συμφέρον του υπευθύνου επεξεργασίας είναι υπέρτερο σε σχέση με την προσβολή των δικαιωμάτων και των ελευθερίες των υποκειμένων των δεδομένων – άρα, πρέπει να υπάρχουν κατάλληλες διασφαλίσεις για τα υποκείμενα των δεδομένων. Όσον αφορά σε φορείς του δημόσιου τομέα, η λειτουργία ενός συστήματος βιντεοεπιτήρησης μπορεί να στηριχθεί στη νομική βάση του άρθρου 6 παρ. 1 ε', καθώς ένας φορέας έχει συνήθως αρμοδιότητα να προστατεύει το χώρο του, τα αγαθά του και το προσωπικό του. Στην περίπτωση αυτή, και πάλι γίνεται αντίστοιχη στάθμιση δικαιωμάτων, όπως με το έννομο συμφέρον, η αρχή της ελαχιστοποίησης επιβάλει τα δεδομένα να περιορίζονται μόνο σε αυτά που είναι αναγκαία για την ικανοποίηση του σκοπού ενώ η κρίση της νομιμότητας της επεξεργασίας βασίζεται και πάλι στην ικανοποίηση της αρχής της αναλογικότητας. Πρακτικά, αυτό συνεπάγεται ότι πρέπει να υπάρχουν περιορισμοί στα σημεία τοποθέτησης και στα πεδία λήψης των καμερών, αλλά και σε λοιπά χαρακτηριστικά της επεξεργασίας, προκειμένου να τεκμαίρεται ότι πράγματι η



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επεξεργασία είναι απολύτως αναγκαία εν όψει του επιδιωκόμενου σκοπού, ο οποίος δεν μπορεί να επιτευχθεί με ηπιότερα και λιγότερο επαχθή μέσα και δεν θίγονται ελευθερίες των προσώπων σε βαθμό τέτοιο που να υπερισχύουν του έννομου συμφέροντος (ιδιωτικός τομέας) ή να υπερβαίνουν αυτό που είναι πραγματικά απαραίτητο για την άσκηση της αρμοδιότητας (δημόσιος τομέας) του υπευθύνου επεξεργασίας.

Για την εν λόγω περίπτωση, η Αρχή έχει εκδώσει την Οδηγία 1/2011 [85], η οποία παρέχει ειδικές κατευθύνσεις και θα πρέπει να λαμβάνεται υπόψη από τους υπευθύνους επεξεργασίας (ανεξαρτήτως της φύσης του φορέα – Δημόσιος ή μη). Αν και η Οδηγία εκδόθηκε προ του ΓΚΠΔ, οι βασικές προϋποθέσεις νόμιμης εγκατάστασης και λειτουργίας τέτοιων συστημάτων (ήτοι επιτρεπτά σημεία τοποθέτησης και πεδία λήψης, μέγιστος χρόνος τήρησης καταγεγραμμένων δεδομένων κ.α.) παραμένουν ουσιαστικά ανεπηρέαστες – ενώ βέβαια, μετά το ΓΚΠΔ, είναι «αυξημένες» οι απαιτήσεις για διαφάνεια της επεξεργασίας, ήτοι τα πρόσωπα που καταγράφονται πρέπει ευχερώς να λαμβάνουν πλήρη ενημέρωση για τα χαρακτηριστικά της επεξεργασίας, όπως περιγράφεται στη συνέχεια.

☞ Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας οφείλει – σύμφωνα και με την αρχή της λογοδοσίας - να κάνει ανάλυση κινδύνων και την κατάλληλη στάθμιση μεταξύ των αντικρουόμενων συμφερόντων, προκειμένου να λάβει αποφάσεις για το εάν θα εγκαταστήσει σύστημα βιντεοεπιτήρησης και, σε καταφατική περίπτωση, με τι χαρακτηριστικά. Άλλωστε, σε συγκεκριμένες περιπτώσεις, είναι υποχρεωτική και η εκπόνηση ΕΑΠΔ πριν την έναρξη της επεξεργασίας, όπως είδαμε και στην Ενότητα 10. Η Οδηγία 1/2011 της Αρχής (αλλά και η συναφής νομολογία της) θα πρέπει να λαμβάνεται υπόψη.

**<u>Ποιος (μπορεί να) είναι ο υπεύθυνος επεξεργασίας</u>**

Η εγκατάσταση και λειτουργία συστήματος βιντεοεπιτήρησης σε έναν χώρο για την ασφάλεια αυτού μπορεί να πραγματοποιηθεί μόνο από το (φυσικό ή νομικό) πρόσωπο που έχει εμπράγματο δικαίωμα επί του χώρου για την ασφάλεια αυτού – όπως, κατά



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

περίπτωση, ο ιδιοκτήτης του χώρου ή όποιος τον διαχειρίζεται ή έχει νομική υποχρέωση για την ασφάλειά του. Οι κάμερες θα πρέπει να λαμβάνουν εικόνα από χώρο για τον οποίο ο υπεύθυνος επεξεργασίας έχει αρμοδιότητα επιτήρησης και όχι από άλλον χώρο.

**Παράδειγμα:** Δημόσιος φορέας μπορεί κατ' αρχήν – υπό τις προϋποθέσεις που αναλύονται στη συνέχεια – να τοποθετήσει κάμερες στους χώρους του για την προστασία προσώπων και αγαθών. Εφόσον όμως ο φορέας στεγάζεται σε συγκρότημα κατοικιών ή γραφείων, στο οποίο συγκρότημα στεγάζονται, μεταξύ άλλων, και άλλες Υπηρεσίες, ο φορέας δεν μπορεί να εγκαταστήσει κάμερες σε κοινόχρηστους χώρους (π.χ. σε διαδρόμους ορόφων ή στην κεντρική είσοδο του συγκροτήματος). Για την ασφάλεια των κοινόχρηστων χώρων, κάμερες μπορούν να εγκατασταθούν – υπό προϋποθέσεις – μόνο με απόφαση του οργάνου που είναι αρμόδιο για τη διαχείριση του συγκροτήματος (π.χ. της Γενικής Συνέλευσης), σύμφωνα με τις ειδικές διατάξεις του οικείου Κανονισμού[82].

**Επιτρεπτά και μη σημεία τοποθέτησης καμερών**

Όπως έχει κρίνει η Αρχή με την Οδηγία 1/2011:

1. Κατά την επιτήρηση της περιμέτρου κτιρίων με σκοπό την ασφάλεια προσώπων ή/και αγαθών (π.χ. προστασία της ιδιοκτησίας από φθορές), απαγορεύεται η λήψη εικόνας από παράπλευρες οδούς και πεζοδρόμια (μόνο σε εξαιρετικές περιπτώσεις και υπό προϋποθέσεις θα μπορούσε να είναι επιτρεπτή μία τέτοια επιτήρηση).
2. Δεν επιτρέπεται η λήψη εικόνας από εισόδους ή εσωτερικό γειτονικών κατοικιών ή κτιρίων.
3. Απαγορεύεται η εγκατάσταση τέτοιων συστημάτων σε χώρους για τους οποίους μία τέτοια εγκατάσταση θα προσέβαλε το σκληρό πυρήνα του

[82] Για ειδικές περιπτώσεις όπου σε όροφο κτιρίου δεν στεγάζεται άλλη Υπηρεσία/γραφείο ή οικία, ή στεγάζονται αλλά υπάρχει σύμφωνη γνώμη όσων επηρεάζονται από το σύστημα βιντεοεπιτήρησης, η Αρχή έχει εξειδικεύσει κανόνες για τη νόμιμη εγκατάσταση και λειτουργία (βλ. [104]).

δικαιώματος στην προστασία της ιδιωτικής ζωής – όπως για παράδειγμα χώροι και προθάλαμοι τουαλετών, ανεξάρτητα του είδους της επιχείρησης ή του φορέα που βρίσκονται οι χώροι αυτοί.

4. Σε έναν τυπικό χώρο γραφείων οργανισμού, η βιντεοεπιτήρηση πρέπει να περιορίζεται σε χώρους εισόδου και εξόδου, χωρίς να επιτηρούνται συγκεκριμένες αίθουσες γραφείων ή διάδρομοι. Εξαίρεση μπορεί να αποτελούν χώροι όπως ταμεία ή χώροι με χρηματοκιβώτια, ηλεκτρομηχανολογικό εξοπλισμό κτλ., υπό τον όρο ότι οι κάμερες εστιάζουν στο αγαθό που προστατεύουν κι όχι στους χώρους των εργαζομένων. Επίσης επιτρέπεται η εγκατάσταση καμερών σε χώρους στάθμευσης οχημάτων. Σε κάθε περίπτωση, το σύστημα δεν θα πρέπει να χρησιμοποιείται για την επιτήρηση εργαζομένων.

Ειδικότερες περιπτώσεις αναλύονται επίσης στην Οδηγία 1/2011 της Αρχής, όπως τα σχολεία και λοιποί χώροι που δραστηριοποιούνται ανήλικοι, καθώς επίσης και τα νοσοκομεία.

☞ Πρέπει να επισημανθεί ότι η περίπτωση χρήσης καμερών για επιτήρηση ασθενών στο πλαίσιο της παροχής υπηρεσιών υγείας αποτελεί επίσης ειδική έκφανση της προστασίας προσώπων και αγαθών. Ωστόσο, όπως κατευθύνει η Αρχή με την Οδηγία 1/2011, πρόσθετες προϋποθέσεις νομιμότητας πρέπει να συντρέχουν σε μία τέτοια περίπτωση – ενδεικτικά αναφέρεται ότι η ανάγκη χρήσης καμερών για το σκοπό της παροχής υπηρεσιών υγείας πρέπει να τεκμηριώνεται από επιτροπή αποτελούμενη από αρμόδιο ιατρικό και νοσηλευτικό προσωπικό, η οποία θα αποφασίσει για τους χώρους τοποθέτησης των καμερών και την εμβέλειά τους, ενώ η μονάδα ελέγχου του κυκλώματος θα πρέπει να εγκαθίσταται σε απομονωμένο χώρο, πρόσβαση στην οποία θα μπορούν να έχουν μόνο τα εξουσιοδοτημένα πρόσωπα του ιατρικού/νοσηλευτικού προσωπικού που ασχολούνται με την παρακολούθηση των ασθενών (η μονάδα ελέγχου θα πρέπει να είναι διαχωρισμένη από μονάδα ελέγχου καμερών που έχουν εγκατασταθεί για τους γενικότερους σκοπούς της ασφάλειας) [85].



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Χαρακτηριστικά της επεξεργασίας**

Όπως έχει κρίνει η Αρχή με την Οδηγία 1/2011:

1) Οι κάμερες με λειτουργία στρέψης και εστίασης κατά κανόνα δεν επιτρέπονται. Μπορούν να χρησιμοποιηθούν σε ειδικές περιπτώσεις κατά τις οποίες ο υπεύθυνος επεξεργασίας παρακολουθεί κινήσεις φυσικών προσώπων σε πραγματικό χρόνο προκειμένου να επέμβει άμεσα προς αποτροπή κάποιου συμβάντος (π.χ. νυχτερινή ασφάλεια σε μεγάλους χώρους, όπως εργοστάσια, αποθήκες κ.α.) και εφόσον έχουν ληφθεί όλα τα απαιτούμενα τεχνικά μέτρα για τον περιορισμό της περιοχής λήψης στην απολύτως απαραίτητη (π.χ. με χρήση της λειτουργίας απόκρυψης περιοχών - λειτουργία "μάσκας").
2) Δεν επιτρέπεται η καταγραφή ήχου (παρά μόνο σε ελάχιστες περιπτώσεις, κατ' εξαίρεση, όπου μπορεί να τεκμηριωθεί ότι είναι απόλυτα αναγκαίος για την επίτευξη του επιδιωκόμενου σκοπού).
3) Χρήση τεχνολογιών φιλικές προς την ιδιωτικότητα (π.χ. τεχνικές «θόλωσης») πρέπει να προτιμώνται, εφόσον με αυτές είναι επιτεύξιμος ο επιδιωκόμενος σκοπός.

**Χρόνος τήρησης των δεδομένων**

Όπως έχει κρίνει η Αρχή με την Οδηγία 1/2011, τα καταγεγραμμένα δεδομένα πρέπει να καταστρέφονται το αργότερο εντός δεκαπέντε ημερών, εφόσον δεν προκύπτει επέλευση συμβάντος που εμπίπτει στον επιδιωκόμενο σκοπό (και εφόσον δεν προβλέπεται κάτι διαφορετικό από ειδικότερες διατάξεις). Ο χρόνος τήρησης μπορεί να παραταθεί κατάλληλα εφόσον υπάρξει συμβάν.

Σημειώνεται ότι ακόμα και αν γίνεται μόνο λήψη εικόνας, χωρίς καταγραφή, εξακολουθεί να πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα.

**Ενημέρωση των υποκειμένων των δεδομένων και λοιπά δικαιώματα**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ο υπεύθυνος επεξεργασίας θα πρέπει να φροντίζει, στο πλαίσιο της υποχρέωσης ενημέρωσης των υποκειμένων των δεδομένων, ώστε πριν ένα πρόσωπο εισέλθει στην εμβέλεια του συστήματος βιντεοεπιτήρησης, να ενημερώνεται ότι πρόκειται να εισέλθει σε χώρο που βιντεοσκοπείται. Για αυτό, όπως αναφέρει και η Αρχή, στην Οδηγία 1/2011, πρέπει να αναρτώνται να αναρτώνται σε επαρκή αριθμό και εμφανές μέρος ευδιάκριτες πινακίδες, όπου θα αναγράφεται, μεταξύ άλλων, το πρόσωπο για λογαριασμό του οποίου γίνεται η βιντεοσκόπηση.

Μετά τη θέση σε ισχύ του ΓΚΠΔ, η Αρχή δημοσίευσε στην ιστοσελίδα της συστάσεις και υποδείγματα για την ικανοποίηση του δικαιώματος ενημέρωσης κατά την επεξεργασία δεδομένων μέσω συστημάτων βιντεοεπιτήρησης.. Οι συστάσεις αυτές βασίζονται στις σχετικές κατευθυντήριες γραμμές 3/2019 του ΕΣΠΔ [94] και μια από τις προτεινόμενες πινακίδες απεικονίζεται στην Εικόνα 12. Η εν λόγω ενημέρωση αποτελεί μία ενημέρωση 1ου επιπέδου, με τις βασικές πληροφορίες: ο υπεύθυνος επεξεργασίας θα πρέπει, ευχερώς, να διαθέτει και ενημέρωση αναλυτικότερη δευτέρου επιπέδου, για την οποία η Αρχή παρέχει επίσης υπόδειγμα[83].

[83] Βλ. το διαδικτυακό τόπο
**https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/eisagwgi_videoepitirisi/pilirofories_upef_videoepitirisi/ipodigmata_enimerosis**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης


**Εικόνα 12 - Πρότυπο ενημερωτικής πινακίδας για λειτουργία συστήματος βιντεοεπιτήρησης για το σκοπό της προστασίας προσώπων και αγαθών (από το site** www.dpa.gr **της Αρχής)**

Επίσης, ο υπεύθυνος επεξεργασίας οφείλει να ανταποκρίνεται κατάλληλα και στα δικαιώματα των υποκειμένων των δεδομένων – ιδίως δε στο δικαίωμα πρόσβασης, για το οποίο το υποκείμενο των δεδομένων πρέπει να υποδεικνύει την ημερομηνία και ώρα που βρέθηκε στο πεδίο λήψης των καμερών. Ο υπεύθυνος επεξεργασίας οφείλει, σύμφωνα με τα διαλαμβανόμενα στο άρθρο 12 του ΓΚΠΔ, να δώσει, σε περίπτωση άσκησης δικαιώματος πρόσβασης, αντίγραφο του τμήματος της εγγραφής σήματος εικόνας όπου έχει καταγραφεί το υποκείμενο των δεδομένων ή έντυπη σειρά στιγμιοτύπων από τις καταγεγραμμένες εικόνες ή, αναλόγως, να ενημερώσει εγγράφως ότι είτε το υποκείμενο των δεδομένων δεν απεικονίζεται είτε ότι έχει διαγραφεί το αντίστοιχο τμήμα του καταγεγραμμένου αρχείου. Εναλλακτικά, εφόσον συμφωνεί το υποκείμενο των δεδομένων, μπορεί να γίνει απλή επίδειξη της



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

καταγραφής (video).

> ☞ Κατά την ικανοποίηση του δικαιώματος πρόσβασης για καταγεγραμμένο από κάμερες υλικό, τυχόν λοιπά δεδομένα τρίτων εικονιζόμενων προσώπων πρέπει να απαλείφονται (π.χ. με θόλωση εικόνας). Αν το δικαίωμα πρόσβασης μπορεί να ικανοποιηθεί με απλή επίδειξη του υλικού, δεν χρειάζεται μία τέτοια απαλοιφή.

**Ασφάλεια της επεξεργασίας**

Και στην περίπτωση της επεξεργασίας μέσω συστημάτων βιντεοεπιτήρησης, ισχύει κατ' αναλογία η υποχρέωση του υπευθύνου επεξεργασίας για ασφάλεια αυτής. Στη συγκεκριμένη περίπτωση, η υποχρέωση αυτή «μεταφράζεται», μεταξύ άλλων, στην αποφυγή διάδοσης του καταγεγραμμένου υλικού σε μη νόμιμους αποδέκτες, τον έλεγχο της πρόσβασης στον κεντρικό χώρο ελέγχου και το χώρο αποθήκευσης του υλικού, την αποφυγή αλόγιστης χρήσης οθονών προβολής, την ασφαλή μετάδοση σήματος εικόνας κτλ.

**Ερώτηση δραστηριότητας**: Η Διοίκηση ενός φορέα αποφασίζει την εγκατάσταση κάμερας στην είσοδο του κτιρίου που στεγάζεται, για το σκοπό της ασφάλειας (προστασίας προσώπων και αγαθών). Σχετική ενημερωτική πινακίδα, κατά το πρότυπο της Εικόνα 12, έχει αναρτηθεί σε ευκρινές σημείο. Στο εν λόγω κτίριο δεν στεγάζεται άλλη Υπηρεσία. Στην οθόνη παρακολούθησης έχει πρόσβαση ο Διευθυντής, ο οποίος επίσης επιβλέπει για να δει αν οι εργαζόμενοι που εισέρχονται «χτυπάνε» τις κάρτες τους οι ίδιοι, επειδή έχει ισχυρές ενδείξεις ότι άτομα που αργούν να προσέλθουν δίνουν τις κάρτες τους σε συναδέλφους τους, για να «κρύψουν» την αργοπορημένη προσέλευσή τους. Σχολιάστε την επεξεργασία αυτή ως προς τη νομιμότητά της.

**Ερώτηση δραστηριότητας**: Η Διοίκηση ενός φορέα επιθυμεί την εγκατάσταση κάμερας σε σημείο του οδοστρώματος μπροστά από την είσοδο του κτιρίου που



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

στεγάζεται, επειδή στο σημείο αυτό παρκάρει συχνά Υπηρεσιακό όχημα. Σχολιάστε τη νομιμότητα της εν λόγω επεξεργασίας για τις εξής δύο περιπτώσεις: α) το εν λόγω σημείο δεν είναι αποκλειστικής χρήσης του φορέα (ήτοι επιτρέπεται να παρκάρει ο οποιοσδήποτε, ακόμα και ιδιώτης), β) το εν λόγω σημείο έχει διατεθεί με πράξη του οικείου Δήμου στο φορέα, για αποκλειστική στάθμευση Υπηρεσιακού οχήματος.

### 14.5.2 Επίβλεψη δημόσια προσβάσιμων χώρων

Όπως είδαμε νωρίτερα, ένας υπεύθυνος επεξεργασίας δεν μπορεί, για την ασφάλεια χώρου επί του οποίου έχει αρμοδιότητα να εγκαταστήσει κάμερες για την ασφάλειά του, να λαμβάνει εικόνα από περιβάλλοντα δημόσιο χώρο (π.χ. δρόμο ή/και πεζοδρόμιο). Η επιτήρηση δημόσια προσβάσιμου χώρου μπορεί να είναι επιτρεπτή για συγκεκριμένους σκοπούς και μόνο από αρμόδιες για τους εν λόγω σκοπούς αρχές. Ειδικότερα, ο ν. 3917/2011 προβλέπει, στο άρθρο 14 παρ. 1, ότι «*η εγκατάσταση και λειτουργία συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους, εφόσον συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα, επιτρέπεται μόνο για: α) τη διαφύλαξη της εθνικής άμυνας, β) την προστασία του πολιτεύματος και την αποτροπή εγκλημάτων προδοσίας της χώρας, γ) την αποτροπή και καταστολή εγκλημάτων που συνιστούν επιβουλή της δημόσιας τάξης, δ) την αποτροπή και καταστολή εγκλημάτων βίας, εμπορίας ναρκωτικών, κοινώς επικίνδυνων εγκλημάτων, εγκλημάτων κατά της ασφάλειας των συγκοινωνιών και εγκλημάτων κατά της ιδιοκτησίας, όταν με βάση πραγματικά στοιχεία συντρέχουν επαρκείς ενδείξεις ότι τελέσθηκαν ή πρόκειται να τελεσθούν τέτοιες πράξεις και ε) τη διαχείριση της κυκλοφορίας.*». Στο ίδιο άρθρο (παρ. 3) ορίζεται και η έννοια των δημόσιων χώρων, ως «*α) οι κατά την κείμενη νομοθεσία και τα σχέδια πόλεων προοριζόμενοι για κοινή χρήση, β) οι ελευθέρως προσβάσιμοι σε απροσδιόριστο αριθμό προσώπων ανοικτοί χώροι (περιφραγμένοι ή μη) που τίθενται σε κοινή χρήση με νόμιμο τρόπο και γ) οι σταθμοί διακίνησης επιβατών με μέσα μαζικής μεταφοράς*».

Ο νόμος προβλέπει την έκδοση Προεδρικού Διατάγματος για τη ρύθμιση, μεταξύ άλλων, των αρμόδιων κρατικών αρχών, της διαδικασίας και των προϋποθέσεων για



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

την εγκατάσταση και λειτουργία των συστημάτων επιτήρησης και των κριτηρίων για την τήρηση της αναλογικότητας μεταξύ των χρησιμοποιούμενων μέσων και του επιδιωκόμενου σκοπού. Το εν λόγω Προεδρικό Διάταγμα εκδόθηκε το 2020 (Π.Δ. 75/2020), αφού προηγουμένως η Αρχή είχε γνωμοδοτήσει επί σχεδίου αυτού (βλ. Γνωμοδότηση 3/2020 [60]). Πολλές από τις παρατηρήσεις της Αρχής ενσωματώθηκαν στις τελικές διατάξεις. Το περιεχόμενο των εν λόγω κειμένων εκφεύγει του αντικειμένου του παρόντος. Αξίζει ωστόσο να αναφερθεί ότι στην εν λόγω Γνωμοδότηση της Αρχής λαμβάνονται υπόψη οι σχετικές προβλέψεις τόσο του ΓΚΔΠ όσο και του Κεφαλαίου Δ του ν. 4624/2019 που ενσωματώνει την Οδηγία 2016/680 (αφού, στο μέτρο που αφορά επεξεργασία για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων εφαρμόζονται οι διατάξεις της Οδηγίας αυτής).

### 14.5.3 Άλλοι σκοποί επεξεργασίας

Η νομιμότητα επεξεργασίας δεδομένων εικόνας ή/και ήχου, μέσω καμερών, για άλλους σκοπούς, πέραν αυτών που συζητήθηκαν ανωτέρω, πρέπει να εξετάζεται ανά περίπτωση. Άλλοι πιθανοί σκοποί επεξεργασίας μπορεί να είναι, π.χ., η προβολή εκδήλωσης σε κοινωνικά δίκτυα ή στο Διαδίκτυο ευρύτερα (π.χ. βιντεοσκόπηση σχολικής εορτής), η διαφάνεια συνεδριάσεων συλλογικών οργάνων (π.χ. βιντεοσκόπηση ή μετάδοση συνεδρίασης Δημοτικού Συμβουλίου), εκπαιδευτικοί σκοποί όπως η τηλεκπαίδευση, τουριστικοί σκοποί (προβολή δράσεων Δήμου ή webcams σε τουριστικά σημεία) κτλ. Για κάθε σκοπό πρέπει να αναγνωρίζεται η κατάλληλη νομική βάση και να πληρούνται τα κατάλληλα εχέγγυα για τη διασφάλιση των ελευθεριών των υποκειμένων των δεδομένων – ενώ, πιθανότατα, σύμφωνα με τα όσα ειπώθηκαν στην Ενότητα 10, να είναι υποχρεωτική η προηγούμενη εκπόνηση ΕΑΠΔ.

## 14.6 Επεξεργασία βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου

Μία ιδιαίτερη περίπτωση επεξεργασίας δεδομένων είναι αυτή των βιομετρικών



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

δεδομένων. Σύμφωνα με το άρθρο 4 του ΓΚΠΔ, *βιομετρικά δεδομένα είναι δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα*. Ουσιαστικά, τα βιομετρικά δεδομένα αφορούν μόνιμα χαρακτηριστικά ενός ατόμου, μέσω των οποίων είναι δυνατή η αναγνώριση ή επαλήθευση της ταυτότητάς του με χρήση κατάλληλων τεχνολογιών. Στην κατηγορία αυτή εμπίπτουν τόσο σωματικά χαρακτηριστικά, όπως το δακτυλικό αποτύπωμα, το σχήμα παλάμης χεριού, η ίριδα του ματιού, η γεωμετρία του προσώπου κτλ. όσο και συμπεριφοράς (π.χ. τρόπος βαδίσματος).

Όπως ήδη είδαμε στην Ενότητα 5, τα βιομετρικά δεδομένα, εφόσον χρησιμοποιούνται για το σκοπό της αδιαμφισβήτητης ταυτοποίησης ενός προσώπου, θεωρούνται δεδομένα ειδικών κατηγοριών. Αυτή είναι μία εκ των πολλών «καινοτομιών» του ΓΚΔΠ σε σχέση με το προηγούμενο νομικό πλαίσιο, στο οποίο τα δεδομένα αυτά δεν θεωρούνταν ευαίσθητα. Ωστόσο, παρά το ότι δεν ήταν ευαίσθητα δεδομένα, οι ευρωπαϊκές αρχές προστασίας δεδομένων αντιμετώπιζαν κάθε τέτοια επεξεργασία ως επεξεργασία «ιδιαίτερης έντασης» και με πολλούς κινδύνους (καθώς, για παράδειγμα, η συλλογή βιομετρικών δεδομένων ενός χρήστη μπορεί να γίνεται ερήμην του): αυτή η θεώρηση των αρχών ουσιαστικά «επικυρώθηκε» με το ΓΚΠΔ, αφού πλέον κάθε τέτοια επεξεργασία, για να είναι επιτρεπτή, πρέπει επιπροσθέτως να πληροί μία εκ των εξαιρέσεων του άρθρου 9 του ΓΚΠΔ.

Ένα βιομετρικό σύστημα αυθεντικοποίησης χρήστη (π.χ. αναγνώριση μέσω δακτυλικού αποτυπώματος), προκειμένου να λειτουργήσει, θα πρέπει να διέλθει από τα ακόλουθα στάδια (βλ. [87]):

Α) «Εγγραφή» χρήστη. Στο στάδιο αυτό, που γίνεται μία φορά στην αρχή για τον κάθε χρήστη που θα αυθεντικοποιείται μέσω αυτού του συστήματος, πραγματοποιείται αρχικά η συλλογή των στοιχείων βιομετρίας του (π.χ. του δακτυλικού αποτυπώματος) με χρήση ειδικού αισθητήρα και, ακολούθως, από τα στοιχεία βιομετρίας εξάγεται το βιομετρικό «σχεδιότυπο» κάθε χρήστη: το



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

σχεδιότυπο αποτελεί μία διαρθρωμένη «σμίκρυνση» του βιομετρικού στοιχείου, το οποίο αποτελεί ένα είδος μέτρησής του (ήτοι μοναδικό σχεδιότυπο για τον κάθε χρήστη, εφόσον είναι μοναδικό για τον καθένα το πρωταρχικό βιομετρικό δεδομένο). Τέλος, το σχεδιότυπο (και όχι το πρωταρχικό βιομετρικό δεδομένα) αποθηκεύεται είτε σε μία κεντρική βάση δεδομένων που αποτελεί τμήμα του συνολικού βιομετρικού συστήματος επεξεργασίας είτε σε μία οπτική ή «έξυπνη» κάρτα: στην περίπτωση δε της κάρτας, οι χρήστες προφανώς μπορούν να τη φέρουν μαζί τους ως μέσο αναγνώρισης.

Β) Αυθεντικοποίηση (επαλήθευση) του χρήστη. Κάθε φορά που για το χρήστη χρήζει επαλήθευσης η ταυτότητά του, γίνεται «ανάγνωση» του αρχικού βιομετρικού του δεδομένου, υπολογίζεται εκ νέου το σχεδιότυπο και ελέγχεται αν το σχεδιότυπο που υπολογίστηκε ταυτίζεται με αυτό που είναι γνωστό ότι αντιστοιχεί στο χρήστη (είτε αυτό τηρείται σε βάση δεδομένων είτε σε κάρτα).

### 14.6.1 Έλεγχος πρόσβασης μέσω βιομετρικού συστήματος

Μία συνήθης χρήση βιομετρικού συστήματος είναι για τον έλεγχο της πρόσβασης σε έναν χώρο – ήτοι να ελέγχεται ακριβώς ποιος είναι ο εισερχόμενος. Αυτή η δυνατότητα μπορεί να αξιοποιηθεί για την επίτευξη διαφόρων επιμέρους σκοπών, χωρίς όμως να είναι όλοι επιτρεπτοί από τη σκοπιά της προστασίας δεδομένων προσωπικού χαρακτήρα.

Για παράδειγμα, η Αρχή έχει ήδη κρίνει, με το προηγούμενο νομικό πλαίσιο (προ ΓΚΠΔ), ότι η χρήση βιομετρικού συστήματος για τον έλεγχο της τήρησης του ωραρίου από υπαλλήλους δεν είναι επιτρεπτή. Συγκεκριμένα, όπως αποτυπώνεται, π.χ., στην Ετήσια Έκθεση της Αρχής για 2014 (σελ. 53), η Αρχή απαγόρευσε τη χρήση ενός τέτοιου συστήματος σε Δημοτικά κτίρια και νοσοκομεία, με το σκεπτικό ότι η χρήση βιομετρικού συστήματος εισάγει μια επαχθή και δυσανάλογη για τα υποκείμενα επεξεργασία σε σχέση με τον επιδιωκόμενο σκοπό, χωρίς αυτό να είναι απαραίτητο, καθώς ο έλεγχος μπορεί να πραγματοποιηθεί επαρκώς και με άλλα ηπιότερα εναλλακτικά μέσα, όπως με τη χρήση μαγνητικών καρτών χωρίς βιομετρικά



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

στοιχεία, με συνδυασμό δειγματοληπτικών ελέγχων προς επιβεβαίωση της παρουσίας των υπαλλήλων [88]. Καθίσταται απόλυτα σαφές ότι μία τέτοια επεξεργασία, για το συγκεκριμένο σκοπό, δεν είναι επιτρεπτή ούτε με το ΓΚΠΔ, με τον οποίο πλέον, το συναφές πλαίσιο είναι ακόμα πιο αυστηρό αφού πρόκειται πια για δεδομένα ειδικών κατηγοριών.

Μία τέτοια επεξεργασία θα μπορούσε να είναι επιτρεπτή για άλλους σκοπούς – π.χ. για τον έλεγχο της πρόσβασης σε εξαιρετικά κρίσιμες εγκαταστάσεις, όπου υπάρχουν μεγάλοι κίνδυνοι ασφάλειας αν εισέλθει πρόσωπο μη εξουσιοδοτημένο (π.χ. σε κρίσιμες εγκαταστάσεις αεροδρομίου). Σε τέτοιες περιπτώσεις, θα πρέπει πάντως να συντρέχει μία περίπτωση του άρθρου 9 βάσει της οποίας θα μπορούσε, κατ' εξαίρεση, να είναι επιτρεπτή η επεξεργασία – για παράδειγμα, μία πιθανή εξαίρεση είναι αυτή της παρ. 2 στοιχ. ζ' («*η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων*»).

**Ερώτηση δραστηριότητας**: Η Διοίκηση ενός φορέα επιθυμεί την εγκατάσταση βιομετρικού συστήματος αυθεντικοποίησης εισερχομένων στα κτίριά της, για τον έλεγχο της τήρησης του ωραρίου του προσωπικού, λόγω του ότι υπάρχουν ισχυρές ενδείξεις ότι οι μαγνητικές κάρτες που χρησιμοποιούνται για το σκοπό αυτό δεν είναι αποτελεσματικές, επειδή εργαζόμενοι που αργοπορούν δίνουν την κάρτα τους σε συνάδελφό τους για να την «χτυπήσει» την σωστή ώρα. Σχολιάστε τη νομιμότητα μίας τέτοιας επεξεργασίας.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# 15. Ειδικά θέματα τεχνολογιών και διαδικασιών

Πλησιάζοντας στο τέλος του παρόντος υλικού, θα δώσουμε έμφαση σε κάποια ειδικότερα τεχνολογικά θέματα τα οποία πρέπει να έχει κανείς υπόψη του, στο πλαίσιο της συμμόρφωσής του στην πράξη με τον ΓΚΠΔ. Τα θέματα αυτά ουσιαστικά δεν περιγράφονται ρητά εντός του κειμένου του ΓΚΠΔ – δηλαδή δεν θα τα βρει κανείς αναζητώντας τα εντός του (τουλάχιστον για την πλειοψηφία αυτών). Ωστόσο, απορρέουν κατ' ουσίαν από τις γενικότερες υποχρεώσεις που θέτει ο ΓΚΠΔ.

## 15.1 Πολιτική ασφάλειας

Η πολιτική ασφάλειας (security policy) αποτελεί θεμελιώδη λίθο για την ασφάλεια των δεδομένων (όχι μόνο προσωπικών δεδομένων αλλά κάθε είδους πληροφορίας) που επεξεργάζεται ένας οργανισμός. Ουσιαστικά, η πολιτική ασφάλειας είναι ένα κείμενο, εγκεκριμένο από τη Διοίκηση του οργανισμού, το οποίο αποτυπώνει τους γενικούς στόχους ασφάλειας των δεδομένων και συστημάτων επεξεργασίας του οργανισμού, προσδιορίζοντας κατ' αυτόν τον τρόπο την προσέγγιση που ακολουθεί ο οργανισμός στη διαχείριση της ασφάλειας. Αν και ο όρος «πολιτική ασφάλειας» στην πράξη χρησιμοποιείται με διάφορες έννοιες, η πιο κλασική του ερμηνεία είναι ότι πρόκειται για ένα κείμενο γενικού χαρακτήρα, το οποίο κατά κανόνα δεν αναμένεται να μεταβάλλεται συχνά και περιγράφει μόνο τα επιθυμητά αποτελέσματα και όχι τους τρόπους επίτευξής τους [97].

Μία πολιτική ασφάλειας θα πρέπει να «συνοδεύεται» από ειδικότερα κείμενα, που είθισται να λέγονται «τομεακές πολιτικές ασφάλειας», τα οποία είναι επιμέρους πολιτικές (σύνολο κανόνων): κάθε μία καλύπτει κάποιο ειδικό θέμα και απευθύνεται σε συγκεκριμένη ομάδα ατόμων εντός του οργανισμού. Παραδείγματα τέτοιων επιμέρους πολιτικών είναι η πολιτική ελέγχου πρόσβασης, η πολιτική ηλεκτρονικού ταχυδρομείου, η πολιτική αντιγράφων ασφαλείας, η πολιτική ασφάλειας επικοινωνιών, η πολιτική αποσπώμενων αποθηκευτικών μέσων, η πολιτική ορθής επιλογής συνθηματικών (passwords) κ.α. Πολύ συχνά, το σύνολο των επιμέρους πολιτικών περιγράφεται με τον όρο σχέδιο ασφάλειας (security plan). Οι επιμέρους



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

πολιτικές, εφόσον εξειδικεύουν κανόνες και μέτρα που πρέπει να ακολουθούνται, θα πρέπει να επικαιροποιούνται ανά τακτά διαστήματα και σίγουρα όταν ανακύπτει ανάγκη αλλαγής (π.χ. αν λάβει χώρα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα, από την αντιμετώπιση του οποίου προκύπτει ότι κάποια επιμέρους πολιτική ασφάλειας χρήζει τροποποίησης προς αποφυγή αντίστοιχου περιστατικού στο μέλλον).

Η γενική πολιτική ασφάλειας, όπως και οι επιμέρους πολιτικές, πρέπει να κοινοποιούνται στο προσωπικό του οργανισμού[84], να είναι εύκολα κατανοητές και εφαρμόσιμες. Για τη σωστή κατάρτιση των διαφόρων πολιτικών, είναι σημαντικό να υπάρξει προηγουμένως διαδικασία διαχείρισης κινδύνων ασφάλειας (βλ. Ενότητα 10).

Η έννοια της πολιτικής ασφάλειας ουσιαστικά υπάρχει και στο ΓΚΠΔ, αν και ίσως όχι ξεκάθαρα διατυπωμένη: συγκεκριμένα, όπως είδαμε και στην Ενότητα 10, το άρθρο 24 του ΓΚΠΔ ορίζει ότι μεταξύ των μέτρων που ενδεχομένως είναι απαραίτητο να λάβει ο υπεύθυνος επεξεργασίας προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι και η εφαρμογή κατάλληλων πολιτικών για την προστασία των προσωπικών δεδομένων. Μία πολιτική ασφάλειας, όπως περιγράφεται εδώ, αποτελεί μία έκφανση – προσανατολισμένη στην ασφάλεια, άρα στα μέτρα που αφορούν το άρθρο 32 - μίας τέτοιας γενικότερης πολιτικής για την προστασία δεδομένων.

> ☞ Η πολιτική ασφάλειας είναι επίσης στενά συνυφασμένη με την αρχή της λογοδοσίας του ΓΚΠΔ. Πολύ δύσκολα μπορεί ένας φορέας να αποδείξει ότι, αναφορικά με την ασφάλεια των δεδομένων, έχει προβεί στις απολύτως απαραίτητες ενέργειες για την ασφάλεια εάν δεν υπάρχει πολιτική ασφάλειας ή αν υπάρχει και δεν εφαρμόζεται.

Μία χρήσιμη πηγή για πολιτικές και σχέδια ασφαλείας είναι το [90].

[84] Βέβαια, όπως προαναφέρθηκε, κάποιες τομεακές πολιτικές απευθύνονται μόνο σε συγκεκριμένες κατηγορίες εργαζομένων



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## 15.2 Σύστημα Διαχείρισης Ασφάλειας - Οργανωτικά και τεχνικά μέτρα ασφάλειας

Όπως είδαμε στην Ενότητα 10, ο ΓΚΠΔ προκρίνει ουσιαστικά τη διαχείριση κινδύνων (risk management) ως προς την ασφάλεια της επεξεργασίας προσωπικών δεδομένων, προκειμένου να ληφθούν, τεκμηριωμένα, οι σωστές αποφάσεις για τα μέτρα ασφάλειας που θα υλοποιηθούν. Με άλλα λόγια, δεν ορίζονται κατ' αρχάς υποχρεωτικά μέτρα ασφάλειας που θα πρέπει να εφαρμόζει κάθε υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία, ανεξαρτήτως των άλλων παραμέτρων αυτής (η φύση της, το είδος και το πλήθος των δεδομένων, η σοβαρότητα των συνεπειών για τα θιγόμενα πρόσωπα σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα) αλλά αυτά πρέπει να αποφασίζονται, να υλοποιούνται, να εξετάζεται η αποτελεσματικότητά τους και να επικαιροποιούνται στο πλαίσιο ενός Συστήματος Διαχείρισης Ασφάλειας: ένα τέτοιο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (στις οποίες πληροφορίες ανήκουν προφανώς και τα προσωπικά δεδομένα) ορίζεται ως το σύνολο των πολιτικών, διαδικασιών, οδηγιών και πόρων που απαιτούνται προκειμένου να επιτευχθούν οι στόχοι που έχει θέσει ο οργανισμός για την ασφάλεια των πληροφοριών [97]. Το Σύστημα Διαχείρισης Ασφάλειας πρέπει να έχει τη συνεχή στήριξη της Διοίκησης σε ανώτατο επίπεδο: η καθιέρωση, η συντήρηση και η διαρκής επικαιροποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών αποτελούν ισχυρή ένδειξη ότι ο οργανισμός είναι σε θέση να ικανοποιήσει τις απαιτήσεις ασφάλειας που έχει καθορίσει [97].

Οι στόχοι ενός Συστήματος Διαχείρισης Ασφάλειας πρέπει να είναι προσανατολισμένοι στις απαιτήσεις ασφάλειας που έχει προδιαγράψει ο οργανισμός, οι οποίες με τη σειρά τους πρέπει να προσδιορίζονται με βάση μελέτη ανάλυσης και διαχείρισης κινδύνων. Η έννοια της ανάλυσης και διαχείρισης κινδύνων (η οποία είναι ευρύτερη και αφορά την ασφάλεια κάθε πληροφορίας, όχι μόνο των προσωπικών δεδομένων) συνίσταται στη συστηματική καταγραφή των αγαθών (πόρων) που χρήζουν προστασίας[85], της αποτίμησης των απειλών για κάθε ένα εξ

[85] Εφόσον εστιάζουμε στην προστασία δεδομένων προσωπικού χαρακτήρα, τα αγαθά είναι τα ίδια τα δεδομένα αλλά και κάθε υλικοτεχνικός εξοπλισμός που σχετίζεται με την επεξεργασία προσωπικών δεδομένων



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αυτών (όπου ως απειλή ορίζεται μία δυνητική αιτία πρόκλησης περιστατικού παραβίασης ασφάλειας), των ευπαθειών του κάθε αγαθού (όπου ως ευπάθεια ορίζεται ένα «αδύνατο» σημείο που θα μπορούσε να επιτρέψει την πραγματοποίηση/εκδήλωση μίας ή περισσότερων απειλών), και του αντίστοιχου κινδύνου (τι συνεπάγεται, τελικά, ως προς τη σοβαρότητα των συνεπειών, η εκδήλωση μιας απειλής).

**Παράδειγμα:** Για έναν απλό σταθμό εργασίας ενός φορέα που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων (συνδέεται με κεντρική βάση δεδομένων που τηρεί ο φορέας μέσω εσωτερικού δικτύου, αλλά οι χρήστες του σταθμού εργασίας μπορούν να αποθηκεύουν και αντίγραφα τοπικά), ως απειλή μπορεί να θεωρηθεί ένα φυσικό φαινόμενο (π.χ. πλημμύρα, φωτιά), ένα πρόβλημα τεχνικής φύσης (π.χ. αστοχία του «σκληρού» δίσκου, βλάβη συσκευής δικτύου, αστοχία λογισμικού εφαρμογής κ.α.), μία κακόβουλη ενέργεια από άνθρωπο (π.χ. εξωτερικός εισβολέας, κακόβουλο λογισμικό, κλοπή κ.α.) ή και μία αθέλητη ενέργεια καλόβουλου χρήστη (π.χ. κατά λάθος διαγραφή αρχείου, κατά λάθος αποστολή σε λάθος παραλήπτη κ.α.). Συναφείς ευπάθειες μπορούν να είναι π.χ. η έλλειψη διαδικασιών απόσυρσης ή/και συντήρησης υλικού, έλλειψη τεκμηρίωσης εφαρμογών, μη τήρηση αντιγράφων ασφαλείας, χρήση μη ασφαλών δικτύων, ευπάθειες κτιρίου ως προς φυσικά φαινόμενα, κ.α. Κάποιες δε ευπάθειες είναι «αναπόφευκτες».

Σε κάθε μεθοδολογία διαχείρισης κινδύνων, ο κίνδυνος (risk) προκύπτει ως συνάρτηση τόσο των συνεπειών που θα επέλθουν, σε περίπτωση εκδήλωσης συγκεκριμένης απειλής σε συγκεκριμένο αγαθό, όσο και της πιθανότητας εκδήλωσης της απειλής. Για τον υπολογισμό της πιθανότητας εκδήλωσης της απειλής λαμβάνονται υπόψη και τυχόν υπάρχοντα μέτρα ασφάλειας που ήδη είναι σε εφαρμογή για την αντιμετώπιση της συγκεκριμένης απειλής.

Υπάρχουν πολλές διαφορετικές μεθοδολογίες διαχείρισης κινδύνων ασφάλειας πληροφοριών – οι οποίες μεθοδολογίες είναι γενικότερες και αφορούν κάθε πληροφορία που επεξεργάζεται ένας οργανισμός και όχι μόνο προσωπικά δεδομένα (βλ. σχετικά και Ενότητα 10). Προφανώς, οι εν λόγω μεθοδολογίες μπορούν να



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προσαρμοστούν κατάλληλα για την περίπτωση της διαχείρισης κινδύνων ασφάλειας των προσωπικών δεδομένων. Οι συγκεκριμένες μεθοδολογίες «κατευθύνουν» τον οργανισμό στο να εκπονήσει ορθά τα βήματα που προαναφέρθηκαν – ήτοι να εκτιμήσει τις απειλές, τις ευπάθειες και τους κινδύνους – καθώς επίσης και να λάβει αποφάσεις, τεκμηριωμένα, για την ανάγκη ή μη λήψης πρόσθετων μέτρων ασφάλειας. Ο ΓΚΠΔ δεν προκρίνει κάποια συγκεκριμένη μεθοδολογία – και ούτε είναι υποχρεωτικό να ακολουθηθεί, από έναν οργανισμό, υποχρεωτικά μία εκ των γνωστών μεθοδολογιών. Το σημαντικό είναι να μπορεί τελικά ο οργανισμός, σύμφωνα και με την αρχή της λογοδοσίας, να αποδεικνύει ότι λαμβάνει τα δέοντα μέτρα ασφάλειας εν όψει των κινδύνων για την κάθε επεξεργασία.

Αν και, όπως αναφέρθηκε, καμία συγκεκριμένη μεθοδολογία διαχείρισης κινδύνων ασφάλειας δεν είναι υποχρεωτική, χρήσιμο είναι να γίνει μία αναφορά σε μία μεθοδολογία που ανέπτυξε ο Ευρωπαϊκός Οργανισμό Κυβερνοασφάλειας (ENISA) [91]. Ο λόγος είναι ότι η συγκεκριμένη μεθοδολογία είναι ειδικά προσανατολισμένη στην ασφάλεια των προσωπικών δεδομένων – οπότε η αποτίμηση των συνεπειών σε περίπτωση παραβίασης της ασφάλειας γίνεται με αυτό ως γνώμονα. Η μεθοδολογία αυτή απευθύνεται ιδίως σε μικρο-μεσαίες επιχειρήσεις, ωστόσο μπορεί να αξιοποιηθεί και από σύνολο δημοσίων φορέων.

Οι περισσότερες μεθοδολογίες διαχείρισης κινδύνων ασφάλειας καταλήγουν σε ένα σύνολο μέτρων ασφάλειας, κάποια εκ των οποίων θα πρέπει να επιλεγούν από τον οργανισμό που εκπονεί τη διαχείριση κινδύνων ως αποτέλεσμα αυτής ακριβώς της διαδικασίας διαχείρισης. Για παράδειγμα, η ως άνω αναφερθείσα μεθοδολογία του ENISA παραθέτει ένα σύνολο μέτρων ασφάλειας, βασισμένη στην αντίστοιχη λίστα του προτύπου ISO 27001. Ουσιαστικά, η μεθοδολογία προτείνει, με βάση την έκβαση της διαχείρισης κινδύνων, την υλοποίηση συγκεκριμένων μέτρων[86] (π.χ. εάν ο

[86] Όπως ειδικότερα αναφέρεται στο [91], *"(...) The matching of measures to specific risk levels should not be perceived as absolute. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk. Furthermore, the proposed list of measures does not take into account other additional sector specific security requirements, as well as specific regulatory obligations (...). In an attempt to further facilitate this procedure a mapping of the proposed group of measures with the ISO/IEC 27001:2013 security controls is also included*".



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κίνδυνος είναι υψηλός, απαιτούνται περισσότερα μέτρα από ό,τι αν κρίνεται χαμηλός).

Τα μέτρα ασφάλειας εντάσσονται σε δύο κύριες κατηγορίες: στα **οργανωτικά μέτρα ασφάλειας** και στα **τεχνικά μέτρα ασφάλειας**. Με απλά λόγια, στην πρώτη κατηγορία εντάσσονται διαδικασίες οργανωσιακού χαρακτήρα ενώ στη δεύτερη εντάσσονται μέτρα που σχετίζονται με συγκεκριμένες υλοποιήσεις τεχνικού χαρακτήρα. Υπάρχουν επικαλύψεις και συνέργειες μεταξύ των δύο κατηγοριών: για παράδειγμα, η διαχείριση χρηστών ενός πληροφοριακού συστήματος (ήτοι η λήψη αποφάσεων ως προς τι δικαιώματα πρόσβασης θα έχει κάθε χρήστης, είτε εσωτερικός είτε εξωτερικός, τι θα συμβαίνει με την αποχώρηση υπαλλήλου ή την μετακίνησή του σε άλλον τομέα/γραφείο κτλ.) είναι ένα μέτρο οργανωτικό, όμως η υλοποίηση στην πράξη των αποφάσεων που λαμβάνονται για τη διαχείριση χρηστών ενέχει και υλοποίηση κατάλληλων μηχανισμών ελέγχου πρόσβασης, που είναι ένα αμιγώς τεχνικό μέτρο ασφάλειας.

Στο υπόλοιπο της υπο-ενότητας παρουσιάζονται οι βασικές κατηγορίες οργανωτικών και τεχνικών μέτρων ασφάλειας. Η κάθε μία εξ αυτών αφήνει περιθώριο για διαφορετικούς τρόπους υλοποίησης, αναλόγως με τις ειδικές αποφάσεις που θα λάβει ο οργανισμός στο πλαίσιο της διαχείρισης κινδύνων – ενώ, επιπροσθέτως, κάποιες εξ αυτών των κατηγοριών μέτρων ασφάλειας ενδέχεται να είναι άνευ αντικειμένου σε ορισμένες περιπτώσεις οργανισμών. Το πώς θα υλοποιούνται στην πράξη οι εν λόγω κατηγορίες μέτρων ασφάλειας (εάν κριθεί αναγκαία, από τον οργανισμό, η υλοποίησή τους) μπορεί να αποτυπώνεται σε τομεακές πολιτικές ασφάλειας (βλ. υποενότητα 15.1).

### 15.2.1 Οργανωτικά μέτρα ασφάλειας

#### 15.2.1.1 Υπεύθυνος Ασφάλειας Πληροφοριών/Συστημάτων

Για τα θέματα ασφάλειας πληροφοριακών συστημάτων και δικτύων, μέσω των οποίων γίνεται επεξεργασία (και) προσωπικών δεδομένων, είναι σημαντικό να είναι



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

επιφορτισμένοι αρμόδιοι άνθρωποι με αρμοδιότητες επίβλεψης, παρακολούθησης, ελέγχου εφαρμογής πολιτικής ασφάλειας και μέτρων ασφάλειας, καθώς και εισήγησης για βελτιώσεις/αναθεωρήσεις μέτρων ασφάλειας ή/και πολιτικών ασφάλειας. Προς τούτο, είναι σημαντικό να υπάρχει διακριτή θέση υπευθύνου ασφαλείας πληροφοριών/συστημάτων (ενδεχομένως να αποτελείται ομάδα ατόμων), με σαφώς προδιαγεγραμμένες και καταγεγραμμένες αρμοδιότητες. Ο ρόλος του υπευθύνου ασφαλείας είναι καίριος και για την εκπόνηση διαχείρισης κινδύνων, αλλά και σε τυχόν εκπόνηση ΕΑΠΔ.

Είναι αυτονόητο ότι ένας τέτοιος ρόλος πρέπει να ανατίθεται σε άτομο που διαθέτει τα απαραίτητα επαγγελματικά προσόντα από πλευράς τεχνικών γνώσεων (π.χ. γνώσεων συστημάτων πληροφορικής και ασφάλειας συστημάτων) και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

Υπενθυμίζεται ότι, όπως είδαμε και στην Ενότητα 9, σε έναν τέτοιο ρόλο εντός ενός οργανισμού δεν θα πρέπει να ανατεθεί και ρόλος ΥΠΔ.

15.2.1.2 Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων

Κάθε Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών προβλέπει την θέσπιση σαφούς διαδικασίας για τη διαχείριση/αντιμετώπιση περιστατικών παραβίασης της ασφάλειας. Αντιστοίχως πρέπει να υπάρχει μία διαδικασία ειδικά για την περίπτωση περιστατικών παραβίασης προσωπικών δεδομένων: μια τέτοια διαδικασία θα ήταν ούτως ή άλλως υποχρεωτική, πολλώ δε μάλλον από τη στιγμή που ο ΓΚΠΔ θέτει και κάποιες ειδικές υποχρεώσεις ως προς αυτό το ζήτημα (όπως υποβολή γνωστοποίησης στην Αρχή, αξιολόγηση των κινδύνων έτσι ώστε, αν είναι υψηλοί, να ενημερωθούν αμελλητί τα θιγόμενα πρόσωπα κτλ.).

Μία τέτοια διαδικασία – η οποία δέον είναι να είναι καταγεγραμμένη σε μία αντίστοιχη πολιτική – θα πρέπει μεταξύ άλλων να αποσαφηνίζει ποιες περιπτώσεις θεωρούνται περιστατικά παραβίασης προσωπικών δεδομένων και να περιγράφει τον τρόπο αναφοράς των περιστατικών από τον οποιονδήποτε εργαζόμενο αντιληφθεί την



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ύπαρξη κάποιου (είτε αυτό έλαβε χώρα και δεν είναι πια σε εξέλιξη είτε είναι ακόμα σε εξέλιξη).

> ☞ Ως ενδεικτικά παραδείγματα, οι εργαζόμενοι θα πρέπει να γνωρίζουν ότι, π.χ., αν χαθεί έγγραφο με προσωπικά δεδομένα (είτε σε έντυπη μορφή είτε σε ψηφιακή – π.χ. απώλεια usb stick που περιείχε έγγραφα) ή αν διαπιστώσουν «ύποπτο» εισερχόμενο ηλεκτρονικό μήνυμα ή κάποια διαφορετική συμπεριφορά του υπολογιστή στον οποίον εργάζονται, αυτό θα πρέπει αμελλητί να κοινοποιηθεί στα κατάλληλα άτομα εντός του οργανισμού βάσει συγκεκριμένης διαδικασίας: τόσο το ποια είναι τα άτομα που πρέπει να ενημερωθούν, όσο και οι σχετικές διαδικασίες που θα ακολουθηθούν, πρέπει να είναι σαφώς καταγεγραμμένα.

15.2.1.3 Σχέδιο ανάκαμψης από καταστροφές

Ένα περιστατικό παραβίασης δεδομένων μπορεί να εξελιχθεί σε ένα σοβαρό ζήτημα που να πλήξει κατά τέτοιο τρόπο τα πληροφοριακά συστήματα και εν γένει την επεξεργασία προσωπικών δεδομένων ώστε να απαιτούνται δραστικά μέτρα προκειμένου ο οργανισμός να είναι σε θέση να ανακάμψει: για παράδειγμα, αν ο κεντρικός εξυπηρετητής Διαδικτύου (web server) ενός φορέα «καταρρεύσει» πλήρως (π.χ. λόγω μεγάλης τεχνικής βλάβης ή λόγω φυσικής καταστροφής ή λόγω εκτενούς διαδικτυακής επίθεσης), έτσι ώστε να μην είναι εφικτό σε εύλογο χρονικό διάστημα να είναι ξανά λειτουργικός, θα πρέπει να έχει προσχεδιαστεί μία διαδικασία που θα επιτρέψει τη συνέχιση λειτουργίας της κεντρικής ιστοσελίδας του φορέα.

Ένα σχέδιο ανάκαμψης από καταστροφές πρέπει να καταγράφει τις διαδικασίες που θα ακολουθούνται για την προστασία των προσωπικών δεδομένων σε περιπτώσεις εκτάκτων περιστατικών σημαντικού εύρους και δυσκολίας. Πρέπει κατ' ελάχιστο να περιγράφει τις συνθήκες υπό τις οποίες θα ενεργοποιείται (το σχέδιο), καθώς επίσης και να ορίζει τους σχετικούς ρόλους και αρμοδιότητες του προσωπικού που θα συντελέσουν στην υλοποίησή του. Ένα τέτοιο σχέδιο αναμένεται να είναι



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

προσανατολισμένο στα επιμέρους πληροφοριακά συστήματα ενός οργανισμού – και, άρα, είναι μοναδικό για τον κάθε οργανισμό. Θα πρέπει να επικαιροποιείται μετά από κάθε σημαντική αλλαγή στο πληροφοριακό σύστημα, αλλά και να διασφαλίζεται η αποτελεσματικότητά του με εκτέλεση δοκιμών για διάφορα σενάρια ενεργοποίησής του.

Περισσότερες πληροφορίες για τα χαρακτηριστικά ενός σχεδίου ανάκαμψης από καταστροφές υπάρχουν και στην ιστοσελίδα της Αρχής[87].

15.2.1.4 Υποχρέωση εμπιστευτικότητας του προσωπικού

Οι υπάλληλοι (μόνιμοι, συμβασιούχοι, εποχικοί), καθώς και οι εξωτερικοί συνεργάτες που εξουσιοδοτούνται να έχουν πρόσβαση σε προσωπικά δεδομένα, πρέπει να δεσμεύονται εγγράφως σχετικά με την τήρηση της εχεμύθειας και της εμπιστευτικότητας κατά τη διάρκεια της απασχόλησης και μετά την αποχώρησή τους. Ο οργανισμός, ως υπεύθυνος επεξεργασίας, οφείλει να κάνει τις δέουσες ενέργειες ώστε να διασφαλίζει κατ' ελάχιστον, ότι όλοι οι εργαζόμενοι είναι πλήρως ενήμεροι για τις υποχρεώσεις τους: η υποχρέωση αυτή προκύπτει ουσιαστικά και από τη διάταξη του άρθρου 32 παρ. 4 του ΓΚΠΔ, σύμφωνα με την οποία «*ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας*».

- ☞ Αν ένας Δημόσιος φορέας δεν προβεί σε καμία τέτοια ενημέρωση προς τους εργαζομένους του, θεωρώντας εκ προοιμίου ότι γνωρίζουν όλοι τις συναφείς υποχρεώσεις τους που απορρέουν, π.χ., από τον Κώδικα Δημοσίων Υπαλλήλων, πολύ δύσκολα μπορεί να αποδείξει ότι προέβη σε όλες τις απαραίτητες ενέργειες για την ασφάλεια των δεδομένων που επεξεργάζεται

[87] Βλ. **https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/sxedioanakamsisasfaleiaproswpikwnsxedioanakamsisasfaleiaproswpikwn** (τελευταία πρόσβαση: Ιανουάριος 2021).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

(ως οφείλει, σύμφωνα με την αρχή της λογοδοσίας).

15.2.1.5 Διαχείριση πληροφοριακών αγαθών

Για τα αγαθά/πόρους που σχετίζονται με την επεξεργασία προσωπικών δεδομένων (πέραν των ίδιων των - φυσικών ή ηλεκτρονικών - αρχείων με τα δεδομένα, τέτοια αγαθά μπορεί να είναι προγράμματα λογισμικού, υλισμικό (hardware), στοιχεία δικτύου τα οποία υπεισέρχονται σε επεξεργασία προσωπικών δεδομένων κτλ.) θα πρέπει να υπάρχει τόσο καταγραφή τους όσο και κατάλληλες διαδικασίες για τη διαχείρισή τους.

**Παράδειγμα:** Οργανισμός ενδεχομένως να κρίνει σκόπιμο, στο πλαίσιο διαχείρισης κινδύνων που θα εκπονήσει, να καταρτίσει ειδική διαδικασία για τη διαχείριση φορητών/αποσπώμενων αποθηκευτικών μέσων (π.χ. εξωτερικοί «σκληροί» δίσκοι, φορητοί υπολογιστές κτλ.). Μία τέτοια διαδικασία/πολιτική θα μπορούσε, για παράδειγμα, να περιλαμβάνει την έγκριση αρμόδιου προσώπου για τη μεταφορά ενός τέτοιου μέσου, που περιέχει προσωπικά δεδομένα, εκτός του οργανισμού, την υποχρεωτική κρυπτογράφηση αυτού ή και ακόμα την απαγόρευση αποθήκευσης συγκεκριμένων κατηγοριών αρχείων με προσωπικά δεδομένα κ.α.

15.2.1.6 Διαχείριση χρηστών

Είναι σημαντικό να υπάρχουν σαφώς αποτυπωμένες διαδικασίες (ιδανικά, μία σε μία πολιτική ασφάλειας) ως προς τη διαχείριση των χρηστών ενός πληροφοριακού συστήματος, η οποία θα πρέπει να περιλαμβάνει τουλάχιστον τα εξής:

α) διαδικασία για εισαγωγή νέου χρήστη ή για μεταβολή των δικαιωμάτων των χρηστών (π.χ. κατά τη μετάθεση υπαλλήλου σε άλλο Γραφείο/Τμήμα) στο σύστημα,

β) διαδικασία για τη διαγραφή μη ενεργού χρήστη (π.χ. σε περίπτωση αποχώρησης υπαλλήλου),

γ) κατηγοριοποίηση των χρηστών σε ομάδες ανάλογα με τα δικαιώματα πρόσβασης που αυτοί έχουν στους πόρους του συστήματος (τα οποία δικαιώματα θα πρέπει να αποφασίζονται στην βάση της λεγόμενης αρχής «need-to-know» - δηλαδή, ο κάθε



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

εργαζόμενος θα πρέπει να έχει πρόσβαση σε προσωπικά δεδομένα μόνο εφόσον αυτό είναι αναγκαίο με βάση το ρόλο/καθήκοντα που του έχουν ανατεθεί – και όχι σε περισσότερα προσωπικά δεδομένα από ό,τι τα καθήκοντά του απαιτούν).

Η διαχείριση χρηστών αφορά και εξωτερικούς συνεργάτες (π.χ. προσωπικό εκτελούντος την επεξεργασία που έχει πρόσβαση στο πληροφοριακό σύστημα).

15.2.1.7 Εκτελούντες την επεξεργασία

Οι συμβάσεις (ή άλλες νομικές πράξεις) μεταξύ ενός υπευθύνου επεξεργασίας και εκτελούντων την επεξεργασία θα πρέπει να έχουν συγκεκριμένο περιεχόμενο που να διασφαλίζει ότι οι τελευταίοι γνωρίζουν τις υποχρεώσεις τους οι οποίες απορρέουν από το νομικό πλαίσιο για την προστασία προσωπικών δεδομένων – ειδικότερα δε ότι οι εκτελούντες δρουν μόνο κατ' εντολή του υπευθύνου επεξεργασίας, υπόκεινται σε καθεστώς εχεμύθειας/εμπιστευτικότητας και ότι εφαρμόζουν τις κατάλληλες πολιτικές ασφάλειας.

Όπως είδαμε στην Ενότητα 7, ο ΓΚΠΔ δίνει ιδιαίτερη βαρύτητα στο περιεχόμενο των συμβάσεων (ή άλλων νομικών πράξεων) μεταξύ υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασίας, θέτοντας σχετικώς ειδικότερες υποχρεώσεις (βλ. άρθρο 28 παρ. 3 του ΓΚΠΔ).

15.2.1.8 Καταστροφή δεδομένων

Λαμβάνοντας υπόψη την αρχή του περιορισμού της περιόδου αποθήκευσης (άρθρο 5 του ΓΚΠΔ), είναι κρίσιμο να διασφαλίζεται ότι, κατά τη διαγραφή/καταστροφή αρχείων με προσωπικά δεδομένα – είτε έγχαρτα είτε ηλεκτρονικά – αυτή γίνεται με τέτοιο τρόπο ώστε να μην είναι εφικτή η ανάκτηση των αρχείων. Με άλλα λόγια, πρέπει να υπάρχουν σαφείς διαδικασίες/πολιτικές αναφορικά με την ασφαλή καταστροφή δεδομένων. Για παράδειγμα, η ρίψη εντύπων με προσωπικά δεδομένα σε κάδο απορριμμάτων δεν αποτελεί μία διαδικασία ασφαλούς καταστροφής των εντύπων: αντ' αυτού, θα πρέπει να χρησιμοποιηθεί, π.χ., καταστροφέας εγγράφων. Αντίστοιχα, και στα ηλεκτρονικά αρχεία, η απλή διαγραφή του αρχείου – ακόμα και



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

από τον λεγόμενο «κάδο ανακύκλωσης» (recycle bin) – δεν συνεπάγεται αυτόματα ότι το αρχείο καθίσταται μη ανακτήσιμο: αντ' αυτού, υπάρχουν, π.χ., κατάλληλα εργαλεία λογισμικού που μπορούν να διασφαλίσουν την καθολική, μη αναστρέψιμη, διαγραφή ηλεκτρονικών/ψηφιακών αρχείων.

☞ Η Αρχή έχει εκδώσει την Οδηγία 1/2005 αναφορικά με την ασφαλή καταστροφή δεδομένων [92].

15.2.1.9 Εκπαίδευση του προσωπικού

Η εκπαίδευση των εργαζομένων αναφορικά με θέματα ασφάλειας αποτελεί ένα πολύ σημαντικό οργανωτικό μέτρο ασφάλειας, λαμβάνοντας υπόψη ότι ο ανθρώπινος παράγοντας αποτελεί μία βασική πηγή για περιστατικά παραβίασης δεδομένων: για παράδειγμα, ένα συχνό φαινόμενο διαχρονικά – όχι μόνο για δημόσιους αλλά και για ιδιωτικούς φορείς – είναι η παρείσφρυση κακόβουλου λογισμικού στα πληροφοριακά συστήματα του οργανισμού λόγω ενός παραπλανητικού κακόβουλου ηλεκτρονικού μηνύματος (e-mail) το οποίο «άνοιξε» κάποιος εργαζόμενος. Αν οι εργαζόμενοι ήταν σε θέση να «αναγνωρίζουν» ύποπτα ηλεκτρονικά μηνύματα, πολλά εξ αυτών των περιστατικών θα είχαν αποφευχθεί.

Ο οργανισμός θα πρέπει, ως οργανωτικό μέτρο ασφάλειας, να διασφαλίζει την εκπαίδευση του προσωπικού σε θέματα ασφάλειας δεδομένων – το εύρος και το αντικείμενο της οποίας προφανώς θα ποικίλει, αναλόγως την κατηγορία εργαζομένων στους οποίους θα απευθύνεται αλλά και, βεβαίως, της φύσης των επεξεργασιών προσωπικών δεδομένων που πραγματοποιούνται (για αυτό και οι ανάγκες εκπαίδευσης θα πρέπει, ιδανικά, να ανακύπτουν και να προσδιορίζονται στο πλαίσιο μιας διαχείρισης κινδύνων που θα εκπονήσει ο οργανισμός). Ανακαλώντας την αρχή της λογοδοσίας που εισάγει ο ΓΚΠΔ, ο υπεύθυνος επεξεργασίας θα πρέπει να καταδεικνύει – εφόσον η εκπαίδευση προκύπτει ως αναγκαίο οργανωτικό μέτρο ασφάλειας – ότι ακολουθεί συστηματική διαδικασία για την εκπαίδευση του προσωπικού (π.χ. μέσω συγκεκριμένων φυλλαδίων/εντύπων, εκπαιδευτικών σεμιναρίων κτλ.).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ο οργανισμός θα πρέπει επίσης να υποστηρίζει την εξειδικευμένη εκπαίδευση αναφορικά με τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών στο αρμόδιο προς τούτο προσωπικό (όπως, π.χ., σε διαχειριστές των συστημάτων, στελέχη Τμήματος Ασφάλειας Πληροφοριών και Δικτύων κτλ.).

15.1.10 Μέτρα φυσικής ασφάλειας

Κατάλληλες πολιτικές πρέπει να εφαρμόζονται αναφορικά και με τη φυσική ασφάλεια. Εδώ εμπίπτουν, μεταξύ άλλων, μέτρα για το χώρο εγκατάστασης κρίσιμου τεχνολογικού εξοπλισμού για το πληροφοριακό σύστημα (π.χ. ελεγχόμενη πρόσβαση – πόρτα ασφαλείας, κλιματισμός, πυρανίχνευση κτλ.), μέτρα ασφάλειας για το φυσικό αρχείο (π.χ. κλειδωμένα ντουλάπια), πολιτική «καθαρού γραφείου» κ.α.

## 15.2.2 Τεχνικά μέτρα ασφάλειας

15.2.2.1 Αναγνώριση και αυθεντικοποίηση

Ο οργανισμός πρέπει να λάβει τα κατάλληλα μέτρα για την αναγνώριση (identification) και αυθεντικοποίηση (authentication) χρηστών στα συστήματά του: αυτό ισχύει τόσο για εσωτερικούς χρήστες (εργαζόμενους) όσο και για εξωτερικούς χρήστες (στην περίπτωση όπου ο οργανισμός παρέχει διαδικτυακή υπηρεσία προς το κοινό, στην οποία πολίτες μπορούν να εγγράφονται προκειμένου να υποβάλουν διαδικτυακά αιτήματα, ερωτήματα κτλ. και να παρακολουθούν την έκβαση αυτών – ή και να ολοκληρώνεται η διεκπεραίωσή τους – μέσω διαδικτυακής πύλης). Μη εξουσιοδοτημένες προσβάσεις, λόγω λανθασμένης αυθεντικοποίησης ενός χρήστη, μπορούν να επιφέρουν εξαιρετικά δυσμενείς συνέπειες.

Στενά συνυφασμένη με τις έννοιες της αναγνώρισης και αυθεντικοποίησης χρηστών είναι η έννοια του *ελέγχου πρόσβασης (access control)*. Για να διασφαλίζεται ότι κάθε χρήστης έχει πρόσβαση μόνο στους πόρους που του είναι επιτρεπτό (βλ. τη διαχείριση χρηστών που συζητήθηκε ανωτέρω ως οργανωτικό μέτρο ασφάλειας)



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

πρέπει να είναι σε ισχύ κατάλληλοι μηχανισμοί αυθεντικοποίησης, όπως βέβαια και να έχει γίνει η ανάθεση κατάλληλων εξουσιοδοτήσεων ανά αυθεντικοποιημένο χρήστη. Ο πιο κλασικός μηχανισμός αυθεντικοποίησης είναι η χρήση συνθηματικού (password), αλλά ανάλογα με το αποτέλεσμα της διαχείρισης κινδύνων ενδέχεται σε αρκετές πια περιπτώσεις ένα συνθηματικό να μην είναι αρκετό και να απαιτούνται ισχυρότεροι μηχανισμοί αυθεντικοποίησης – όπως αυθεντικοποίηση πολλών παραγόντων (multi-factor authentication), ψηφιακά πιστοποιητικά κτλ.

**Διαχείριση συνθηματικών**

Η χρήση συνθηματικών αποτελεί αναμφίβολα τον πιο ευρέως διαδεδομένο μηχανισμό αυθεντικοποίησης (τόσο για δημόσιους όσο και για ιδιωτικούς φορείς) και, ως εκ τούτου, και έναν «αγαπημένο» στόχο για κακόβουλους εισβολείς. Κατά συνέπεια, πρέπει να γίνεται σωστή διαχείριση των συνθηματικών των χρηστών – η οποία, ιδανικά, θα πρέπει να αποτυπώνεται σε μία ειδική (τομεακή) πολιτική για τα συνθηματικά («password security policy»). Η σωστή διαχείριση των συνθηματικών καλύπτει δύο κύριους άξονες:

α) Επιλογή ασφαλών (μη προβλέψιμων) συνθηματικών από την πλευρά των χρηστών. Ο οργανισμός οφείλει να προβαίνει σε δέουσες ενέργειες ώστε να διασφαλίζει ότι χρήστες οι οποίοι έχουν πρόσβαση σε προσωπικά δεδομένα και αυθεντικοποιούνται, μέσω συνθηματικών, σε πληροφοριακά συστήματα, επιλέγουν μη προβλέψιμα συνθηματικά. Για την επίτευξη αυτού, πέραν της καθοδήγησης που μπορούν να έχουν οι χρήστες, θα πρέπει και ο οργανισμός με τεχνικά μέσα να θέτει συγκεκριμένους κανόνες για την επιλογή συνθηματικών, έτσι ώστε να μην επιτρέπεται σε έναν χρήστη να επιλέξει συνθηματικό που παραβιάζει τους κανόνες – π.χ. ορισμός ελάχιστου επιτρεπτού μήκους, απαίτηση για υποχρεωτική χρήση τόσο αλφαριθμητικών όσο και μη αλφαριθμητικών χαρακτήρων κ.α.

β) Προστασία των συνθηματικών. Ο οργανισμός θα πρέπει, ακριβώς λόγω της κρισιμότητάς τους και των σοβαρών συνεπειών που θα ανακύψουν από τυχόν διαρροή τους, να λαμβάνει τα κατάλληλα μέτρα για την προστασία των

συνθηματικών των χρηστών. Προς τούτο, βασικός κανόνας που πρέπει να τηρείται είναι ότι τα συνθηματικά των χρηστών δεν τηρούνται αυτούσια σε αναγνώσιμη μορφή: κατ' αυτόν τον τρόπο διασφαλίζεται ότι αφενός, σε περίπτωσης παραβίασης του σχετικού αρχείου, ο υποκλοπέας δεν θα μπορεί να «διαβάσει» τα αποθηκευμένα συνθηματικά και, αφετέρου, ούτε όσοι έχουν νόμιμη πρόσβαση στο σχετικό αρχείο συνθηματικών (π.χ. οι διαχειριστές (administrators) συστημάτων) γνωρίζουν τα συνθηματικά των χρηστών.

Για την επίτευξη του ως άνω στόχου – ήτοι την τήρηση συνθηματικών σε μη αναγνώσιμη μορφή κατά τρόπο τέτοιο ώστε να είναι εφικτή η αυθεντικοποίηση χρήστη που εισάγει το σωστό συνθηματικό – καλή πρακτική αποτελεί η χρήση μίας **κρυπτογραφικής συνάρτησης κατακερματισμού** (cryptographic hash function). Πρόκειται για μία ειδικού τύπου κρυπτογραφική λειτουργία η οποία, με απλά λόγια, έχει τις ακόλουθες ιδιότητες:[88]

i) Μετασχηματίζει ένα μήνυμα εισόδου σε ένα ακατάληπτο μήνυμα στην έξοδο (στην περίπτωσή μας, το συνθηματικό μετατρέπεται σε κάτι ακατάληπτο), η οποία έξοδος είναι μη αντιστρεπτή: γνώση του μηνύματος εξόδου (το οποίο ονομάζεται «αποτύπωμα» του αρχικού μηνύματος) δεν επιτρέπει τον υπολογισμό του μηνύματος εισόδου. Απόρροια αυτής της ιδιότητας είναι ότι έστω και μικρές αλλαγές σε ένα μήνυμα επιφέρουν μεγάλες αλλαγές στο αποτύπωμά του.

ii) Είναι πρακτικά αδύνατον να υπάρξουν δύο διαφορετικές είσοδοι οι οποίες να έχουν το ίδιο αποτύπωμα.

[88] Οι ιδιότητες παρουσιάζονται εδώ με απλά λόγια και δεν είναι αυστηρά μαθηματικά διατυπωμένες ούτε πλήρεις, αφού κάτι τέτοιο θα εξέφευγε του αντικειμένου του παρόντος.



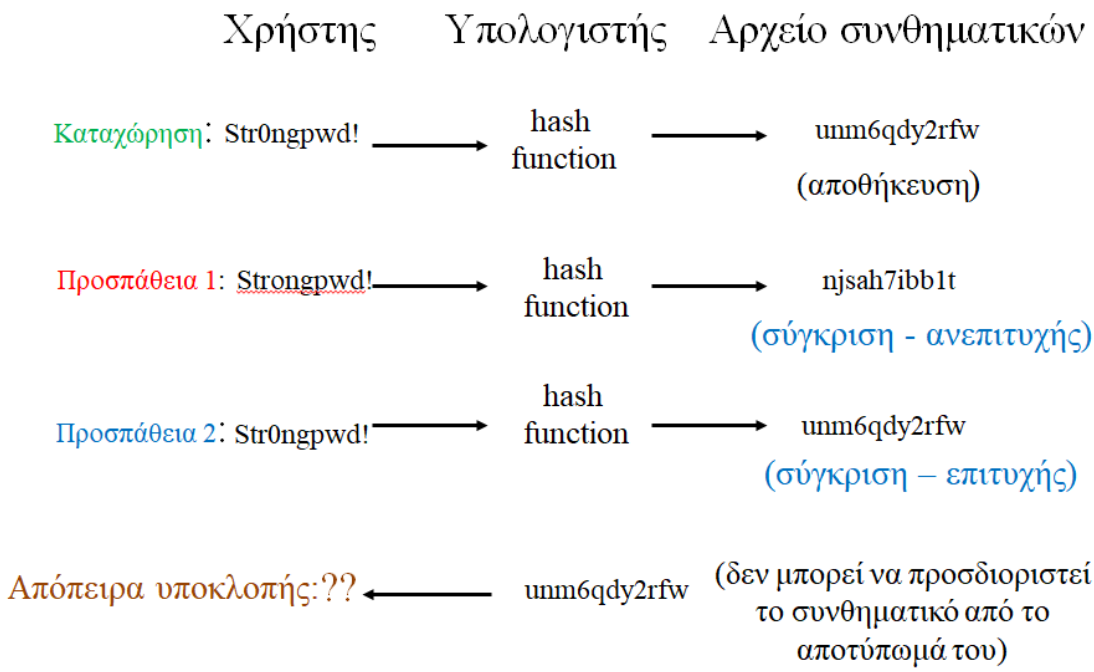
Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Η διαδικασία αυτή αποτυπώνεται στην Εικόνα 13 η οποία καταδεικνύει το σενάριο όπου ένας χρήστης, μόλις εγγράφεται σε ένα πληροφοριακό σύστημα και καλείται να επιλέξει συνθηματικό προκειμένου αυτό να καταχωρηθεί, επιλέγει τη λέξη «Str0ngpwd!». Η λέξη αυτή δεν θα αποθηκευτεί σε κανένα αρχείο του συστήματος: αντ' αυτής, το σύστημα θα υπολογίσει το αποτύπωμα της λέξης για συγκεκριμένη συνάρτηση κατακερματισμού – το οποίο αποτύπωμα, στην εν λόγω περίπτωση, είναι η λέξη «unm6qdy2rfw» - και αποθηκεύει αυτό.

Εάν ο χρήστης συνδεθεί αργότερα και πληκτρολογήσει κατά την αυθεντικοποίησή του, π.χ., έναν χαρακτήρα λανθασμένα εκ παραδρομής, το σύστημα θα υπολογίσει το αποτύπωμα της λέξης που πληκτρολόγησε ο χρήστης και θα το συγκρίνει με αυτό που έχει ήδη αποθηκευμένο για αυτόν το χρήστη (βλ. την Προσπάθεια 1 στην Εικόνα 13): έστω και ένας μόνο χαρακτήρας να είναι λάθος, το αποτύπωμα θα είναι διαφορετικό (και μάλιστα, θα είναι και κατά πολύ διαφορετικό), οπότε και ο χρήστης δεν θα αυθεντικοποιηθεί και δεν θα του επιτραπεί η πρόσβαση. Φυσικά, εάν ο χρήστης εισάγει το σωστό συνθηματικό (βλ. την Προσπάθεια 2 στην Εικόνα 13), τότε το σύστημα θα είναι σε θέση, με αντίστοιχη σύγκριση, να αυθεντικοποιήσει το χρήστη (δηλαδή να υπάρξει βεβαιότητα ότι ο χρήστης εισήγαγε το σωστό συνθηματικό και να του επιτρέψει πρόσβαση) παρόλο που το ίδιο το σύστημα δεν «γνωρίζει» το αρχικό συνθηματικό αφού δεν το τηρεί. Τέλος, λόγω της μη αντιστρεψιμότητας της συνάρτησης κατακερματισμού, δεν μπορεί κάποιος που θα αποκτήσει πρόσβαση στο αρχείο στο οποίο τηρούνται τα «αποτυπώματα» των συνθηματικών να τα αναστρέψει και να μάθει τα συνθηματικά των χρηστών.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης




**Εικόνα 13 - Χρήση κρυπτογραφικής συνάρτησης κατακερματισμού για αποθήκευση συνθηματικών**

**Ερώτηση δραστηριότητας**: Πολίτης εγγράφεται στις ηλεκτρονικές υπηρεσίες δημόσιου φορέα και επιλέγει όνομα χρήστη (login name) και συνθηματικό (password), εισάγοντας και λοιπά στοιχεία που χρειάζονται για την ταυτοποίησή του, όπως επίσης και μία ηλεκτρονική διεύθυνση. Μετά από ημέρες δεν θυμάται το συνθηματικό που είχε επιλέξει και ζητάει, μέσω της κατάλληλης επιλογής, ανάκτηση του συνθηματικού. Ακολούθως, λαμβάνει μήνυμα στην ηλεκτρονική του διεύθυνση το οποίο περιέχει το συνθηματικό που είχε επιλέξει. Σχολιάστε τη διαχείριση συνθηματικών του φορέα, με βάση τα ανωτέρω (είναι ασφαλής ή όχι και γιατί).

Αν και η κρυπτογραφική συνάρτηση κατακερματισμού έχει όπως είδαμε πολλές επιθυμητές ιδιότητες για την προστασία των συνθηματικών, δεν είναι κατά κανόνα αρκετή: αν ένας εισβολέας καταφέρει να «υποκλέψει» το αρχείο αυτό, τότε μπορεί να προσπαθήσει να «μαντέψει» συνθηματικά για διάφορους χρήστες και, για κάθε τέτοια «πρόβλεψη» που θα κάνει, να υπολογίζει το αποτύπωμα και να ελέγξει αν ταυτίζεται με το αποτύπωμα που αναγράφεται στο αρχείο. Εάν βρει ταύτιση, έχει ουσιαστικά



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

βρει («μαντέψει») το συνθηματικό. Άρα, ναι μεν δεν υπάρχει δυνατότητα αντιστροφής της κρυπτογραφικής συνάρτησης κατακερματισμού, αλλά υπάρχει η δυνατότητα «μαντέματος» και ελέγχου αν το μάντεμα είναι σωστό. Συνεπώς, αν κάποιος χρήστης έχει επιλέξει συνθηματικό που μπορεί να προβλεφθεί, η τήρηση των συνθηματικών σε μορφή αποτυπωμάτων δεν είναι αρκούντως αποτελεσματική. Προσοχή: η «πρόβλεψη» συνθηματικού μπορεί να είναι πολύ πιο εύκολη από ό,τι νομίζουμε διότι υπάρχουν κατάλληλα εργαλεία λογισμικού που μπορούν με αυτόν τον τρόπο να βρουν συνθηματικά δοθέντων των αποτυπωμάτων τους, αξιοποιώντας – μεταξύ άλλων - πολύ μεγάλες λίστες λέξεων («λεξικά») με πιθανά συνθηματικά.

Για την αντιμετώπιση του ανωτέρου κινδύνου, θα πρέπει για τον υπολογισμό του αποτυπώματος ενός συνθηματικού να υπεισέρχεται και μία πρόσθετη τυχαία ποσότητα: αυτήν την ποσότητα (που είθισται να αποκαλείται «**salt**») δεν την ξέρει ούτε ο χρήστης, αφού παράγεται εξ αρχής από το ίδιο το σύστημα κατά την επιλογή του συνθηματικού που κάνει ο χρήστης. Το «salt» είναι διαφορετικό για κάθε χρήστη. Για παράδειγμα, επιστρέφοντας στο παράδειγμα της Εικόνα 13, αν ο χρήστης επιλέξει το συνθηματικό Str0ngpwd! , τότε το σύστημα θα δημιουργήσει μία τυχαία συμβολοσειρά ως «salt» - έστω, π.χ. f1ndDre7 – και ακολούθως θα υπολογίσει το αποτύπωμα της «επαυξημένης» συμβολοσειράς Str0ngpwd!f1ndDre7 (αντί για το αποτύπωμα του συνθηματικού Str0ngpwd!). Κάθε φορά που ο χρήστης θα επιχειρεί να αυθεντικοποιηθεί εισάγοντας το συνθηματικό του, τότε το σύστημα – που τηρεί το «salt» που αντιστοιχεί στον κάθε χρήστη – θα υπολογίζει το αποτύπωμα της συμβολοσειράς που προκύπτει από τη λέξη που εισήγαγε ο χρήστης «επαυξημένη» με το «salt» αυτού και ακολούθως θα κάνει τον έλεγχο αν το αποτέλεσμα ταυτίζεται με το αποτύπωμα το οποίο τηρεί για τον εν λόγω χρήστη.

Με αυτόν τον τρόπο επιτυγχάνονται τα εξής: i) ακόμα και αν δύο χρήστες επιλέξουν ίδια συνθηματικά, τα αντίστοιχα αποτυπώματά τους θα είναι διαφορετικά, ii) δυσκολεύει σημαντικά κάθε προσπάθεια κακόβουλου εισβολέα να «μαντέψει» συνθηματικό, δοθέντος ενός αποτυπώματος αυτού που προέκυψε κατά τον τρόπο που περιγράφηκε.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**Παράδειγμα:** Οργανισμός δέχεται κυβερνοεπίθεση και γίνεται διαρροή, προς άγνωστους τρίτους, των ηλεκτρονικών διευθύνσεων εγγεγραμμένων στις υπηρεσίες του χρηστών, καθώς και των αποτυπωμάτων των συνθηματικών τους που χρησιμοποιούν για την είσοδο στις διαδικτυακές υπηρεσίες.

Σενάριο 1: Αν για τα αποτυπώματα των συνθηματικών δεν έχει χρησιμοποιηθεί salt, τότε οι κίνδυνοι για τους χρήστες είναι υψηλοί[89] και θα πρέπει να ενημερωθούν, σύμφωνα με το άρθρο 34 του ΓΚΠΔ.

Σενάριο 2: Αν για τα αποτυπώματα των συνθηματικών έχει χρησιμοποιηθεί salt το οποίο όμως διέρρευσε επίσης, τότε οι κίνδυνοι για τους χρήστες είναι υψηλοί και θα πρέπει να ενημερωθούν, σύμφωνα με το άρθρο 34 του ΓΚΠΔ.

Σενάριο 3: Αν για τα αποτυπώματα των συνθηματικών έχει χρησιμοποιηθεί salt το οποίο όμως δεν διέρρευσε, και εφόσον η συνάρτηση κατακερματισμού είναι ασφαλής και το «salt» μη προβλέψιμο, τότε οι κίνδυνοι για τους χρήστες δεν είναι υψηλοί και δεν προκύπτει, κατ' αρχάς, υποχρέωση να ενημερωθούν σύμφωνα με το άρθρο 34 του ΓΚΠΔ. Καλή πρακτική ωστόσο θα ήταν, για τον υπεύθυνο επεξεργασίας, να τους ενημερώσει ζητώντας τους να αλλάξουν το συνθηματικό τους, ιδίως αν χρησιμοποιούν το ίδιο και σε άλλες διαδικτυακές υπηρεσίες/εφαρμογής (είναι προς την ασφάλειά τους να ενημερωθούν να το αλλάξουν από όπου το χρησιμοποιούν).

☞ Σε πολλούς υπάρχει σύγχυση ως προς το ότι μία κρυπτογραφική συνάρτηση κατακερματισμού (cryptographic hash function) ταυτίζεται με έναν αλγόριθμο κρυπτογράφησης (βλ. Ενότητα 10). Οι δύο έννοιες δεν ταυτίζονται: ένας

[89] Ακόμα και αν ο οργανισμός εφαρμόζει πολιτικές για ισχυρά συνθηματικά, δεν μπορεί να αποκλειστεί το ενδεχόμενο κάποιος χρήστης να έχει επιλέξει ένα που να είναι μεν σύμφωνο με τις πολιτικές αλλά, τελικά, να μπορεί να προβλεφθεί. Π.χ. το συνθηματικό «Passw0rd!» έχει περισσότερους από 8 χαρακτήρες, τόσο κεφαλαίους όσο και πεζούς, ενώ επίσης έχει και αριθμούς και σημεία στίξης: παρόλα αυτά, είναι εξαιρετικά προβλέψιμο (υπάρχει σε όλα τα «λεξικά» μαντέματος συνθηματικών).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κρυπτογραφικός αλγόριθμος είναι ευθέως και ευχερώς αντιστρεπτός για όποιον γνωρίζει το κλειδί αποκρυπτογράφησης. Από την άλλη πλευρά, οι συναρτήσεις κατακερματισμού δεν είναι αντιστρεπτές (είτε με την κλασική τους χρήση όπου δεν υπεισέρχεται κλειδί, είτε αν υπεισέρχεται κλειδί ή «salt»). Οι δύο έννοιες εξυπηρετούν διαφορετικές απαιτήσεις ασφαλείας.

**Αυθεντικοποίηση πολιτών σε υπηρεσίες ηλεκτρονικής διακυβέρνησης**

Για τις διαδικασίες εγγραφής και αυθεντικοποίησης χρηστών σε υπηρεσίες ηλεκτρονικής διακυβέρνησης, πρέπει να λαμβάνεται υπόψη και το Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (ΥΑΠ Φ.40.4/1/989, ΦΕΚ 1301/Β/2012). Το εν λόγω Πλαίσιο κατηγοριοποιεί σε επίπεδα εμπιστοσύνης τις υπηρεσίες ηλεκτρονικής διακυβέρνησης με βάση την αλληλεπίδρασή τους με τους πολίτες: το χαμηλότερο επίπεδο αφορά υπηρεσίες που είναι απλά ενημερωτικού χαρακτήρα (π.χ. ο πολίτης μπορεί να «κατεβάσει» νόμους, εγκυκλίους, αλλά όχι να υποβάλει ηλεκτρονικά κάποιο αίτημα), οπότε και δεν απαιτείται καμία ταυτοποίησή του, και το υψηλότερο αφορά περιπτώσεις όπου η διεκπεραίωση αιτήματος πολίτη ολοκληρώνεται πλήρως ηλεκτρονικά και αφορά είτε ευαίσθητα δεδομένα είτε ηλεκτρονικές πληρωμές, οπότε και απαιτείται το μέγιστο επίπεδο εμπιστοσύνης. Αναλόγως του επιπέδου εμπιστοσύνης, καθορίζεται τόσο η διαδικασία εγγραφής του χρήστη στις ηλεκτρονικές υπηρεσίες (π.χ. εάν για την εγγραφή απαιτείται, για την ταυτοποίηση του πολίτη, φυσική του παρουσία ή όχι) όσο και ο μηχανισμός αυθεντικοποίησης.

☞ Εάν δημόσιος οργανισμός, για να αυθεντικοποιεί τους πολίτες σε υπηρεσίες ηλεκτρονικής διακυβέρνησης που παρέχει, αξιοποιεί την υπηρεσία αυθεντικοποίησης του TAXISNET, τότε ουσιαστικά αξιοποιεί μηχανισμό που αντιστοιχεί στο μέγιστο επίπεδο εμπιστοσύνης σύμφωνα με το Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, αφού για να λάβει κάποιος διαπιστευτήρια του TAXISNET απαιτείται πρώτα να ταυτοποιηθεί με



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

φυσική του παρουσία.

### 15.2.2.2 Αρχεία καταγραφής

Για την αποτελεσματική διερεύνηση και αντιμετώπιση ενός περιστατικού παραβίασης της ασφάλειας των δεδομένων, είναι πολύ συχνά απαραίτητο να μελετηθούν ενέργειες χρηστών – είτε εσωτερικών είτε εξωτερικών – οι οποίοι επενέργησαν με τα πληροφοριακά συστήματα ενός οργανισμού: για παράδειγμα, αν ένας κακόβουλος εξωτερικός εισβολέας κατάφερε να παρεισφρύσει στα συστήματα, θα πρέπει να διερευνηθεί ο τρόπος με τον οποίο το κατόρθωσε. Προς τούτο, κατάλληλα αρχεία καταγραφής ενεργειών (log files) πρέπει να τηρούνται, ακριβώς για να επιτρέπουν τη διερεύνηση περιστατικών.

Η τήρηση τέτοιων αρχείων ως μέτρο ασφάλειας αναμένεται, μεταξύ άλλων, να περιλαμβάνει ενέργειες όπως καταγραφή επιτυχημένων και αποτυχημένων προσπαθειών σύνδεσης των χρηστών, τόσο σε επίπεδο λειτουργικού συστήματος όσο και σε επίπεδο (web) εφαρμογών.

| IP Address | Date | Request | Sta... | Size | Country |
|---|---|---|---|---|---|
| 10.30.33.10 | 22/4/2010 9:42:26 πμ | GET /index.php?action=admin;area=manage... | 200 | 10849 | N/A |
| 10.30.33.10 | 22/4/2010 9:42:29 πμ | GET /index.php?action=admin;area=manage... | 200 | 10813 | N/A |
| 10.30.33.26 | 22/4/2010 9:42:44 πμ | POST /index.php?action=admin;area=mana... | 302 | 455 | N/A |
| 10.30.33.26 | 22/4/2010 9:42:44 πμ | GET /index.php?action=admin;area=manage... | 200 | 10852 | N/A |
| 10.30.33.26 | 22/4/2010 9:42:45 πμ | GET /index.php?type=rss;action=.xml HTTP/1.1 | 200 | 1255 | N/A |
| 10.30.33.26 | 22/4/2010 9:42:48 πμ | GET /favicon.ico HTTP/1.1 | 404 | 505 | N/A |
| 10.30.33.26 | 22/4/2010 9:42:59 πμ | POST /index.php?action=admin;area=mana... | 200 | 10804 | N/A |
| 10.30.33.26 | 22/4/2010 9:43:00 πμ | GET /index.php?type=rss;action=.xml HTTP/1.1 | 200 | 1255 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:00 πμ | POST /index.php?action=admin;area=mana... | 302 | 455 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:00 πμ | GET /index.php?action=admin;area=manage... | 200 | 10891 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:06 πμ | GET /index.php?action=admin;area=manage... | 200 | 10882 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:13 πμ | POST /index.php?action=admin;area=mana... | 302 | 454 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:13 πμ | GET /index.php?action=admin;area=manage... | 200 | 10862 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:17 πμ | GET /index.php?action=admin;area=manage... | 200 | 10817 | N/A |
| 10.30.33.26 | 22/4/2010 9:43:35 πμ | POST /index.php?action=admin;area=mana... | 302 | 455 | N/A |
| 10.30.33.26 | 22/4/2010 9:43:35 πμ | GET /index.php?action=admin;area=manage... | 200 | 10860 | N/A |
| 10.30.33.26 | 22/4/2010 9:43:37 πμ | GET /index.php?type=rss;action=.xml HTTP/1.1 | 200 | 1255 | N/A |
| 10.30.33.26 | 22/4/2010 9:43:37 πμ | GET /favicon.ico HTTP/1.1 | 404 | 505 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:46 πμ | POST /index.php?action=admin;area=mana... | 302 | 455 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:46 πμ | GET /index.php?action=admin;area=manage... | 200 | 10886 | N/A |
| 10.30.33.10 | 22/4/2010 9:43:49 πμ | GET /index.php?action=admin;area=manage... | 200 | 10833 | N/A |

**Εικόνα 14 - Αρχείο καταγραφής προσβάσεων σε εξυπηρετητή ιστού (web server)**

**Παράδειγμα:** Δημόσιος οργανισμός διατηρεί ιστοσελίδα, η οποία υποστηρίζεται από έναν εξυπηρετητή ιστού (web server). Επειδή κάθε ιστοσελίδα μπορεί ανά πάσα στιγμή να γίνει στόχος διαδικτυακών επιθέσεων, θα πρέπει – για σκοπούς ασφάλειας – να τηρούνται αρχεία καταγραφής των προσβάσεων σε αυτή (σχετικό ενδεικτικό



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

δείγμα απεικονίζεται στην Εικόνα 14). Πρόκειται στην ουσία για μία επεξεργασία δεδομένων προσωπικού χαρακτήρα, αφού οι διευθύνσεις διαδικτύου (IP διευθύνσεις) των επισκεπτών της ιστοσελίδας λογίζονται ως προσωπικά δεδομένα. Συνεπώς, για αυτήν την επεξεργασία πρέπει, μεταξύ άλλων, να παρέχεται ενημέρωση προς τα υποκείμενα των δεδομένων (επισκέπτες της ιστοσελίδας), όπως επίσης και να περιγράφεται στο αρχείο δραστηριοτήτων του οργανισμού (βλ. Ενότητα 8).

Παρά τη σπουδαιότητά τους, τα αρχεία καταγραφής ενδέχεται να εγείρουν και ζητήματα προστασίας προσωπικών δεδομένων, εάν γίνει χρήση τους για άλλο σκοπό – π.χ. εάν χρησιμοποιηθούν για επιτήρηση της διαδικτυακής συμπεριφοράς των εργαζομένων. Ακριβώς για αυτό το λόγο, ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει μέριμνα στο να διασφαλίζει τη θεμιτή επεξεργασία τους. Κρίσιμο, μεταξύ άλλων, είναι να καταγράφονται και οι ενέργειες των διαχειριστών των συστημάτων, όπως επίσης και να διασφαλίζεται η ακεραιότητα των αρχείων καταγραφής. Μία χρήσιμη πηγή είναι η [93].

#### 15.2.2.3 Αντίγραφα ασφαλείας

Βασικό μέτρο για τη διασφάλιση της διαθεσιμότητας των δεδομένων, ακόμα και αν επέλθει περιστατικό παραβίασής της, είναι η ύπαρξη αντιγράφων ασφαλείας (backup) για τα αρχεία με τα προσωπικά δεδομένα. Για παράδειγμα, αν ανακαλέσουμε τη διαχείριση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα που συζητήσαμε στην Ενότητα 10, σε περίπτωση, π.χ., που οργανισμός πληγεί από κακόβουλο λογισμικό τύπου ransomware και καταστούν τα αρχεία του μη διαθέσιμα, οι κίνδυνοι που απορρέουν δεν είναι υψηλοί εφόσον για τα αρχεία αυτά υπάρχουν αντίγραφα ασφαλείας και η ανάκτησή τους είναι ευχερής.

Ειδικότερα, ο οργανισμός πρέπει να ακολουθεί συγκεκριμένη διαδικασία (πολιτική) λήψης αντιγράφων ασφαλείας, η οποία θα καθορίζει, μεταξύ άλλων, τι ακριβώς θα περιέχει το κάθε αντίγραφο ασφαλείας, κάθε πότε θα δημιουργούνται, σε ποιο χώρο θα τηρούνται και με ποιον τρόπο, καθώς επίσης και μέτρα για την ασφαλή αποθήκευσή τους. Ο οργανισμός πρέπει να διασφαλίζει την ορθή δημιουργία



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

αντιγράφων ασφαλείας (π.χ. με περιοδικό έλεγχο ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται).

#### 15.2.2.4 Διαμόρφωση περιβάλλοντος υπολογιστών

Στα τεχνικά μέτρα ασφάλειας που μπορεί να λάβει ένας οργανισμός εντάσσονται και οι ρυθμίσεις, ως προς θέματα ασφάλειας, των υπολογιστικών συστημάτων – ή, αλλιώς, η διαμόρφωση (configuration) του περιβάλλοντος. Τέτοιες ρυθμίσεις μπορεί μεταξύ άλλων να περιλαμβάνουν, ανά περίπτωση και με βάση την αξιολόγηση των σχετικών κινδύνων, τα εξής:

1) Εγκατάσταση «αντιϊκού» προγράμματος, που θα ενημερώνεται τακτικά και αυτόματα.
2) Αυτόματες – ή ενεργοποιημένες από τους διαχειριστές συστημάτων – ενημερώσεις ασφαλείας (updates) όλων των λογισμικών (συμπεριλαμβανομένων των ενημερώσεων του λειτουργικού συστήματος)
3) «Κλείδωμα» στους απλούς χρήστες της δυνατότητάς τους να εγκαθιστούν οι ίδιοι δικές τους εφαρμογές στους σταθμούς εργασίας τους
4) «Κλείδωμα» της δυνατότητας εξαγωγής ή εισαγωγής αρχείων με αποσπώμενα μέσα (π.χ. usb stick)
5) Κρυπτογράφηση των «σκληρών» δίσκων – είτε σε σταθερούς σταθμούς εργασίας είτε σε φορητούς υπολογιστές (laptop).

#### 15.2.2.5 Ασφάλεια επικοινωνιών

Λαμβάνοντας υπόψη ότι οι μεταφορές κάθε είδους δεδομένων γίνονται, κατά κανόνα, μέσω δικτύων – και ιδίως μέσω Internet – καθίσταται σαφές ότι η ασφάλεια των επικοινωνιών είναι ύψιστης σημασίας. Όταν ο οργανισμός καλείται να εξετάσει και να λάβει μέτρα για την ασφάλεια των επικοινωνιών, πρέπει να εξετάσει όλων των ειδών τις επικοινωνίες, όπως επικοινωνίες μέσω ηλεκτρονικού ταχυδρομείου, εσωτερικά δίκτυα, «αποκομμένα» από το Internet, εντός του οργανισμού που μπορούν να χρησιμοποιούν οι εργαζόμενοι για ανταλλαγές αρχείων/δεδομένων,



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

συνδέσεις στο Διαδίκτυο/Internet (τόσο των εργαζομένων όσο όμως και πολιτών που συνδέονται σε διαδικτυακή πύλη του οργανισμού για υπηρεσίες ηλεκτρονικής διακυβέρνησης), αλλά και τυχόν ασύρματες επικοινωνίες. Μάλιστα, με την έλευση της τηλεργασίας, προστέθηκαν και νέες προκλήσεις ως προς την ασφάλεια των επικοινωνιών, αφού πρέπει να ληφθεί μέριμνα για την ασφαλή σύνδεση ενός εργαζομένου που βρίσκεται στον προσωπικό του χώρο με τα πληροφοριακά συστήματα και δίκτυα του οργανισμού.

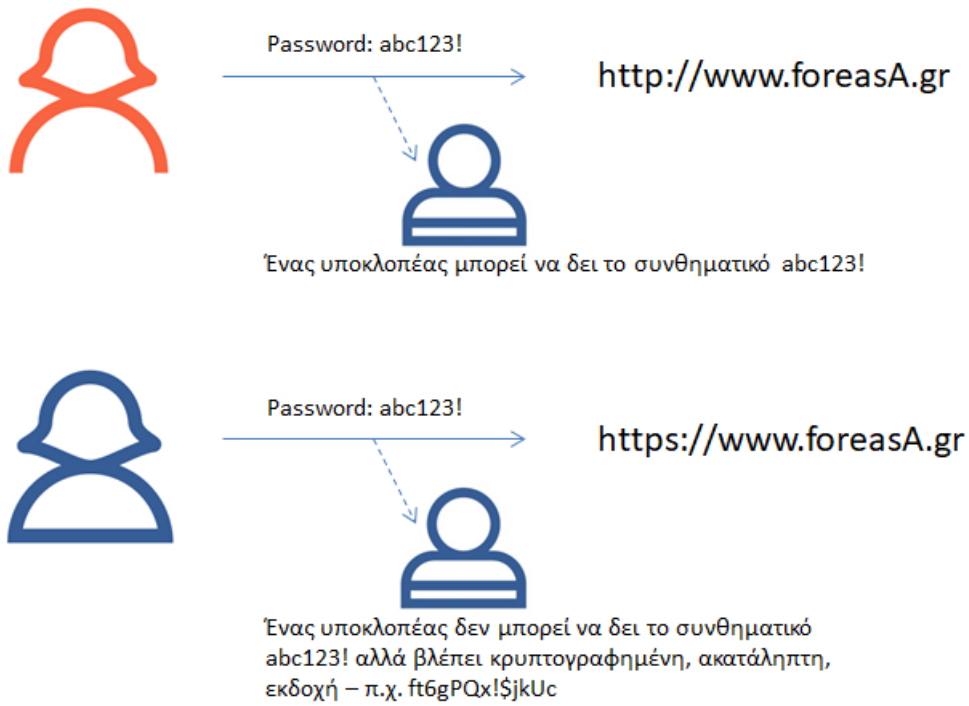
Υπάρχουν τεχνολογικές λύσεις που μπορούν να χρησιμοποιηθούν για την ασφάλεια των επικοινωνιών, στις οποίες συγκαταλέγονται τεχνικές ελέγχου πρόσβασης (π.χ. μόνο εξουσιοδοτημένοι χρήστες θα πρέπει να μπορούν να εισέλθουν στο εσωτερικό δίκτυο ενός οργανισμού), κατάλληλος διαχωρισμός δικτύων (π.χ. τμήμα δικτύου του οργανισμού δεν θα πρέπει να είναι διασυνδεδεμένο με το Internet ή με άλλο τμήμα δικτύου του οργανισμού που εξυπηρετεί άλλους σκοπούς) και βεβαίως κρυπτογράφηση των μεταδιδόμενων δεδομένων - π.χ. μέσω εικονικού ιδιωτικού δικτύου (Virtual Private Network - VPN). Αν και εδώ οι τελικές λύσεις θα επιλεγούν, από τον κάθε οργανισμό, στο πλαίσιο διαχείρισης και αποτίμησης κινδύνων, κάποιες επιλογές προκύπτουν ότι είναι «εκ των ουκ άνευ»: για παράδειγμα, κάθε απομακρυσμένη σύνδεση, από τοποθεσία εκτός του οργανισμού, σε πληροφοριακό σύστημα εντός του οργανισμού πρέπει να είναι κρυπτογραφημένη. Στο πλαίσιο αυτό, κάθε υπηρεσία ηλεκτρονικής διακυβέρνησης που παρέχεται προς το κοινό πρέπει να διασφαλίζει, κατ' ελάχιστον, την κρυπτογράφηση των δεδομένων που εισάγουν οι χρήστες (εφόσον η υπηρεσία απαιτεί από τους χρήστες να εισάγουν προσωπικά τους δεδομένα και δεν είναι απλά μία υπηρεσία αμιγώς πληροφοριακού χαρακτήρα).

**Παράδειγμα:** Δημόσιος οργανισμός διατηρεί ιστοσελίδα, η οποία υποστηρίζεται από έναν εξυπηρετητή ιστού (web server). Χρήστες μπορούν, μέσω πλοήγησής τους στην ιστοσελίδα, να ενημερωθούν για σχετικούς νόμους/εγκυκλίους, να εισάγουν – εάν το επιθυμούν - την ηλεκτρονική τους διεύθυνση για να λαμβάνουν ενημερωτικά δελτία (newsletters), αλλά και αν θέλουν να δημιουργήσουν ηλεκτρονικό λογαριασμό μέσω του οποίου θα υποβάλουν αιτήσεις.



Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Εφόσον η ιστοσελίδα διατίθεται σε όλους τους πολίτες ανεξαιρέτως, δεν μπορούν να υπάρξουν κατ' αρχάς μέτρα ασφάλειας που να περιορίζουν την πρόσβαση σε αυτή[90]. Όμως, η ιστοσελίδα, από τη στιγμή που οι πολίτες μπορούν να επενεργήσουν με αυτή εισάγοντας προσωπικά τους δεδομένα, θα πρέπει οπωσδήποτε να υλοποιεί διαδικτυακό πρωτόκολλο ασφαλείας. Στη συγκεκριμένη περίπτωση, το πλέον ενδεδειγμένο πρωτόκολλο είναι το TLS (Transport Layer Security), το οποίο μετατρέπει το πρωτόκολλο http σε https: με αυτόν τον τρόπο, κάθε πληροφορία που αποστέλλουν ή λαμβάνουν οι χρήστες είναι κρυπτογραφημένη (βλ. και Εικόνα 15), κάθε αλλοίωση της μεταδιδόμενης πληροφορίας θα γίνεται αντιληπτή, ενώ επίσης οι πολίτες μπορούν να είναι σίγουροι ότι έχουν συνδεθεί στη σωστή ιστοσελίδα και όχι σε κάποια κακόβουλη η οποία «υποδύεται» την αυθεντική.




**Εικόνα 15 - Η διαφορά μεταξύ http και https από πλευράς κρυπτογράφησης**

[90] Διάφορη βέβαια είναι η περίπτωση όπου η ιστοσελίδα δέχεται διαδικτυακή επίθεση οπότε, προς αντιμετώπισή της, μπορεί είτε προσωρινά να «κατεβεί» ή να αποκοπεί η δυνατότητα σύνδεσης σε συγκεκριμένες διευθύνσεις Διαδικτύου (IP διευθύνσεις) από τις οποίες φαίνεται να ξεκινά η επίθεση (σύμφωνα με τα αρχεία καταγραφής).



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- Το πρωτόκολλο TLS έχει πολλές διαφορετικές εκδόσεις, ενώ η κάθε έκδοση επιτρέπει εξειδίκευση ρυθμίσεων (π.χ. συγκεκριμένους κρυπτογραφικούς αλγορίθμους). Κάποιες όμως εκ των εκδόσεων του TLS είναι γνωστό ότι έχουν κάποιες ευπάθειες. Κατά κανόνα δεν αρκεί για έναν φορέα να υλοποιήσει μία οποιαδήποτε έκδοση του TLS: ανακαλώντας ότι ο ΓΚΠΔ ρητά αναφέρει (βλ., π.χ., άρθρο 32) στο ότι οι πρόσφατες τεχνολογικές εξελίξεις (state-of-the-art) πρέπει να λαμβάνονται υπόψη, προκύπτει ότι ο οργανισμός πρέπει να προσέχει ιδιαίτερα ποια έκδοση του TLS θα χρησιμοποιείται (ιδανικά, η πιο πρόσφατη κάθε φορά), καθώς επίσης τις ρυθμίσεις με τις οποίες θα υλοποιηθεί.
- Γενικότερα, ανακαλώντας ότι τα μέτρα ασφάλειας πρέπει να αναθεωρούνται και να επικαιροποιούνται (βλ. άρθρο 32 του ΓΚΔΠ), προκύπτει – εμμέσως πλην σαφώς – ως υποχρέωση για έναν οργανισμό ο διαρκής έλεγχος ενός εξυπηρετητή Διαδικτύου (web server) ως προς τυχόν ευπάθειές του. Προς τούτο, μπορούν να αξιοποιούνται, σε συστηματική βάση, γνωστά και έγκυρα εργαλεία ανίχνευσης ευπαθειών (vulnerability assessment tools).

**Προστασία δεδομένων κατά την τηλεργασία**

Η Αρχή εξέδωσε τις Κατευθυντήριες Γραμμές 2/2020 [94] αναφορικά με τη λήψη μέτρων ασφάλειας στο πλαίσιο της τηλεργασίας. Στις εν λόγω Κατευθυντήριες Γραμμές, παρέχονται μεταξύ άλλων κατευθύνσεις και για το ζήτημα της πρόσβασης στο δίκτυο, οι οποίες αναφέρουν, μεταξύ άλλων, τα εξής:

*« 1. Διασφάλιση ότι δεν υπάρχει δυνατότητα μη ασφαλούς απομακρυσμένης πρόσβασης σε πόρους των πληροφοριακών συστημάτων του φορέα, όπως υπολογιστές εσωτερικού δικτύου και εσωτερικά αρχεία. Η ασφαλής σύνδεση μπορεί, ενδεικτικώς, να επιτευχθεί μέσω εικονικού ιδιωτικού δικτύου στο οποίο πραγματοποιείται κρυπτογράφηση των δεδομένων και αυθεντικοποίηση των χρηστών (π.χ. IPSec VPN).*

*i. Καθορισμός και περιορισμός των πόρων στους οποίους επιτρέπεται η απομακρυσμένη πρόσβαση στο απολύτως απαραίτητο, ανάλογα με τα καθήκοντα που*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*επιτελεί ο τηλεργαζόμενος.*

*ii. Σύνδεση σε υπολογιστικά συστήματα του φορέα μέσω υπηρεσίας "απομακρυσμένης επιφάνειας εργασίας" ("Remote Desktop Protocol - RDP"), μόνο εφόσον αυτή γίνεται μέσω ασφαλούς εικονικού ιδιωτικού δικτύου (VPN).*

*2. Χρήση ασφαλούς πρωτοκόλλου WPA2 με ισχυρό κωδικό, όταν η σύνδεση της συσκευής του τηλεργαζόμενου στο Διαδίκτυο γίνεται μέσω ασύρματου δικτύου (Wi-Fi). Τούτο ισχύει ακόμα καιόταν μετά τη σύνδεση στο Διαδίκτυο, γίνεται ασφαλής σύνδεση στο δίκτυο του φορέα π.χ. με χρήση VPN.*

*3. Αποφυγή αποθήκευσης αρχείων με προσωπικά δεδομένα σε υπηρεσίες διαδικτυακής αποθήκευσης (π.χ. Dropbox, One Drive, google drive), εκτός και αν υπάρχουν τα κατάλληλα εχέγγυα, όπως π.χ. να πρόκειται για υπηρεσία που παρέχεται, με κατάλληλα μέτρα ασφάλειας, από τον φορέα ή τα δεδομένα να αποθηκεύονται αποκλειστικά σε κατάλληλα κρυπτογραφημένη μορφή».*

Στις ίδιες κατευθυντήριες γραμμές καλύπτεται και το ζήτημα χρήσης εφαρμογών για ηλεκτρονικό ταχυδρομείο (e-mail) και ανταλλαγής μηνυμάτων (instant messaging).

## 15.3 Προηγμένα ζητήματα – Κρυπτογραφία, ψευδωνυμοποίηση και ανωνυμοποίηση

Ολοκληρώνοντας την παρούσα ενότητα, θα γίνει μία σύντομη επισκόπηση σε κάποια προηγμένα ζητήματα που σχετίζονται με κρυπτογράφηση, ψευδωνυμοποίηση (για τα οποία έγινε ήδη μία εισαγωγή στην Ενότητα 10) και ανωνυμοποίηση των δεδομένων (για την οποία δεν έχει γίνει ακόμα καμία συζήτηση στις προηγούμενες ενότητες). Τα εν λόγω θέματα θα μπορούσαν, λόγω του εύρους τους, να καλύψουν αποκλειστικά ύλη ενός ολόκληρου εκπαιδευτικού προγράμματος: στο παρόν θα επικεντρωθούμε, όπως προαναφέρθηκε, σε μία σύντομη συζήτηση επί βασικών σημείων/εννοιών, χωρίς μαθηματική αυστηρότητα.

**<u>Κρυπτογραφία: ευρύτερη της εμπιστευτικότητας των δεδομένων</u>**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Όπως προαναφέρθηκε (βλ. Ενότητα 10, αλλά και παραπάνω στην παρούσα Ενότητα), η κρυπτογραφία είναι ο κατ' εξοχήν μηχανισμός για την προάσπιση της εμπιστευτικότητας των δεδομένων (είτε τηρούνται σε κάποιο υπολογιστικό σύστημα είτε μεταδίδονται μέσω δικτύου). Πέραν όμως της εμπιστευτικότητας, η κρυπτογραφία μπορεί να διασφαλίσει τα εξής:

i) Την ακεραιότητα των δεδομένων. Για παράδειγμα, στο πρωτόκολλο TLS που αναφέρθηκε νωρίτερα, αν ένας κακόβολος επίδοξος υποκλοπέας «παραποιήσει» το μεταδιδόμενο κρυπτογραφημένο μήνυμα, αυτή η τροποποίηση θα γίνει αντιληπτή στον παραλήπτη. Πρέπει να σημειωθεί ότι η αλλοίωση/παραποίηση ενός μηνύματος μπορεί να επιφέρει εξαιρετικά δυσμενείς συνέπειες. Ως ένα απλοϊκό, αλλά ρεαλιστικό παράδειγμα, ας αναλογιστούμε το εξής: Αν ο επιτιθέμενος γνωρίζει ότι ένα τμήμα του κρυπτογραφημένου μηνύματος αντιστοιχεί στο μήνυμα «IBAN ΛΟΓΑΡΙΑΣΜΟΣ ΤΟΥ Χ: GR3205555111112233445567», τότε, παρόλο που δεν γνωρίζει το μυστικό κλειδί, μπορεί να τροποποιήσει το κρυπτογραφημένο μήνυμα κατά τρόπο τέτοιο ώστε ο παραλήπτης να αποκρυπτογραφήσει και να διαβάσει άλλον έγκυρο IBAN λογαριασμό – αυτόν που επιθυμεί ο υποκλοπέας: μία τέτοια απειλή υφίσταται αν δεν ληφθεί μέριμνα, με κρυπτογραφικές τεχνικές, για τη διασφάλιση της ακεραιότητας του μεταδιδόμενου κρυπτογραφημένου μηνύματος[91].

ii) Την αυθεντικοποίηση του αποστολέα. Χαρακτηριστικό παράδειγμα – αν και όχι το μόνο – είναι η περίπτωση των ψηφιακών υπογραφών. Η ψηφιακή υπογραφή είναι ψηφιακή πληροφορία που προσαρτάται σε έναν ηλεκτρονικό μήνυμα η οποία επιτρέπει στον οποιονδήποτε τρίτο να επιβεβαιώσει ποιος είναι ο δημιουργός του αρχείου (κατ' αναλογία με την ιδιόχειρη υπογραφή, η οποία ομοίως πιστοποιεί την ταυτότητα του υπογράφοντα), καθώς επίσης και ότι το αρχείο δεν έχει αλλοιωθεί (κάθε αλλαγή του, αφότου υπογραφεί, θα είναι «ορατή»[92] αφού η υπογραφή δεν θα είναι πλέον έγκυρη).

[91] Ο συναφής όρος είναι αυθεντικοποιημένη κρυπτογράφηση (authenticated encryption).
[92] Δηλαδή, όποιος ελέγχει τη γνησιότητα του εγγράφου θα είναι σε θέση να αναγνωρίζει ότι η εκδοχή αυτή του εγγράφου δεν είναι η γνήσια που υπογράφηκε από το δημιουργό του



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Τόσο για την ακεραιότητα των δεδομένων, όσο και για την αυθεντικοποίηση αποστολέα, χρησιμοποιούνται κατάλληλες κρυπτογραφικές τεχνικές στις οποίες κατά κανόνα υπεισέρχονται κρυπτογραφικές συναρτήσεις κατακερματισμού, τις οποίες συζητήσαμε ήδη νωρίτερα σε άλλο πλαίσιο (στη διαχείριση συνθηματικών).

**Ερώτηση δραστηριότητας**: Όλα τα έγγραφα που αναρτώνται στη ΔΙΑΥΓΕΙΑ – είτε αφορούν φυσικά πρόσωπα και, ως εκ τούτου, περιέχουν προσωπικά τους δεδομένα είτε όχι - είναι ψηφιακά υπογεγραμμένα. Τι ζήτημα ασφάλειας, ως προς την προστασία προσωπικών δεδομένων, θα μπορούσε να δημιουργηθεί εάν έγγραφο που περιέχει προσωπικά δεδομένα αναρτηθεί στη ΔΙΑΥΓΕΙΑ χωρίς ψηφιακή υπογραφή;

Οι ανωτέρω στόχοι ασφάλειας για τους οποίους η κρυπτογραφία παρέχει λύσεις είναι μάλλον γνωστοί. Υπάρχουν όμως και άλλες περιπτώσεις όπου η κρυπτογραφία μπορεί να προσφέρει λύσεις από πλευράς προστασίας δεδομένων, διασφαλίζοντας τήρηση συγκεκριμένων αρχών όπως της ελαχιστοποίησης των δεδομένων: στις περιπτώσεις αυτές αναφερόμαστε στις λεγόμενες *προηγμένες κρυπτογραφικές τεχνικές (advanced encryption techniques):* για παράδειγμα, ίσως πολλοί δεν γνωρίζουν ότι υπάρχουν τεχνικές που εξασφαλίζουν ότι δύο υπεύθυνοι επεξεργασίας, όπου έκαστος τηρεί αρχείο προσωπικών δεδομένων, μπορούν να βρουν – εφόσον χρειάζεται – τις κοινές και μόνο εγγραφές των δύο αρχείων χωρίς να χρειάζεται να ανταλλάξουν τα πλήρη αρχεία (μία τέτοια ανταλλαγή θα προσέκρουε στη αρχή της ελαχιστοποίησης των δεδομένων). Μία περιγραφή όλων των προηγμένων κρυπτογραφικών τεχνικών, σε συνάρτηση με τις απαιτήσεις του ΓΚΠΔ για τις οποίες μπορούν να παρέχουν λύσεις, δίνεται στο [95].

**<u>Ψευδωνυμοποίηση (και η σχέση της με την κρυπτογράφηση)</u>**

Η ψευδωνυμοποίηση αποσκοπεί ιδίως στην απόκρυψη της «ταυτότητας» των προσώπων (βλ. Ενότητα 10). Ουσιαστικά, για να αναφερόμαστε σε ψευδωνυμοποιημένα δεδομένα, θα πρέπει κατ' ελάχιστον να μην εμφανίζεται στα δεδομένα κανένα αναγνωριστικό (identifier) προσώπου – ακόμα και αν το αναγνωριστικό μπορεί να επιφέρει αποκάλυψη της «ταυτότητας» ενός προσώπου



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

μόνο σε συγκεκριμένο πλαίσιο επεξεργασίας.

Για παράδειγμα, ένα αρχείο καταγραφής προσβάσεων σε έναν εξυπηρετητή ιστού (web server) όπως αυτό απεικονίζεται στην Εικόνα 14, το οποίο περιέχει διευθύνσεις δικτύου (IP διευθύνσεις), δεν είναι ψευδωνυμοποιημένο αρχείο, παρά το γεγονός ότι για έναν τρίτο, κατά κανόνα, δεν είναι (ευχερώς) εφικτό να ανακαλύψει το χρήστη που βρίσκεται «πίσω» από μία IP διεύθυνση: όμως η IP διεύθυνση αποτελεί αναγνωριστικό που, σε συγκεκριμένο πλαίσιο, μπορεί να επιτρέψει αναγνώριση (π.χ. οι τηλεπικοινωνιακοί πάροχοι σε συγκεκριμένες περιπτώσεις γνωρίζουν τους χρήστες στους οποίους έχουν ανατεθεί συγκεκριμένες IP διευθύνσεις, ενώ και ένας δημόσιος φορέας μπορεί να έχει σταθερές, μη μεταβαλλόμενες, IP διευθύνσεις στα υπολογιστικά του συστήματα, για τα οποία έχει κάνει αντιστοίχιση σε συγκεκριμένο εργαζόμενο). Άρα, σε μία τέτοια περίπτωση δεν πρόκειται για ψευδωνυμοποιημένα δεδομένα.

Όμως, στο ίδιο παράδειγμα, αν οι IP διευθύνσεις αντικατασταθούν με ειδικού τύπου «αναγνωριστικά» (τα οποία ονομάζονται *ψευδώνυμα*) που από μόνα τους δεν επιτρέπουν σε καμία περίπτωση αναγνώριση προσώπου (π.χ. αντικατάσταση κάθε IP διεύθυνσης σε ένα τέτοιο αρχείο με αύξοντες αριθμούς «1», «2», «3» κτλ., με βάση τη σειρά εμφάνισής τους) παρά μόνο αν κάποιος αποκτήσει πρόσβαση στον πίνακα αντιστοιχίσεων («10.30.33.10» -> «1», «10.30.33.26» -> «2» κ.ο.κ. – βλ. Εικόνα 14).

Τα ψευδωνυμοποιημένα δεδομένα λοιπόν, σύμφωνα και με τον ορισμό τους στο άρθρο 4 του ΓΚΠΔ (βλ. και Ενότητα 10), δεν μπορούν να αποδοθούν σε συγκεκριμένο ταυτοποιημένα ή ταυτοποιήσιμο πρόσωπο, εκτός αν αξιοποιηθούν πρόσθετες πληροφορίες που όμως προστατεύονται ειδικώς. Όμως, πρέπει να προσεχθεί το εξής:

α) Σύμφωνα με την αιτιολογική σκέψη 26 του ΓΚΠΔ, «*οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (...) Οι αρχές της προστασίας δεδομένων δεν θα πρέπει συνεπώς να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή*



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

*πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί.*» Από εδώ προκύπτει ότι τα ανώνυμα δεδομένα, για τα οποία θα αναφερθούμε στη συνέχεια, δεν αποτελούν δεδομένα προσωπικού χαρακτήρα και εκφεύγουν του πεδίου εφαρμογής του ΓΚΠΔ.

β) Όμως, η ίδια αιτιολογική σκέψη 26 αναφέρει επίσης το εξής: «*Τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο*». Άρα, <u>τα ψευδωνυμοποιημένα δεδομένα δεν θα πρέπει να θεωρούνται ανώνυμα δεδομένα και, άρα, είναι δεδομένα προσωπικού χαρακτήρα.</u> Συνεπώς, παρόλο που εκ της φύσης τους μειώνουν τους κινδύνους από την επεξεργασία, εξακολουθούν να αποτελούν προσωπικά δεδομένα και, άρα, ισχύουν όλες οι συναφείς υποχρεώσεις του υπευθύνου επεξεργασίας.

Παρόλο που τα ψευδωνυμοποιημένα δεδομένα είναι προσωπικά (και όχι ανώνυμα) δεδομένα, ο ΓΚΠΔ σαφώς προκρίνει τη χρήση της ψευδωνυμοποίησης. Όπως αναφέρει η αιτιολογική σκέψη 27 του ΓΚΠΔ, *η χρήση της ψευδωνυμοποίησης στα δεδομένα προσωπικού χαρακτήρα μπορεί να μειώσει τους κινδύνους για τα υποκείμενα των δεδομένων και να διευκολύνει τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να τηρήσουν τις οικείες υποχρεώσεις περί προστασίας των δεδομένων.* Πράγματι, η ψευδωνυμοποίηση αναφέρεται σε διάφορα σημεία εντός του ΓΚΠΔ. Συγκεκριμένα, αναφέρεται ως ένα πιθανό μέτρο που μπορεί να παρέχει τις κατάλληλες εγγυήσεις στις εξής περιπτώσεις:

- Επεξεργασία δεδομένων για άλλο σκοπό από αυτόν για τον οποίο έχουν αρχικώς συλλεγεί, η οποία δεν βασίζεται στη συγκατάθεση του προσώπου, προκειμένου να εξακριβωθεί κατά πόσον η επεξεργασία αυτή είναι συμβατή με τον αρχικό σκοπό (άρ. 6, παρ. 3 του ΓΚΠΔ).
- Διασφάλιση της προστασίας των δεδομένων ήδη από το σχεδιασμό (άρ. 25, παρ. 1 του ΓΚΠΔ).
- Ασφάλεια της επεξεργασίας (άρ. 32, παρ. 1 του ΓΚΠΔ).
- Επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή

σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς (άρ. 89, παρ. 1 του ΓΚΠΔ).

- Ενθάρρυνση για να λαμβάνεται υπόψη κατά την κατάρτιση κωδίκων δεοντολογίας (άρ. 40, παρ. του ΓΚΠΔ).

☞ Η ψευδωνυμοποίηση προκρίνεται και από το ΕΣΠΔ με τις συστάσεις 1/2020 [96] για την περίπτωση διαβιβάσεων σε τρίτες χώρες (βλ. και Ενότητα 5).

Η κρυπτογραφία μπορεί επίσης να αξιοποιηθεί για την επίτευξη καλής ψευδωνυμοποίησης. Για παράδειγμα, κρυπτογραφώντας τα αναγνωριστικά χρηστών (π.χ. ηλεκτρονικές διευθύνσεις, ΑΜΚΑ, ΑΦΜ, ονοματεπώνυμα κτλ.) προκύπτουν «ψευδώνυμα» από τα οποία δεν μπορεί κάποιος τρίτος να ανακτήσει τα αρχικά αναγνωριστικά εφόσον δεν έχει το κλειδί αποκρυπτογράφησης. Δεδομένου του πλήθους των κρυπτογραφικών αλγορίθμων και των διαφορετικών ιδιοτήτων τους, διάφορα είδη ψευδωνυμοποιήσεων μπορούν να υλοποιηθούν (π.χ. το ίδιο ψευδώνυμο πάντα για το ίδιο πρόσωπο ή διαφορετικό ψευδώνυμο ακόμα και για το ίδιο πρόσωπο αν εμφανίζεται πολλές φορές σε μία λίστα). Στην περίπτωση αυτή, θα μπορούσε να ειπωθεί ότι το μυστικό κλειδί αποκρυπτογράφησης αποτελεί συμπληρωματική πληροφορία που επιτρέπει την αντιστοίχιση των ψευδωνυμοποιημένων δεδομένων σε ταυτοποιημένα ή ταυτοποιήσιμα πρόσωπα και, άρα, πρέπει προφανώς να προστατεύεται και να τηρείται ξεχωριστά από τα ψευδωνυμοποιημένα δεδομένα.

**Παράδειγμα:** Δημόσιος οργανισμός που τηρεί οικονομικά στοιχεία πολιτών θέλει να δημιουργήσει ψευδωνυμοποιημένο αρχείο, τόσο για σκοπούς ασφάλειας αλλά και για σκοπούς ελαχιστοποίησης των δεδομένων σε περίπτωση που χρειαστεί να διαβιβάσει τα στοιχεία σε άλλο φορέα με τρόπο τέτοιο ώστε να μην αποκαλύπτονται τα στοιχεία ταυτοποίησης των πολιτών. Για το σκοπό αυτό, εφαρμόζει μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function) στους Αριθμούς Φορολογικού Μητρώου (ΑΦΜ) των πολιτών, παράγοντας ψευδώνυμα (βλ. Εικόνα 16). Θεωρεί ότι είναι μία καλή τεχνική ψευδωνυμοποίησης, επειδή μία κρυπτογραφική συνάρτηση



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κατακερματισμού είναι μη αναστρέψιμη και, ταυτόχρονα, με αυτή παράγεται πάντα το ίδιο ψευδώνυμο για το ίδιο πρόσωπο (ΑΦΜ), το οποίο επιτρέπει, π.χ., διεξαγωγή στατιστικής ανάλυσης (π.χ. για πόσους πολίτες τα αντίστοιχα οικονομικά δεδομένα αυξήθηκαν ή μειώθηκαν με το χρόνο κτλ.).

Ωστόσο, κάποιος τρίτος που θα λάβει γνώση του εν λόγω ψευδωνυμοποιημένου αρχείου – είτε πρόκειται για κακόβουλο χρήστη που θα το αποκτήσει παράνομα είτε για χρήστη που μπορεί να λάβει νομίμως το ψευδωνυμοποιημένο αρχείο αλλά δεν θα πρέπει να είναι σε θέση να αντιστοιχίσει τα ψευδωνυμοποιημένα δεδομένα σε ταυτοποιήσιμα πρόσωπα – θα μπορεί να υπολογίσει τους ΑΦΜ που αντιστοιχούν σε κάθε ψευδώνυμα. Συγκεκριμένα, όπως φαίνεται και στην Εικόνα 17, μπορεί κάποιος να υπολογίσει τα αποτυπώματα για δοθείσα λίστα πιθανών ΑΦΜ (ή, ακόμα χειρότερα, και για όλους τους πιθανούς ΑΦΜ[93]) και ακολούθως να ελέγξει αν τα αποτυπώματα που υπολόγισε βρίσκονται εντός της λίστας.

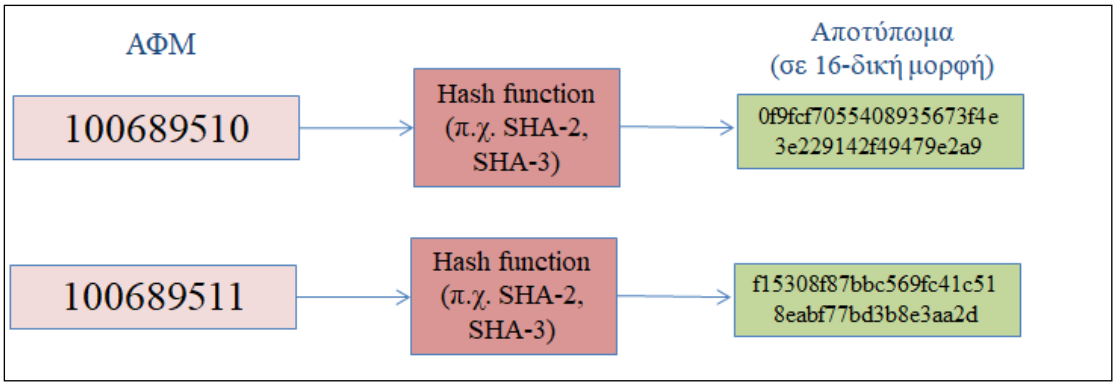
Άρα, μία κρυπτογραφική συνάρτηση κατακερματισμού πιθανότατα δεν αποτελεί μία καλή τεχνική ψευδωνυμοποίησης – και σίγουρα δεν αποτελεί καλή τεχνική σε περιπτώσεις όπως αυτή του παραδείγματος (και αυτό θα το καταδείκνυε και μία ΕΑΠΔ). Εάν επρόκειτο για περιστατικό παραβίασης του εν λόγω αρχείου, οι κίνδυνοι θα έπρεπε να αξιολογηθούν ως υψηλοί.

Εάν όμως, για τον υπολογισμό του αποτυπώματος (ψευδωνύμου) χρησιμοποιείται και ένα μυστικό κλειδί, που το γνωρίζει μόνο ο υπεύθυνος επεξεργασίας, τότε μία τέτοια δυνατότητα αντιστοίχισης ψευδωνύμων σε ταυτοποιήσιμα πρόσωπα δεν μπορεί να γίνει.

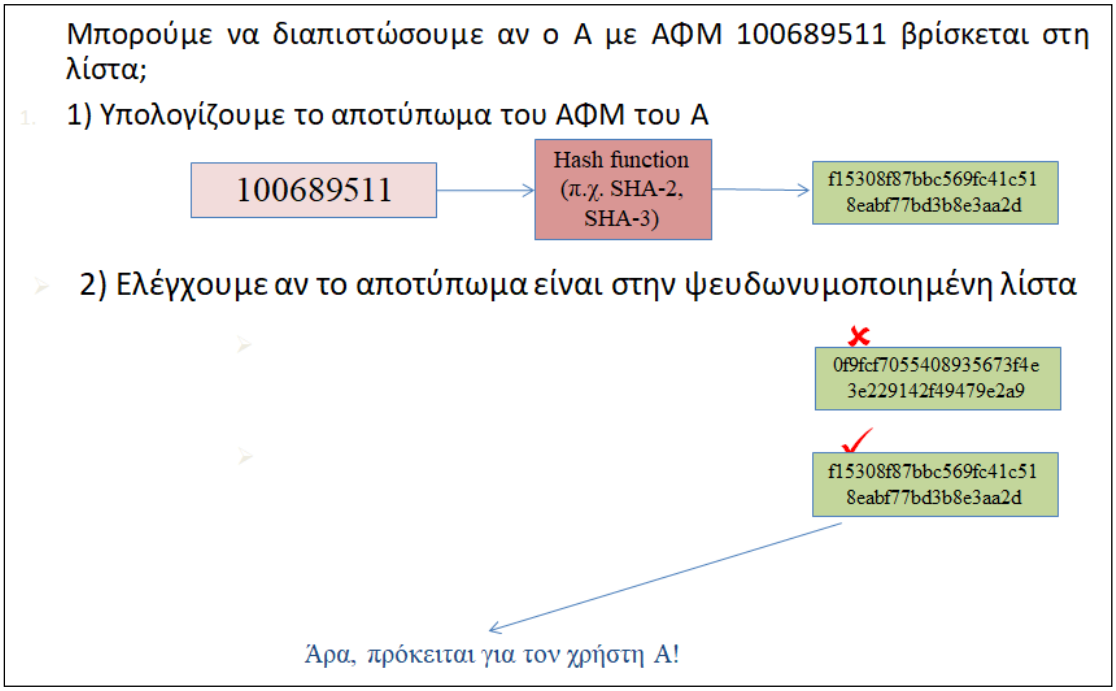
[93] Ένας τέτοιος υπολογισμός είναι υπολογιστικά εφικτός



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης




**Εικόνα 16 - Χρήση κρυπτογραφικής συνάρτησης κατακερματισμού (χωρίς κλειδί) για δημιουργία ψευδωνύμων**




**Εικόνα 17 - "Αναγνώριση" χρήστη Α εντός της ψευδωνυμοποιημένης λίστας, λόγω του ότι χρησιμοποιήθηκε συνάρτηση κατακερματισμού χωρίς κλειδί**

**Ερώτηση δραστηριότητας**: Το Υπουργείο Υγείας θέλει να συλλέγει, από όλες τις μονάδες του ΕΣΥ, δεδομένα ασθενών (φύλο, ηλικία, περιοχή, διάγνωση, θεραπεία, αποτέλεσμα κτλ.) για σκοπούς προστασίας και προαγωγής της δημόσιας υγείας, και αποτελεσματικότερης παρακολούθησης της λειτουργίας των μονάδων υγείας του



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΥ και της στελέχωσης και κατανομής του ανθρώπινου δυναμικού αλλά και των υπόλοιπων εποπτευόμενων από το Υπουργείο Υγείας φορέων. Η σχετική διάταξη που περιγράφει αυτήν την επεξεργασία αναφέρει ρητώς ότι τα δεδομένα «πρέπει να αποστέλλονται κωδικοποιημένα, κατά τρόπο τέτοιο ώστε το Υπουργείο να μην μπορεί να τα αντιστοιχεί σε ταυτοποιημένα ή ταυτοποιήσιμα πρόσωπα».
Θα ήταν καλή λύση το να αποστέλλονται στοιχεία όπου, για κάθε ασθενή, το ψευδώνυμο θα προέκυπτε από εφαρμογή κρυπτογραφικής συνάρτησης κατακερματισμού στον ΑΜΚΑ αυτού; Σχολιάστε την προσέγγιση αυτή.

Η ψευδωνυμοποίηση μπορεί να χρησιμοποιηθεί και ως μέσο επίτευξης της ελαχιστοποίησης των δεδομένων, υπό την έννοια ότι υπάρχουν περιπτώσεις όπου και ο ίδιος ο υπεύθυνος επεξεργασίας δεν πρέπει να γνωρίζει στοιχεία ταυτοποίησης των φυσικών προσώπων (βλ. και τη συναφή πρόβλεψη του άρθρου 11 παρ. 2 του ΓΚΠΔ): και εδώ, τόσο κλασικές όσο και προηγμένες τεχνικές κρυπτογράφησης μπορούν να συνεισφέρουν σημαντικά στην ανάπτυξη αποτελεσματικών σχημάτων ψευδωνυμοποίησης. Για περισσότερη ανάλυση, παραπέμπουμε στα [54], [55], [97].

**Ανωνυμοποίηση (και η σχέση της με την ψευδωνυμοποίηση)**

Δεδομένα τα οποία δεν μπορούν να αντιστοιχηθούν σε ταυτοποιημένα ή ταυτοποιήσιμα πρόσωπα θεωρούνται ανώνυμα δεδομένα. Τα ανώνυμα δεδομένα δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα: όπως είδαμε και νωρίτερα, η Εισαγωγική Σκέψη 26 του ΓΚΠΔ αναφέρει ρητά ότι «*οι αρχές της προστασίας δεδομένων δεν θα πρέπει συνεπώς να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί. Ο παρών κανονισμός δεν αφορά συνεπώς την επεξεργασία τέτοιων ανώνυμων πληροφοριών, ούτε μεταξύ άλλων για στατιστικούς ή ερευνητικούς σκοπούς*».

Ωστόσο, στην ίδια σκέψη περιγράφονται οι προϋποθέσεις υπό τις οποίες θα πρέπει να



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

κρίνεται εάν πράγματι, από δεδομένα που φέρονται να είναι ανωνυμοποιημένα, δεν είναι δυνατόν να υπάρξει αντιστοίχιση με ταυτοποιημένα ή ταυτοποιήσιμα πρόσωπα. Συγκεκριμένα, η ίδια Σκέψη αναφέρει: «*Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας*». Με απλά λόγια, χρήζει ιδιαίτερης προσοχής πριν κάποιος αποφανθεί ότι κάποια δεδομένα είναι ανώνυμα.

- ☞ Κατά κανόνα, η απλή απαλοιφή στοιχείων ταυτοποίησης (αναγνωριστικών) δεν αρκεί για να καταστούν τα δεδομένα ανώνυμα: πρέπει να εξετάζεται εάν, από τις λοιπές πληροφορίες που παραμένουν, είναι ρεαλιστικά εφικτό για κάποιον τρίτο να αναγνωρίσει, έστω και ένα, πρόσωπο.

Γενικά, είναι πολύ δύσκολο να αποφανθεί κάποιος με βεβαιότητα ότι κάποια δεδομένα είναι ανώνυμα (και, άρα, ότι εκφεύγουν του πεδίου εφαρμογής του ΓΚΠΔ). Χρειάζεται ιδιαίτερη προσοχή και, σύμφωνα και με την αρχή της λογοδοσίας, τεκμηρίωση ως προς το γιατί τα δεδομένα κρίθηκαν, από τον υπεύθυνο επεξεργασίας, ανώνυμα.

- ☞ Ακόμα ωστόσο και αν τα δεδομένα καταστούν πράγματι ανώνυμα, η ανωνυμοποίηση προσωπικών δεδομένων αποτελεί, αυτή καθ' αυτή, επεξεργασία δεδομένων προσωπικού χαρακτήρα και ως εκ τούτου, εφαρμόζεται ο ΓΚΠΔ για αυτήν την επεξεργασία. Για παράδειγμα, αν Δημόσιος φορέας ανωνυμοποιεί δεδομένα μετά την πάροδο του αναγκαίου χρόνου τήρησής τους, προκειμένου να μπορεί να συνεχίσει να εξάγει



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

στατιστικά στοιχεία, πρέπει να παρέχει προς τούτο ενημέρωση στα υποκείμενα των δεδομένων, σύμφωνα με τα οριζόμενα στα άρθρα 13 και 14 αναλόγως του ΓΚΠΔ.

**Παράδειγμα:** Νοσοκομείο θέλει να δημοσιοποιήσει στην ιστοσελίδα του ανώνυμα δεδομένα, προκειμένου να παρέχει σε ερευνητές χρήσιμο υλικό για επιστημονική/στατιστική ανάλυση. Για αυτό το λόγο, για κάθε ασθενή του τελευταίου έτους αναρτά τα εξής στοιχεία: «Ημερομηνία γέννησης, φύλο, ταχυδρομικός κώδικας του τόπου κατοικίας, διάγνωση, θεραπεία, εξέλιξη».

Τα εν λόγω δεδομένα, στο πλαίσιο αυτής της επεξεργασίας, δεν μπορούν να θεωρηθούν ανώνυμα. Από αυτές τις πληροφορίες, δύναται για κάποιες περιπτώσεις κάποιος χρήστης να ταυτοποιηθεί (π.χ. αν ο ταχυδρομικός κώδικας αντιστοιχεί σε μία συγκεκριμένη περιοχή μικρής πόλης ή χωριού, οπότε η ημερομηνία γέννησης και φύλο του ατόμου ενδέχεται να επιτρέπουν, σε τρίτους που γνωρίζουν τα πρόσωπα της περιοχής, να αναγνωρίσουν το συγκεκριμένο πρόσωπο). Μάλιστα, το εν λόγω παράδειγμα έχει ήδη μελετηθεί, εδώ και πολλά χρόνια, από ερευνητές στις Η.Π.Α [98], όπου κατέδειξαν, με πρακτική εφαρμογή, ότι πράγματι μπορεί να γίνει αναγνώριση προσώπων – ιδίως δε αν η φερόμενη ως ανωνυμοποιημένη λίστα συγκριθεί με άλλη επώνυμη λίστα που σχετίζεται με αυτή, όπως είναι η λίστα των ψηφοφόρων της περιοχής (στην εργασία [98] περιγράφεται πώς, από μία τέτοια «ανωνυμοποιημένη» λίστα όπως αυτή που περιγράφηκε στο εν λόγω παράδειγμα, αναγνωρίστηκε ο τότε κυβερνήτης της Μασαχουσέτης).

Για αντιμετώπιση (και) τέτοιων κινδύνων, υπάρχει ένα σύνολο τεχνικών ανωνυμοποίησης που, αναλόγως την περίπτωση, μπορούν να εφαρμοστούν. Οι τεχνικές αυτές συνίστανται είτε στην απαλοιφή προσωπικών πληροφοριών (π.χ., στο ανωτέρω παράδειγμα, στην απαλοιφή του φύλου των ασθενών) είτε στη «γενίκευση» (generalisation) των προσωπικών πληροφοριών (π.χ. στο ανωτέρω παράδειγμα, αντικατάσταση της ημερομηνίας γέννησης με το έτος γέννησης ή την τριετία – π.χ. 1970-1973 - εντός της οποίας γεννήθηκε το κάθε πρόσωπο) είτε στην εισαγωγή



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

«θορύβου», δηλαδή μικρής αλλοίωσης στα δεδομένα έτσι ώστε να εξακολουθούν να μην απέχουν ουσιωδώς από τις πραγματικές τους τιμές αλλά να δυσχεραίνουν επιθέσεις αναγνώρισης προσώπων ή διαχωρισμού προσώπων. Ο αναγνώστης που επιθυμεί να εμβαθύνει σε τεχνικές ανωνυμοποίησης, μπορεί να ανατρέξει στα [99] (κατευθυντήριες γραμμές της Ομάδας Εργασίας του Άρθρου 29), [100] (άρθρο επισκόπησης), ενώ μία πρόσφατη πηγή που περιγράφει τόσο την ανωνυμοποίηση όσο και την ψευδωνυμοποίηση από τη σκοπιά της διαχείρισης των σχετικών κινδύνων είναι το [101].

**Παράδειγμα:** Φορέας θέλει να ανωνυμοποιήσει αρχείο με αξιολογήσεις υπαλλήλων, προκειμένου να εξάγονται, επί του ανωνυμοποιημένου αρχείου, κάποια στατιστικά στοιχεία (π.χ. σε τι βαθμό οι αξιολογήσεις εξαρτώνται από τα χρόνια προϋπηρεσίας και την ηλικία, αν υπάρχουν αποκλίσεις μεταξύ ανδρών και γυναικών κ.α.). Οι συναφείς πληροφορίες υπάρχουν στον Πίνακας 1, όπου έχουν απαλειφτεί τα στοιχεία ταυτοποίησής τους.

Ο εν λόγω Πίνακας δεν είναι ανωνυμοποιημένος. Για παράδειγμα, κάποιος που ξέρει τα στοιχεία της εργαζόμενης Α (42 ετών, με 7 έτη προϋπηρεσίας), μπορεί αμέσως να αναγνωρίσει την καταχώρησή της στον Πίνακας 1 και να μάθει την αξιολόγησή της (εν προκειμένω, 8,5).

Ο Πίνακας 2 προκύπτει από τον Πίνακας 1 με τεχνική ανωνυμοποίησης που βασίζεται στις γενικεύσεις των γνωρισμάτων ηλικίας και ετών προϋπηρεσίας (η διάταξη των εγγραφών του πίνακα έχει αλλάξει, για να γίνει πιο εμφανές το όφελος της τεχνικής ανωνυμοποίησης). Πλέον, ακόμα και αν κάποιος ξέρει τα στοιχεία της εργαζομένης Α, δεν μπορεί να την εντοπίσει επακριβώς εντός του ανωνυμοποιημένου πίνακα: το μόνο που ξέρει είναι ότι αντιστοιχεί σε μία εκ τριών πιθανών εγγραφών, όπου οι αξιολογήσεις που έχουν λάβει είναι 8,5, 9,5 και 10 (τις εντοπίζετε κι εσείς στον Πίνακας 2;). Το ίδιο ισχύει για οποιονδήποτε άλλον εργαζόμενο: αν κάποιος ξέρει τα στοιχεία οποιοδήποτε εργαζόμενου, δεν θα μπορεί να τον εντοπίσει επακριβώς στον ανωνυμοποιημένο πίνακα γιατί θα υπάρχουν πάντα τουλάχιστον δύο πιθανές εγγραφές που αντιστοιχούν στον εν λόγω εργαζόμενο.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Για να καταδείξουμε ωστόσο τις δυσκολίες που εγγενώς υπάρχουν σε κάθε τεχνική ανωνυμοποίησης, ας δούμε στο εν λόγω παράδειγμα την εξής περίπτωση: έστω ότι κάποιος τρίτος που βλέπει τον ανωνυμοποιημένο Πίνακας 2 ξέρει τα στοιχεία της εργαζομένης Β (52 ετών, 12 έτη προϋπηρεσίας). Λόγω της ανωνυμοποίησης, δεν μπορεί να εντοπίσει επακριβώς την εγγραφή της στον Πίνακας 2: ωστόσο, και οι δύο πιθανές για την Β εγγραφές έχουν λάβει αξιολόγηση 10. Συνεπώς, παρόλο που δεν μπορεί να εντοπίσει την εγγραφή της, μαθαίνει με βεβαιότητα την αξιολόγησή της. Αυτό καταδεικνύει ότι οι τεχνικές ανωνυμοποίησης πρέπει να λαμβάνουν υπόψη και τέτοιους κινδύνους.

| **Ηλικία** | **Φύλο** | **Έτη προϋπηρεσίας** | **Βαθμός αξιολόγησης** |
|---|---|---|---|
| 34 | Α | 5 | 9,2 |
| 44 | Γ | 8 | 9,5 |
| 42 | Γ | 7 | 8,5 |
| 30 | Α | 3 | 8,5 |
| 33 | Γ | 6 | 9,7 |
| 49 | Α | 10 | 9,6 |
| 45 | Α | 8 | 8,7 |
| 43 | Γ | 6 | 10 |
| 52 | Γ | 12 | 10 |
| 51 | Γ | 14 | 10 |
| 53 | Α | 14 | 9,8 |
| 52 | Α | 13 | 9 |
| 35 | Γ | 8 | 8,7 |

**Πίνακας 1 - Παράδειγμα πίνακα που έχουν απαλειφτεί τα αναγνωριστικά, αλλά δεν έχει εφαρμοστεί τεχνική ανωνυμοποίησης**

| **Ηλικία** | **Φύλο** | **Έτη προϋπηρεσίας** | **Βαθμός αξιολόγησης** |
|---|---|---|---|
| 30-35 | Α | <=5 | 8,5 |
| 30-35 | Α | <=5 | 9,2 |
| 30-35 | Γ | Μεταξύ 6 και 10 | 9,7 |
| 30-35 | Γ | Μεταξύ 6 και 10 | 8,7 |
| 40-50 | Γ | Μεταξύ 6 και 10 | 8,5 |



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

| | | | |
|---|---|---|---|
| 40-50 | Γ | Μεταξύ 6 και 10 | 10 |
| 40-50 | Γ | Μεταξύ 6 και 10 | 9,5 |
| 40-50 | Α | Μεταξύ 6 και 10 | 8,7 |
| 40-50 | Α | Μεταξύ 6 και 10 | 9,6 |
| 50-55 | Γ | Μεταξύ 10 και 15 | 10 |
| 50-55 | Γ | Μεταξύ 10 και 15 | 10 |
| 50-55 | Α | Μεταξύ 10 και 15 | 9 |
| 50-55 | Α | Μεταξύ 10 και 15 | 9,8 |

**Πίνακας 2 - Τα δεδομένα του Πίνακα 1, έχοντας "γενικευτεί" προς επίτευξη ανωνυμοποίησης**

Κλείνοντας αυτήν την Ενότητα, θα πρέπει να σημειωθεί ότι οι τεχνικές ανωνυμοποίησης, όπως αυτές που συνοπτικά περιγράφηκαν νωρίτερα, μπορούν να αξιοποιηθούν ακόμα και αν δεν μπορεί να υπάρξει εγγύηση ότι το τελικό αποτέλεσμα συνιστά πράγματι ανώνυμα δεδομένα: σε κάθε περίπτωση δυσχεραίνουν τη δυνατότητα επανα-ταυτοποίησης και, αναλόγως την περίπτωση και τους σχετικούς κινδύνους, όπως βεβαίως και της μεθόδου ανωνυμοποίησης που έχει χρησιμοποιηθεί αλλά και των παραμέτρων υλοποίησής της, μπορεί να κριθεί ως επαρκής από πλευράς προστασίας δεδομένων (ακόμα και αν δεν μπορούν να χαρακτηριστούν τα παραγόμενα δεδομένα, πέραν πάσης αμφιβολίας, ως ανώνυμα). Μάλιστα, δεν αποκλείεται τέτοιες τεχνικές να πρέπει να εφαρμοστούν και σε ψευδωνυμοποιημένα δεδομένα, προκειμένου να καταστεί η ψευδωνυμοποίηση ισχυρή.

## 15.4 Βιβλιογραφία για περισσότερη μελέτη


1. ENISA, “Handbook on security of personal data processing”, Dec. 2017. Διαθέσιμο στο **https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing**
2. ENISA, “Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation”, Jan. 2019. Διαθέσιμο στο **https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions**
3. ENISA, “Pseudonymisation techniques and use practices”, Dec. 2019.




Ευρωπαϊκή Ένωση
Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Διαθέσιμο στο **https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices**

4. ENISA, “Data pseudonymisation: Advanced techniques and use cases”, Jan. 2021. Διαθέσιμο στο **https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases**
5. European Data Protection Board, “Guidelines 3/2019 on processing of personal data through video devices”. Διαθέσιμο στο **https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf** (η ελληνική εκδοχή)
6. M. Finck and F. Pallas, “They who must not be identified—distinguishing personal from non-personal data under the GDPR”, International Data Privacy Law, 2020. Διαθέσιμο στο **https://academic.oup.com/idpl/article/10/1/11/5802594**
7. B. C. M. Fung, K. Wang, R. Chen and P. S. Yu, “Privacy-preserving Data Publishing: A Survey of Recent Developments”, ACM Computing Surveys, 2010. Διαθέσιμο στο **https://www.cs.sfu.ca/~wangk/pub/FWCY10csur.pdf**
8. K. Limniotis, “Cryptography as the means to protect fundamental human rights," Cryptography, 2021. Διαθέσιμο στο **https://www.mdpi.com/2410-387X/5/4/34**
9. NIST, “Information Security - Guide for Developing Security Plans for Federal Information Systems”, Special Publication 800-18, 2006. Διαθέσιμο στο **https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-18r1.pdf**
10. Working Party 29, Opinion 5/2014 on anonymisation techniques. Διαθέσιμο στο **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf** (η εκδοχή στα ελληνικά)
11. Working Party 29, Opinion 2/2017 on data processing at work. Διαθέσιμο στο **https://ec.europa.eu/newsroom/article29/items/610169** (και στα ελληνικά)
12. NIST, “Security and privacy controls for Information Systems and Organizations”, Special Publication 800-53, rev. 5, 2020. Διαθέσιμο στο **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-**



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

**53r5.pdf**

# 16. Μελέτη περίπτωσης

Η συγκεκριμένη ενότητα αποτελεί έναν, κατά κάποιο τρόπο, οδηγό προκειμένου οι εκπαιδευόμενοι να εφαρμόσουν στην πράξη τις έννοιες που διδαχτήκανε με την παρούσα ύλη και, ακολούθως, να συνδράμουν αναλόγως, εφόσον χρειάζεται, στο φορέα τους.

## 1. Ανάλυση δραστηριοτήτων

Χρησιμοποιήστε ως παράδειγμα το φορέα στον οποίο εργάζεστε. Προσπαθήστε να κάνετε μια πρώτη ανάλυση των δραστηριοτήτων του φορέα, στοχεύοντας κυρίως σε τρεις τομείς:

Α. Προσωπικό του φορέα και η εκτέλεση των διαφόρων υποχρεώσεων του φορέα, σε σχέση με τη μισθοδοσία, την ασφάλιση και τις παροχές στους εργαζόμενούς του.

Β. Επεξεργασία δεδομένων πολιτών, σε σχέση με την εκτέλεση της βασικής αρμοδιότητας του φορέα. Σε περίπτωση που ο φορέας σας εκτελεί πολλές αρμοδιότητες, επιλέξτε τις αρμοδιότητες που γνωρίζετε καλά – όπως, π.χ.αυτές που αντιστοιχούν στο τμήμα το οποίο τώρα εργάζεστε.

Γ. Επεξεργασία δεδομένων επισκεπτών της ιστοσελίδας του φορέα σας

Πιθανές Επεξεργασίες φορέα:

**Α. Προσωπικό**

- Μισθοδοσία
- Άδειες (και αναρρωτικές)
- Αξιολογήσεις
- Κοινωνική πρόνοια
- ……
- ……
- …..

**Β. Αρμοδιότητα Φορέα**

- Διαχείριση αιτημάτων πολιτών
- 
- …..

**Γ. Ιστοσελίδα του φορέα**

- Στοιχεία επισκεπτών για έλεγχο επισκεψιμότητας
- Στοιχεία εγγεγραμμένων χρηστών στις διαδικτυακές υπηρεσίες του φορέα



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

- …..

Για κάθε μία εκ των επεξεργασιών που θα καταγράψετε ανωτέρω, εξειδικεύστε τις κατηγορίες των προσωπικών δεδομένων που υφίστανται επεξεργασία. Επίσης, προσδιορίστε ποια είναι η νομική βάση για την κάθε επεξεργασία.

## 2. Έλεγχος συμμόρφωσης

Εξετάστε την υφιστάμενη κατάσταση στο φορέα σας.

Θεωρείτε ότι καλύπτει τις απαιτήσεις του ΓΚΠΔ; Ποιες ενέργειες απαιτούνται για τη συμμόρφωσή του με τις παρακάτω απαιτήσεις; Αριθμήστε και καταγράψτε, αξιοποιώντας τους πίνακες που σας δίνονται στη συνέχεια (δηλαδή, αφού συμπληρώσετε τους πίνακες, καταγράψτε ποιες ενέργειες πρέπει, κατά τη γνώμη σας, να γίνουν, καθώς και με ποια προτεραιότητα).

Για τη συμπλήρωση των πινάκων που ακολουθούν, προτεραιοποιήστε στον κάθε ένα, από τα πιο σημαντικά (1) έως τα λιγότερο σημαντικά (5).

**Α. Ως Υπεύθυνος επεξεργασίας για την ικανοποίηση των δικαιωμάτων του υποκειμένων των δεδομένων**

| **Α/Α** | **Υποχρέωση (άρθρο)** | **Εκτίμηση υφιστάμενης κατάστασης** | **Απαιτούμενες ενέργειες** | **Προτεραιότητα ενεργειών (1-5)** |
|---|---|---|---|---|
| 1 | Πληροφορίες που παρέχονται κατά τη συλλογή προσωπικών δεδομένων από τα υποκείμενα (13) | | 1) ..<br>2) .. | |
| 2 | Πληροφορίες που παρέχονται κατά τη συλλογή προσωπικών δεδομένων από τρίτες πηγές (13) | | | |
| 3 | Δικαίωμα πρόσβασης (15) | | | |
| 4 | Δικαίωμα διόρθωσης (16) | | | |
| 5 | Δικαίωμα διαγραφής(17) | | | |
| 6 | Δικαίωμα περιορισμού (18) | | | |
| 7 | Δικαίωμα φορητότητας (20) | | | |
| 8 | Δικαίωμα εναντίωσης | | | |



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

| | | | | |
|---|---|---|---|---|
| | (21) | | | |
| **9** | Αυτοματοποιημένη ατομική λήψη αποφάσεων | | | |

**Β. Ως Υπεύθυνος επεξεργασίας για τις σχετικές υποχρεώσεις των κεφαλαίων IV και V.**

| **Α/Α** | **Υποχρέωση (άρθρο)** | **Εκτίμηση υφιστάμενης κατάστασης** | **Απαιτούμενες ενέργειες** | **Προτεραιότητα ενεργειών (1-5)** |
|---|---|---|---|---|
| 1 | Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (25) | | 1) ..<br>2) .. | |
| 2 | Εκτελούντες την επεξεργασία – υποχρέωση έγγραφης ανάθεσης με επαρκείς διαβεβαιώσεις (28-29) | | | |
| 3 | Αρχεία των δραστηριοτήτων επεξεργασίας (30) | | | |
| 4 | Τεχνικά και οργανωτικά μέτρα ασφάλειας (32) | | | |
| 5 | Παραβίαση προσωπικών δεδομένων, γνωστοποίηση – ανακοίνωση (33-34) | | | |
| 6 | Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων – ΕΑΠΔ (35-36) | | | |
| 7 | Ορισμός ΥΠΔ – Υπευθύνου Προστασίας Δεδομένων (37-39) | | | |
| 8 | Διαβιβάσεις δεδομένων σε χώρες εκτός Ε.Ε. (44-49) | | | |



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# Αναφορές


[1] Ευρωπαϊκό Κοινοβούλιο, "ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κα," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN. [Accessed 18 01 2022].

[2] Ευρωπαϊκό Κοινοβούλιο, "Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών," 1995. [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A01995L0046-20031120. [Accessed 18 1 2022].

[3] Ευρωπαϊκό Κοινοβούλιο, "Η Συνθήκη της Λισαβόνας," 2009. [Online]. Available: https://www.europarl.europa.eu/about-parliament/el/powers-and-procedures/the-lisbon-treaty. [Accessed 18 01 2022].

[4] U. N. I. Centre, "ΟΙΚΟΥΜΕΝΙΚΗ ΔΙΑΚΗΡΥΞΗ ΓΙΑ ΤΑ ΑΝΘΡΩΠΙΝΑ ΔΙΚΑΙΩΜΑΤΑ," 1948. [Online]. Available: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=grk. [Accessed 18 01 2022].

[5] Συμβούλιο της Ευρώπης, "https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005," 1950, [Online]. Available: Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου. [Accessed 18 01 2022].

[6] Συμβούλιο της Ευρώπης, "Σύμβαση 108 του Συμβουλίου της Ευρώπης," 1981. [Online]. Available: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. [Accessed 18 01 2022].

[7] Συμβούλιο της Ευρώπης, "Επικαιροποιημένη σύμβαση 108 του Συμβουλίου της Ευρώπης," 2018. [Online]. Available: https://www.coe.int/en/web/data-protection/convention108/modernised. [Accessed 18 01 2022].

[8] Ευρωπαϊκή Ένωση, "Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση," 2012. [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A12012M%2FTXT. [Accessed 18 01 2022].

[9] Ευρωπαϊκή Ένωση, "Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης," 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3A4301854. [Accessed 18 01 2022].

[10] Ευρωπαϊκή Ένωση, "Χάρτης θεμελιωδών δικαιωμάτων της ΕΕ," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33501. [Accessed 18 01 2022].

[11] Ευρωπαϊκό Κοινοβούλιο, "Οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών," 2002. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_el.pdf.

[12] Ευρωπαϊκό Κοινοβούλιο, "Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τροποποίηση της οδηγίας 2002/22/ΕΚ, της οδηγίας 2002/58/ΕΚ και του Κανονισμού (ΕΚ) αριθ. 2006/2004," 2009, [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32009L0136.

[13] Νόμος, "Ν. 2472/1997," [Online]. Available: https://www.dpa.gr/sites/default/files/2019-10/2472_97%20%28SEPT2019%29.pdf. [Accessed 18 01 2022].

[14] Νόμος, "Ν. 3471/2006," 2006. [Online]. Available: https://www.dpa.gr/sites/default/files/2019-09/%CE%9D3471_06.PDF. [Accessed 18 01 2022].




Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

[15] Ευρωπαϊκό Κοινοβούλιο, "Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχν," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016L0680. [Accessed 18 01 2022].

[16] Νόμος, "N. 4624/2019," 2019. [Online]. Available: http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wFqnM3eAbJzrXdtvSoClrL8WkQtR1OJjJd5MXD0LzQTLWPU9yLzB8V68knBzLCmTXKaO6fpVZ6Lx3UnKl3nP8NxdnJ5r9cmWyJWelDvWS_18kAEhATUkJb0x1LIdQ163nV9K--td6SIuYy4kEHGmkxu249n-Zw2yYl0mZ9eBCztpQxx39TqtEEk. [Accessed 18 1 2022].

[17] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Ετήσια έκθεση 2018," 2019. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/etisies-ektheseis/etisia-ekthesi-2018. [Accessed 18 01 2022].

[18] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Γνωμοδότηση 1/2020 - Επί των διατάξεων του Ν. 4624/2019," 2020. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epi-ton-diataxeon-toy-n-46242019. [Accessed 18 01 2022].

[19] Κ. Παπακωνσταντίνου and Λ. Κατσίρας, Πολιτική και δίκαιο Β' γενικού λυκείου, Αθήνα: Οργανισμός Εκδόσεως Διδακτικών Βιβλίων (Ο.Ε.Δ.Β.), 2009.

[20] D. Korff and M. Georges, "The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation," T4DATA Project, 2018. [Online]. Available: https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf . [Accessed 18 01 2022].

[21] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης (FRA - CoE), "γχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων (έκδοση 2018)," 2018. [Online]. Available: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf . [Accessed 18 01 2022].

[22] Β. Σωτηρόπουλος, "Το άρθρο 9Α του Συντάγματος 1975/1986/2001," 2004. [Online]. Available: http://www.greeklaws.com/pubs/uploads/596.pdf. [Accessed 18 01 2022].

[23] European Data Protection Board, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR," 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en. [Accessed 18 01 2022].

[24] Δικαστήριο Ευρωπαϊκής Ένωσης, "Απόφαση στην υπόθεση C 212/13 - František Ryneš κατά Úřad pro ochranu osobních údajů," 2014. [Online]. Available: https://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=EL. [Accessed 18 01 2022].

[25] European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)," 2018. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en. [Accessed 18 01 2022].

[26] Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data - WP 136," [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. [Accessed 18 01 2022].

[27] Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor" - wp169," [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. [Accessed 18 01 2022].

[28] Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability - wp173," [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. [Accessed 18 01 2022].

[29] European Data Protection Board, "Guidelines 2/2019 on the processing of personal data under



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Article 6(1)(b) GDPR in the context of the provision of online services to data subjects," [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en. [Accessed 18 01 2022].

[30] Article 29 Data Protection Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" - WP217," 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. [Accessed 18 01 2022].

[31] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Γνωμοδότηση 1/2021 επί σχεδίου νόμου του Υπουργείου Υποδομών και Μεταφορών," 2021. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gnomodotisi-epi-shedioy-nomoy-toy-ypoyrgeioy-ypodomon-kai-metaforon. [Accessed 18 01 2022].

[32] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679," 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en. [Accessed 18 01 2022].

[33] European Data Protection Board, "Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR," 2021. [Online]. Available: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en. [Accessed 18 01 2022].

[34] Ευρωπαϊκή Επιτροπή, "Standard contractual clauses for data transfers between EU and non-EU countries," 2021. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_el. [Accessed 18 01 2022].

[35] European Data Protection Board, "Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies," 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_ga?order=field_edpb_pc_country&sort=asc. [Accessed 18 01 2022].

[36] European Data Protection Board, "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679," 2018. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_ga. [Accessed 18 01 2022].

[37] European Data Protection Board, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," 2021. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_el. [Accessed 18 01 2022].

[38] Irish Data Protection Commission, "Guidance on Legal Bases for Processing Personal Data," 2019. [Online]. Available: https://www.dataprotection.ie/en/dpc-guidance/guidance-legal-bases-processing-personal-data. [Accessed 18 01 2022].

[39] UK Information Commissioner's Office, "What are the conditions for processing?," 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/. [Accessed 18 01 2022].

[40] Ευρωπαϊκή Επιτροπή, "International dimension of data protection," [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en. [Accessed 18 01 2022].

[41] Article 29 Data Protection Working Party, "Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)," 2018. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/622227/en. [Accessed 18 01 2022].

[42] Article 29 Data Protection Working Party, "Guidelines on the right to data portability," 2017.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

[Online]. Available: https://ec.europa.eu/newsroom/article29/items/611233.

[43] European Data Protection Supervisor, "Opinion 3/2018 on online manipulation and personal data," 2018. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[44] Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679," 2018. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/612053.

[45] M. E. Gilman, "Poverty Lawgorithms: A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms on Low-Income Communities," *Data & Society*, 2020.

[46] European Data Protection Board, "Guidelines 10/2020 on restrictions under Article 23 GDPR," 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_el.

[47] Ευρωπαϊκή Επιτροπή, "Εκτελεστική απόφαση (ΕΕ) 2021/915 της Επιτροπής της 4ης Ιουνίου 2021 για τυποποιημένες συμβατικές ρήτρες μεταξύ υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία βάσει του άρθρου 28 παράγραφος 7 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίο," 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021D0915. [Accessed 18 01 2022].

[48] European Data Protection Board - European Data Protection Supervisor, "Joint Opinion 1/2021 on standard contractual clauses between controllers and processors," 2021. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en. [Accessed 18 01 2022].

[49] European Data Protection Board, "Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)," 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-142019-draft-standard-contractual-clauses_en. [Accessed 18 01 2022].

[50] European Data Protection Board, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default," 2019. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

[51] ENISA, "Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default," 2019. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2.

[52] European Data Protection Supervisor, "Preliminary Opinion 5/2018 on Privacy by Design," 2018. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[53] Article 29 Data Protection Working Party, "Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR," 2018. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/624045/en.

[54] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers ('DPOs')," 2017. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/612048/en.

[55] Article 29 Data Protection Working Party, "Guidelines on Personal data breach notification under Regulation 2016/679," 2018. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/612052/en.

[56] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability,Pseudonymity, and Identity Management," 2010. [Online]. Available: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

[57] ENISA, "Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation," 2019. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions.

[58] ENISA, "Pseudonymisation techniques and best practices," 2019. [Online]. Available: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

[59] K. G. Paterson, "The Cyber Security Body of Knowledge, University of Bristol, 2021, ch. Applied Cryptography, version 1.0.0.," 2021. [Online]. Available: https://www.cybok.org/media/downloads/Applied_Cryptography_KA_webinar_slides.pdf.

[60] European Data Protection Board, "Guidelines 01/2021 on Examples regarding Data Breach Notification," 2021. [Online]. Available: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en.

[61] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA)," 2017. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/611236.

[62] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 65/2018," 2018. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/katalogos-me-ta-eidi-ton-praxeon-epexergasias-poy-ypokeintai-stin.

[63] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Γνωμοδότηση 3/2020 της Αρχής επί του σχεδίου Προεδρικού Διατάγματος σχετικά με τη χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους," 2020. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gnomodotisi-32020-tis-arhis-epi-toy-shedioy-proedrikoy-diatagmatos.

[64] CNIL, "PIA software," [Online]. Available: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

[65] European Data Protection Supervisor, "Necessity Toolkit," 2017. [Online]. Available: https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

[66] European Data Protection Supervisor, "Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data," 2019. [Online]. Available: https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en.

[67] European Data Protection Board, "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679," 2019. [Online]. Available: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring_en.

[68] European Data Protection Board, "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation," [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en.

[69] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 25/2020 - Συμπληρωματικές απαιτήσεις της Αρχής για τη διαπίστευση των φορέων πιστοποίησης με ενσωματωμένες τις συστάσεις της σχετικής γνώμης 22/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων," [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis?field_year_from=2020&field_year_to=2020&field_category=239&field_thematic=All&field_protocol_number=25&field_keywords=.

[70] TRAIN GR-CY consortium, "Problem-based training activities on data protection," 2019. [Online]. Available: http://traingrcy.law.uoa.gr/moodle/#home-page-carousel. [Accessed 18 01 2022].

[71] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Συμμόρφωση με ΓΚΠΔ," [Online]. Available: https://www.dpa.gr/el/foreis/odigos_gkpd. [Accessed 18 01 2022].

[72] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Για το ζήτημα της αρμοδιότητας της Αρχής, σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, να επιλαμβάνεται επί ερωτημάτων και αιτήσεων υπευθύνων επεξεργασίας, των υποκειμένων των δεδομένων ή/και τρίτων σχετικά με ζητήματα επεξεργασίας προσωπι," 2018. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gia-zitima-tis-armodiotitas-tis-arhis-symfona-me-ton-geniko-kanonismo-gia. [Accessed 18 01 2022].

[73] Article 29 Data Protection Working Party, "Guidelines on the Lead Supervisory Authority (wp244rev.01)," 2018. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/611235/en. [Accessed 18 01 2022].



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

[74] Article 29 Data Protection Working Party, "Guidelines on the application and setting of administrative fines (wp253)," 2018. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/611237/en. [Accessed 18 01 2022].

[75] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Ετήσια Έκθεση 2006," 2007, [Online]. Available: https://www.dpa.gr/el/enimerwtiko/etisies-ektheseis/etisia-ekthesi-2006.

[76] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 73/2017," 2017, [Online]. Available: https://www.dpa.gr/index.php/el/enimerwtiko/prakseisArxis/katagrafi-tilefonikon-kliseon-me-skopo-tin-proothisi-proionton-kai.

[77] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 86/2015," 2015. [Online]. Available: https://www.dpa.gr/index.php/el/enimerwtiko/prakseisArxis/exetasi-ypothesis-akroasis-tilefonikon-kliseon-se-tmima-exypiretisis.

[78] Article 29 Data Protection Working Party, "Opinion 04/2012 on Cookie Consent Exemption," 2012. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

[79] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Γνωμοδότηση 6/2013 - Πρόσβαση σε δημόσια έγγραφα," [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/prosbasi-se-dimosia-eggrafa.

[80] Ανεξάρτητη Αρχή Δημοσίων Εσόδων, "Εγχειρίδιο απαντήσεων στα συνηθέστερα ερωτήματα σε θέματα του Κώδικα Διοικητικής Διαδικασίας," 2021. [Online]. Available: https://www.aade.gr/sites/default/files/2021-10/egxeiridio_0.pdf.

[81] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Ετήσια Έκθεση 2009," 2019, [Online]. Available: https://www.dpa.gr/el/enimerwtiko/etisies-ektheseis/etisia-ekthesi-2009.

[82] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 13/2009," 2009. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/ypohreosi-toy-dimoy-os-ypeythynos-epexergasias-sti-basi-ton-diataxeon-toy.

[83] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 123/2017," 2017. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/adeia-gia-horigisi-stoiheion-synypopsifioy.

[84] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 144/2017," 2017, [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/systasi-se-dimosia-ypiresia-gia-mi-enimerosi-ypalliloy-tis-shetika-me.

[85] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 41/2019," 2019. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiplixi-sto-ypoyrgeio-naytilias-kai-nisiotikis-politikis-gia-tin.

[86] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 40/2005," 2005. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/koinoboyleytikos-eleghos-kai-prosbasi-se-stoiheia-synypopsifioy.

[87] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Γνωμοδότηση 3/2009 - Έννομες συνέπειες εισαγγελικής παραγγελίας για τη χορήγηση δημοσίων εγγράφων," 2009. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/ennomes-synepeies-eisaggelikis-paraggelias-gia-ti-horigisi-dimosion.

[88] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 73/2010," 2010. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/prosbasi-kataggellomenoy-se-stoiheia-kataggellontos-sto-plaisio.

[89] Article 29 Data Protection Working Party, "Working document on the surveillance of electronic communications in the workplace," 2002. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

[90] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Οδηγία 115/2001 - Προστασία προσωπικών δεδομένων στο πεδίο των εργασιακών σχέσεων," [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/prostasia-ton-prosopikon-dedomenon-sto-pedio-ton-ergasiakon-sheseon.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

[91] Article 29 Data Protection Working Party, "Opinion 2/2017 on data processing at work," 2017, [Online]. Available: https://ec.europa.eu/newsroom/article29/items/610169/en.

[92] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 34/2018," 2018. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/eleghos-ilektronikoy-ypologisti-ergazomenoy-apo-ton-ergodoti.

[93] Αρχή Προστασίας Δεδομενων Προσωπικού Χαρακτήρα, "Οδηγία 1/2011 - Χρήση συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών," 2011. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/hrisi-systimaton-binteoepitirisis-gia-tin-prostasia-prosopon-kai-agathon.

[94] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices," 2019. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[95] Article 29 Data Protection Working Party, "Working document on biometrics," 2003. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf.

[96] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Ετήσια Έκθεση 2014," 2015. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/etisies-ektheseis/etisia-ekthesi-2014.

[97] Σ. Κάτσικας, Διαχείριση της Ασφάλειας Πληροφοριών, Πεδίο, 2014.

[98] NIST, "Guide for Developing Security Plans for Federal Information Systems (SP 800-18 Rev. 1)," 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final.

[99] ENISA, "Handbook on security of personal data processing," 2017. [Online]. Available: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing.

[100] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Οδηγία 1/2005 για την ασφαλή καταστροφή προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας," [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/odigia-gia-tin-asfali-katastrofi-prosopikon-dedomenon-meta-peras-tis.

[101] NIST, "Guide to Computer Security Log Management (SP800-92)," 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-92/final.

[102] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Κατευθυντήριες Γραμμές 2/2020 για τη λήψη μέτρων ασφάλειας στο πλαίσιο τηλεργασίας," 2020. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/kateythyntiries-grammes-gia-ti-lipsi-metron-asfaleias-sto-plaisio.

[103] K. Limniotis, "Cryptography as the Means to Protect Fundamental Human Rights," *Cryptography*, pp. https://www.mdpi.com/2410-387X/5/4/34, 2021.

[104] European Data Protection Board, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[105] ENISA, "Data Pseudonymisation: Advanced Techniques and Use Cases," 2021. [Online]. Available: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases.

[106] L. Sweeney, "k-Anonymity: A model for protecting privacy," *nternational Journal on Uncertainty, Fuziness and Knowledge-based Systems*, 2002.

[107] Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques," 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[108] B. C. M. Fung, K. Wang, R. Chen and P. S. Yu, "Privacy-preserving Data Publishing: A Survey of Recent Developments," *ACM Computing Surveys*, p. 2010.

[109] M. Finck and F. Pallas, "They who must not be identified—distinguishing personal from non-personal data under the GDPR," *International Data Privacy Law*, 2020.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

[110] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Γνωμοδότηση 1/2017," 2017. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gnostopoiisi-epexergasias-prosopikon-dedomenon-sto-plaisio-toy.

[111] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Απόφαση 65/2016," 2016, [Online]. Available: https://www.dpa.gr/index.php/el/enimerwtiko/prakseisArxis/pragmatopoiisi-tilefonikon-kliseon-me-anthropini-parembasi-gia-skopo-0.

[112] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Γνωμοδότηση 5/2017 - Προϋποθέσεις τοποθέτησης κάμερας στην είσοδο διαμερίσματος αποκλειστικά και μόνο για τον σκοπό της προστασίας των προσώπων που διαμένουν ή εργάζονται σε αυτό, καθώς και των αγαθών των ενοίκων του διαμερίσματος," 2017. [Online]. Available: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/proypotheseis-topothetisis-kameras-stin-eisodo-diamerismatos-apokleistika.



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

# Γλωσσάρι

ΑΠΔΠΧ/ΑΠΔ - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΓΚΠΔ - ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

ΔΕΕ – Δικαστήριο της Ευρωπαϊκής Ένωσης

ΕΑΠΔ – Εκτίμηση αντικτύπου ως προς την προστασία δεδομένων

ΕΔΔΑ - Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου

Ε.Ε./ΕΕ – Ευρωπαϊκή Ένωση

Ε.Ο.Χ./ΕΟΧ – Ευρωπαϊκός Οικονομικός Χώρος (Ισλανδία, Νορβηγία και Λιχτενστάιν)

ΕΣΔΑ - Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου

ΕΣΠΔ/EDPB – Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

ΕΣΥΔ – Εθνικό Σύστημα Διαπίστευσης

Η/Υ – Ηλεκτρονικοί Υπολογιστές

ΚΔΔιαδ – Κώδικας Διοικητικής Διαδικασίας

Κ-Μ – Κράτη Μέλη της Ε.Ε.

ΝΣΚ – Νομικό Συμβούλιο του Κράτους

Ο.Ε. αρ. 29 - Ομάδα Εργασίας του Άρθρου 29 της οδηγίας 95/46/ΕΚ

ΣΕΕ - Συνθήκη για την Ευρωπαϊκή Ένωση

ΣΛΕΕ - Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης

ΣτΕ – Συμβούλιο της Επικρατείας

ΥΠΔ – Υπεύθυνος Προστασίας Δεδομένων

CNIL – Γαλλική Αρχή Προστασίας Δεδομένων

EDPS – Ευρωπαίος Επόπτης για την Προστασία Δεδομενων

ENISA – Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια

ePrivacy - επεξεργασία των δεδομένων προσωπικού χαρακτήρα και προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

ISO - International Organization for Standardization



Ε.Π. ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης