Δικηγορικός Σύλλογος Καρδίτσας

GDPR και DPO:
Γενικός Κανονισμός για την Προστασία Δεδομένων
και
Υπεύθυνος Προστασίας Δεδομένων

Μέρος 1ο (Δικαιώματα – DPO)

Ιούλιος 2018

Πρωτογενές Δίκαιο

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου

- Άρθρο 8: ιδιωτική & οικογενειακή ζωή

Χάρτης Θεμελιωδών Δικαιωμάτων Ευρωπαϊκής Ένωσης

- Άρθρο 7: ιδιωτική & οικογενειακή ζωή
- Άρθρο 8: προστασία προσωπικών δεδομένων

Συνταγματική Κατοχύρωση

ΣΥΝΤΑΓΜΑ ΤΗΣ ΕΛΛΑΔΑΣ
(αναθεώρηση 2001)

- Άρθρο 9Α: προστασία προσωπικών δεδομένων

Υφιστάμενο Νομικό Πλαίσιο

- Η Σύμβαση για την Προστασία των Ατόμων σχετικά με την Αυτόματη Επεξεργασία Προσωπικών Δεδομένων (CETS No. 108), κυρώθηκε με τον ν. 2068/92
- Ο νόμος **2472/1997** (με τις τροποποιήσεις του) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα
  (Εναρμονιστικός - Οδηγία 95/46/ΕΚ)
- Ο νόμος 3471/2006 (προστασία δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών)
- Ο νόμος 3917/2011 (Διατήρηση δεδομένων - συστήματα επιτήρησης σε δημόσιους χώρους)

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων

- **Τέθηκε σε εφαρμογή στις 25 Μαΐου 2018**
- Τέθηκε σε ισχύ ήδη από 24-05-2016
- Καταργεί την Οδηγία 95/46/ΕΚ, η οποία ενσωματώθηκε στο ελληνικό δίκαιο με τον ν. 2472/1997

Ανάγκη αντικατάστασης του υφιστάμενου πλαισίου:

Η υφιστάμενη Οδηγία (95/46/ΕΚ), μετά από περίπου μια εικοσαετία, θεωρείται ξεπερασμένη - δεν ανταποκρίνεται επαρκώς στις ανάγκες της εποχής λόγω:

- Των **ραγδαίων τεχνολογικών εξελίξεων** π.χ. smartphones, Internet of Things (IoT), Artificial Intelligence (AI)
- Της χρήσης **του διαδικτύου** και των νέων υπηρεσιών που παρέχει π.χ. ηλεκτρονικό εμπόριο
- Της ανάπτυξης της **ψηφιακής οικονομίας** π.χ. internet banking
- Της ευρείας **χρήσης των μέσων κοινωνικής δικτύωσης**
- Της **αυξανόμενης δημοσιοποίησης προσωπικών πληροφοριών** και διάθεσής τους σε παγκόσμιο επίπεδο

Πεδίο εφαρμογής του Κανονισμού

- Στο **έδαφος της Ελλάδας**
- Όταν εφαρμόζεται το ελληνικό δίκαιο δυνάμει διεθνούς δικαίου
- Σε διασυνοριακές υποθέσεις που αφορούν πρόσωπα εντός του **Ε**υρωπαϊκού **Ο**ικονομικού **Χ**ώρου (συνδεδεμένες εταιρείες)
- Σε επεξεργασία εκτός ΕΟΧ για υποκείμενα που βρίσκονται εντός ΕΟΧ
- Σε επεξεργασία που εκτελείται εντός ΕΟΧ για υποκείμενα που βρίσκονται εκτός ΕΟΧ

  Ευρωπαϊκός Οικονομικός Χώρος = Ευρωπαϊκή Ένωση (28 κράτη - μέλη) και Ισλανδία, Λίχτενσταϊν και Νορβηγία
- Κύρια εγκατάσταση: όταν μια εταιρεία έχει εγκαταστάσεις σε πολλά κράτη μέλη, κατά κανόνα, ο τόπος κεντρικής διοίκησης στην Ένωση

Ο Κανονισμός **δεν εφαρμόζεται** στην επεξεργασία προσωπικών δεδομένων από φυσικό πρόσωπο **στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας** και άρα χωρίς σύνδεση με κάποια επαγγελματική ή εμπορική δραστηριότητα

Ο Κανονισμός **δεν εφαρμόζεται στα προσωπικά δεδομένα θανόντων**

Καινοτομίες του Κανονισμού

(α) **Ομοιόμορφη εφαρμογή σε όλη την Ευρωπαϊκή Ένωση:**

- διαμορφώνεται ενιαίο νομικό πλαίσιο χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας
- ίδιο επίπεδο νομικά εκτελεστών δικαιωμάτων και υποχρεώσεων, σε όλα τα κράτη μέλη
- επιβολή ισοδύναμων κυρώσεων από τις ΑΠΔΠΧ

(β) **Ενίσχυση** υφιστάμενων **δικαιωμάτων, δημιουργία νέων**

(γ) Ενίσχυση υφιστάμενων αρχών προστασίας δεδομένων

(δ) Αυστηρότερες υποχρεώσεις στους υπεύθυνους επεξεργασίας

(ε) Δικαίωμα αποζημίωσης και για μη υλική ζημία

(στ) Ενδυνάμωση συνεργασίας ΑΠΔΠΧ σε διασυνοριακές υποθέσεις

(ζ) Εισαγωγή του θεσμού της ενιαίας θυρίδας (one stop shop) *(κάθε πολίτης και κάθε επιχείρηση δικαιούται να επιλέξει μία ΑΠΔΠΧ, με την οποία να συναλλάσσεται)*

(η) Διενέργεια προληπτικών ελέγχων (ex ante αντί για ex post)

(θ) Πρόσβαση από την ΑΠΔΠΧ στις κτιριακές εγκαταστάσεις και στον εξοπλισμό του Οργανισμού (υπεύθυνου επεξεργασίας ή εκτελούντα την επεξεργασία)

(ι) Επιβολή αυστηρότερων κυρώσεων

(κ) Κατάργηση Γνωστοποιήσεων και Αδειών Διασύνδεσης / Διαβίβασης, όπως τις γνωρίζαμε προηγουμένως

(λ) **Ευθύνη τόσο σε υπεύθυνους επεξεργασίας όσο και σε εκτελούντες την επεξεργασία**

(μ) Αυστηρές προϋποθέσεις για τη συγκατάθεση: καταργείται η σιωπηρή συγκατάθεση για την επεξεργασία δεδομένων και εισάγονται συγκεκριμένες υποχρεώσεις σχετικά με την απόδειξη ύπαρξης συγκατάθεσης

(ν) **Καθιέρωση του θεσμού του Υπεύθυνου Προστασίας Δεδομένων**

Διοικητικά πρόστιμα

- Αυστηρότατα πρόστιμα, με **ανώτατο όριο 20.000.000€ ή 4% του παγκόσμιου κύκλου εργασιών** για παραβιάσεις των υποχρεώσεων που σχετίζονται, μεταξύ άλλων:
  - με τις βασικές αρχές επεξεργασίας
  - τα δικαιώματα των φυσικών προσώπων
  - την μη παροχή πρόσβασης στην ΑΠΔΠΧ, προκειμένου να είναι σε θέση να ασκήσει τις εποπτικές της αρμοδιότητες
- Προβλέπεται πρόστιμο έως 10.000.000€ ή 2% του παγκόσμιου κύκλου εργασιών για παραβιάσεις που αφορούν, μεταξύ άλλων:
  - στις υποχρεώσεις σχετικά με τη συγκατάθεση ανηλίκων
  - στις υποχρεώσεις του υπεύθυνου επεξεργασίας σχετικά με την εκτέλεση καθηκόντων του Υπεύθυνου Προστασίας Δεδομένων
  - στην προστασία των προσωπικών δεδομένων από τον σχεδιασμό και εξ ορισμού

Βασικοί ορισμοί

- **Δεδομένα προσωπικού χαρακτήρα:** κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («**υποκείμενο των δεδομένων**»)
- **Ταυτοποιήσιμο φυσικό πρόσωπο** είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας
- **Προσωπικά δεδομένα**: [ΕΝΔΕΙΚΤΙΚΑ] στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ.), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες.

  Επίσης, τα **δεδομένα γεωγραφικής θέσης, και online αναγνωριστικά στοιχεία ταυτότητας** (επιγραμμικά στοιχεία), τα οποία παρέχονται από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλά τους και διευκολύνουν τον εντοπισμό του φυσικού προσώπου (π.χ. IP address, εντοπισμός θέσης μέσω GPS)

Βασικοί ορισμοί

- **Προσωπικά δεδομένα ειδικών κατηγοριών**: τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνοτική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην ερωτική του ζωή, τον γενετήσιο προσανατολισμό του.

  Επίσης, τα γενετικά δεδομένα ή βιομετρικά δεδομένα, που υφίστανται επεξεργασία με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου

- Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν **ποινικές καταδίκες και αδικήματα** ή σχετικά μέτρα ασφάλειας που βασίζεται στο άρθρο 6 παράγραφος 1 ΓΚΠΔ διενεργείται μόνο υπό τον έλεγχο επίσημης αρχής ή εάν η επεξεργασία επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων

Βασικοί ορισμοί

- **επεξεργασία:** κάθε πράξη ή σειρά πράξεων που πραγματοποιείται, σε δεδομένα προσωπικού χαρακτήρα, με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, όπως η **συλλογή**, η καταχώριση, η οργάνωση, η διάρθρωση, η **αποθήκευση**, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η **διάδοση** ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η **διαγραφή** ή η **καταστροφή**
- **υπεύθυνος επεξεργασίας:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα τους ή από κοινού με άλλα, **καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας** δεδομένων προσωπικού χαρακτήρα
- **εκτελών την επεξεργασία:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που **επεξεργάζεται** δεδομένα προσωπικού χαρακτήρα **για λογαριασμό** του υπευθύνου της επεξεργασίας

Καινούριοι Ορισμοί (Άρθρο 4)

- **κατάρτιση προφίλ:** αυτοματοποιημένη επεξεργασία με την οποία αξιολογούνται προσωπικές πτυχές π.χ. απόδοση στην εργασία, οικονομική κατάσταση, υγεία, θέση/μετακίνηση φυσικού προσώπου

  Επιτρέπεται όταν τηρούνται οι βασικές αρχές επεξεργασίας και οι λόγοι της επεξεργασίας είναι νόμιμοι

- **γενετικά δεδομένα:** δεδομένα που κληρονομήθηκαν ή αποκτήθηκαν, ιδίως από ανάλυση βιολογικού δείγματος και παρέχουν μοναδικές πληροφορίες για την φυσιολογία ή υγεία **π.χ. DNA**

- **βιομετρικά δεδομένα:** δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία και επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου π.χ. εικόνες προσώπου, **δακτυλοσκοπικά δεδομένα**, ίριδα, παλάμη, φωνή

- **ψευδωνυμοποίηση: επεξεργασία που εκτελείται ώστε τα δεδομένα να μην μπορούν να ταυτοποιήσουν φυσικό πρόσωπο, χωρίς τη χρήση συμπληρωματικών πληροφοριών** – οι συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα που διασφαλίζουν ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο
  - Ενισχύει την ασφάλεια των δεδομένων και την Αρχή της Λογοδοσίας αφού αποδεικνύει συμμόρφωση
  - Μπορεί να επιτευχθεί με κρυπτογράφηση των αναγνωριστικών στοιχείων ταυτότητας.

    π.χ. Η φράση «Ο Πέτρος Αντωνίου γεννήθηκε στις 25 Ιανουαρίου 1970, διαμένει στην Καρδίτσα και εργάζεται σε τράπεζα», μπορεί να καταστεί ψευδώνυμη ως εξής:

    «Ο Π.Α. γεννήθηκε το 1970, διαμένει στην Καρδίτσα και εργάζεται σε τράπεζα» ή

    «Ο 48 διαμένει στην Καρδίτσα και εργάζεται σε τράπεζα» ή

    «Ο ΒΦΓ43ΓΑ διαμένει στην Καρδίτσα και εργάζεται σε τράπεζα»

- **παραβίαση προσωπικών δεδομένων:** 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

- υπηρεσία της κοινωνίας της πληροφορίας: υπηρεσία που παρέχεται συνήθως έναντι αμοιβής, με ηλεκτρονικά μέσα, εξ αποστάσεως (τα συμβαλλόμενα μέρη δεν είναι ταυτόχρονα παρόντα) κατόπιν παραγγελίας ενός αποδέκτη υπηρεσιών. π.χ. YouTube, Amazon, eBay

Διασυνοριακή επεξεργασία

- Η επεξεργασία που λαμβάνει χώρα σε εγκαταστάσεις **σε περισσότερα του ενός κράτη μέλη της Ευρωπαϊκής Ένωσης**, όπου είναι εγκαταστημένος είτε ο υπεύθυνος επεξεργασίας είτε ο εκτελών την επεξεργασία είτε και οι δύο
ή
η επεξεργασία που εκτελείται στη μία μόνο εγκατάσταση του υπεύθυνου επεξεργασίας ή εκτελούντα **αλλά επηρεάζει ή ενδέχεται* να επηρεάσει ουσιωδώς** υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη – μέλη**

ενδέχεται *= *δεν συμπεριλαμβάνει τη μακρινή πιθανότητα ουσιώδους επιρροής. Η ουσιώδης επιρροή πρέπει να είναι περισσότερο πιθανό να συμβεί από το να μη συμβεί* [wp244rev01]
επηρεάσει ουσιωδώς **= κρίνεται κατά περίπτωση. Θα συνεκτιμώνται το πλαίσιο της επεξεργασίας, το είδος των δεδομένων, ο σκοπός της επεξεργασίας και άλλοι παράγοντες [wp244rev01]

Παραδείγματα επεξεργασιών που επηρεάζουν / ενδέχεται να επηρεάσουν ουσιωδώς υποκείμενα σε περισσότερα κράτη μέλη

- Προκαλεί ή ενδέχεται να προκαλέσει ζημία, απώλεια ή ταλαιπωρία σε φυσικά πρόσωπα *(π.χ. διαφημιστική εταιρεία που έχει την κύρια εγκατάσταση της στην ΕΕ αποστέλλει ανεπιθύμητες διαφημίσεις σε ηλεκτρονικές διευθύνσεις πολιτών ΕΕ)*
- Έχει ή ενδέχεται να έχει πραγματική επιρροή όσον αφορά στον περιορισμό των δικαιωμάτων *(π.χ. εταιρεία παροχής επενδυτικών υπηρεσιών ηχογραφεί τις τηλεφωνικές συνομιλίες επενδυτών από διάφορα κράτη - μέλη και δεν ικανοποιεί το δικαίωμα πρόσβασής τους σε αυτές)*
- Επηρεάζει ή ενδέχεται να επηρεάσει την υγεία, την ευεξία και την ψυχική ηρεμία φυσικών προσώπων
- Γίνεται ανάλυση ειδικών κατηγοριών δεδομένων, ιδίως δεδομένων παιδιών
- Έχει αβέβαιες, απρόβλεπτες ή ανεπιθύμητες συνέπειες για τα φυσικά πρόσωπα

- **Συγκατάθεση:** δεν υπήρχε αντίστοιχη ρύθμιση στην Οδηγία για **απόδειξη** λήψης συγκατάθεσης.

  Τώρα τίθενται **αυστηρές προϋποθέσεις για τη συγκατάθεση**

- Ο υπεύθυνος επεξεργασίας **πρέπει να αποδείξει** ότι το άτομο έδωσε τη συγκατάθεσή του
- **Το κείμενο συγκατάθεσης πρέπει να είναι κατανοητό, με σαφή και απλή διατύπωση και ξεχωριστό από αλλά θέματα**
- **Δικαίωμα ανάκλησης συγκατάθεσης ανά πάσα στιγμή**
- **Ελεύθερη συγκατάθεση** στα πλαίσια σύμβασης: το άτομο είναι σε θέση να επιλέξει και δεν διατρέχει τον κίνδυνο εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν συγκατατεθεί

- **Συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας της πληροφορίας**
  π.χ. e-government, e-commerce, eBay, Amazon, gambling

- **Εάν το παιδί <u>είναι 16 ετών ή άνω</u>, η συγκατάθεση δίνεται από το ίδιο το παιδί**
  Εάν το παιδί είναι κάτω των 16 ετών, η συγκατάθεση παρέχεται ή εγκρίνεται μόνο από το πρόσωπο που έχει τη γονική μέριμνα

- **Τα Κράτη Μέλη μπορούν να μειώσουν το όριο ηλικίας με νομική διάταξη, όχι όμως κάτω των 13 ετών**
  (Στο υπό διαβούλευση νομοσχέδιο, το όριο ηλικίας ήταν 15 έτη)

- Ο υπεύθυνος επεξεργασίας επαληθεύει ότι η συγκατάθεση παρέχεται από το πρόσωπο που έχει τη γονική μέριμνα, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία

Αρχές νόμιμης επεξεργασίας (άρθρο 5)

- Εισάγεται η **Αρχή της Λογοδοσίας:**

  Ο Οργανισμός (υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία) θα πρέπει, ανά πάσα στιγμή, να καθορίζει και να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα (σύμφωνα με το άρθρο 32), **για να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό**.

  Οι υπόλοιπες αρχές παραμένουν όμοιες με την Οδηγία:

  1. Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας (lawfulness, fairness and transparency):

  Τα προσωπικά δεδομένα υποβάλλονται σε **νόμιμη και θεμιτή επεξεργασία με διαφανή τρόπο**:

  - Η ενημέρωση είναι συνοπτική, εύκολα προσβάσιμη και κατανοητή. Χρησιμοποιείται σαφής και απλή διατύπωση
  - Ο Οργανισμός αποδεικνύει ότι οι εσωτερικές διαδικασίες του είναι διαφανείς. Γι’ αυτό, εξηγεί τον τρόπο που τα δεδομένα τυγχάνουν επεξεργασίας, ποια τα δικαιώματα των ατόμων και πώς αυτά ασκούνται

Αρχές νόμιμης επεξεργασίας (άρθρο 5)

2. Αρχή του περιορισμού του σκοπού (purpose limitation)**:**

Τα δεδομένα **συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς** και **δεν υποβάλλονται σε επεξεργασία ασύμβατη με τους αρχικούς σκοπούς**

Περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς, εφόσον πληρούνται οι προϋποθέσεις του άρθρου 89 (δεν απαιτείται Άδεια από την ΑΠΔΠΧ για την περαιτέρω επεξεργασία)

3. Αρχή της ελαχιστοποίησης των δεδομένων (data minimisation)**:**

Τα δεδομένα που υφίστανται επεξεργασία **είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς** για τους οποίους υποβάλλονται σε επεξεργασία

Αρχές νόμιμης επεξεργασίας (άρθρο 5)

4. Αρχή της ακρίβειας (accuracy)**:**

Τα δεδομένα είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται·

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

5. Αρχή του περιορισμού της περιόδου αποθήκευσης (storage limitation)**:**

Τα δεδομένα διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των ατόμων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας. Για μεγαλύτερα χρονικά διαστήματα: για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, με τη λήψη κατάλληλων μέτρων

6. Αρχή της ακεραιότητας και εμπιστευτικότητας: (integrity and confidentiality)**:**

Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία **κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλειά τους**

Πότε είναι νόμιμη η επεξεργασία προσωπικών δεδομένων (Άρθρο 6 – Αιτ. Σκέψη 40-50)

- Όταν έχει συναινέσει το υποκείμενο των δεδομένων, ή
- Για εκτέλεση σύμβασης, ή
- Για έννομη υποχρέωση του υπεύθυνου επεξεργασίας, ή
- Για διαφύλαξη ζωτικού συμφέροντος του ατόμου (ανθρωπιστικοί σκοποί π.χ. επιδημίες, ανταπόκριση σε καταστροφές), ή
- Για δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας, ή
- Για το έννομο συμφέρον του υπεύθυνου επεξεργασίας ή τρίτου (μόνο αν υπερέχει των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων)

Η **νόμιμη βάση** επεξεργασίας πρέπει **να προσδιοριστεί** και να καταγραφεί **πριν ξεκινήσει η επεξεργασία**.
Και δεν πρέπει να μεταβάλλεται χωρίς σπουδαίο λόγο

Πότε είναι νόμιμη η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων (Άρθρο 9)

Κατά κανόνα **απαγορεύεται** η επεξεργασία τους

Για τη σύννομη επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων πρέπει να προσδιοριστεί και νόμιμη βάση επεξεργασίας προσωπικών δεδομένων (Άρθρο 6) και μια εξαίρεση που επιτρέπει την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων (Άρθρο 9), όπως:

(α) αν δοθεί **ρητή συγκατάθεση** (όχι σιωπηρή), ή

(β) στον τομέα του εργατικού δικαίου (και δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας – *νέα ρύθμιση*), ή

(γ) για ζωτικό συμφέρον (ανθρωπιστικοί σκοποί π.χ. επιδημίες, ανταπόκριση σε καταστροφές), ή

(δ) για δραστηριότητες ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο – αφορά τα μέλη *(ή τα πρώην μέλη του - νέα ρύθμιση)* ή πρόσωπα που έχουν τακτική επικοινωνία μαζί του, ή

(ε) για δεδομένα που έχουν προδήλως δημοσιοποιηθεί από το άτομο, ή

(στ) για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων καθώς και **όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα**, ή

(ζ) για λόγους ουσιαστικού δημόσιου συμφέροντος, ή

(η) για προληπτική ή επαγγελματική ιατρική, για εκτίμηση ικανότητας προς εργασία, ιατρική διάγνωση, υγειονομική ή κοινωνική περίθαλψη ή θεραπεία ή διαχείριση υγειονομικών και κοινωνικών συστημάτων δυνάμει νόμου (π.χ. πιλότοι ή μάγειρες) ή σύμβασης με επαγγελματία στον τομέα της υγείας που τηρεί το επαγγελματικό απόρρητο, ή

(θ) για λόγους δημόσιου συμφέροντος: π.χ. δημόσια υγείας, διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων, ή

(ι) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον *(νέα ρύθμιση),* για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

Πότε είναι νόμιμη η επεξεργασία προσωπικών δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα (Άρθρο 10)

- Για τη σύννομη επεξεργασία προσωπικών δεδομένων που αφορούν **ποινικές καταδίκες, αδικήματα και μέτρα ασφάλειας** πρέπει να προσδιοριστεί και νόμιμη βάση επεξεργασίας προσωπικών δεδομένων (Άρθρο 6) και η επεξεργασία να γίνεται υπό τον έλεγχο επίσημης αρχής ή να επιτρέπεται από το δίκαιο της Ένωσης ή του κράτους μέλους το οποίο προβλέπει επαρκείς εγγυήσεις (Άρθρο 10)
- Ο νόμος δύναται να επιτρέψει την επεξεργασία για πρόσληψη σε συγκεκριμένα επαγγέλματα π.χ. για αποφυγή πρόσληψης, σε σχολεία, ατόμων που καταδικάστηκαν για αδικήματα σεξουαλικής φύσης / ατόμων που καταδικάστηκαν για ξέπλυμα βρώμικου χρήματος σε τράπεζα
- Πλήρες ποινικό μητρώο τηρείται μόνο υπό τον έλεγχο επίσημης αρχής

Ενδυνάμωση Δικαιωμάτων

- **Δικαίωμα ενημέρωσης** (Right to be provided with information) (Άρθρα 12 - 14)

Η ενημέρωση πρέπει να γίνεται σε συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση, ιδίως για πληροφορία απευθυνόμενη σε παιδιά

- Αυστηρότερες προϋποθέσεις για παροχή συγκατάθεσης τόσο σε ενήλικους (Άρθρα 6, 7) όσο και σε παιδιά (Άρθρο 8)

- **Δικαίωμα πρόσβασης** (Right of access) (Άρθρο 15)

Το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης σε δεδομένα και πληροφορίες που το αφορούν, τις οποίες το ίδιο το υποκείμενο των δεδομένων ή άλλο πρόσωπο έδωσε στον υπεύθυνο επεξεργασίας

- Πρόσβαση σε πληροφορίες και για αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ

- Δικαίωμα παροχής αντιγράφου των προσωπικών δεδομένων, εφόσον δεν επηρεάζει δυσμενώς τα δικαιώματα άλλων προσώπων

- **Δικαίωμα διόρθωσης** (Right to rectification) (Άρθρο 16, Αιτ. Σκέψη 65)

  Το υποκείμενο έχει δικαίωμα να ζητήσει τη διόρθωση των ανακριβών δεδομένων που το αφορούν, χωρίς αδικαιολόγητη καθυστέρηση
  Δικαίωμα συμπλήρωσης ελλιπών προσωπικών δεδομένων, μεταξύ άλλων, μέσω συμπληρωματικής δήλωσης

- **Δικαίωμα διαγραφής «Δικαίωμα στη λήθη»** (Right to erasure – 'right to be forgotten') (Άρθρο 17)

➢ **Το υποκείμενο των δεδομένων έχει δικαίωμα διαγραφής των δεδομένων** όταν:

- δεν είναι πλέον απαραίτητα για τον σκοπό επεξεργασίας, ή
- ανακλήθηκε η συγκατάθεση από το υποκείμενο, ή
- το υποκείμενο αντιτίθεται στην επεξεργασία (Άρθρο 21), ή
- υπήρξε παράνομη επεξεργασία, ή
- υπάρχει νομική υποχρέωση του υπεύθυνου επεξεργασίας, ή
- συλλέχθηκαν κατόπιν συγκατάθεσης δεδομένα παιδιού στα πλαίσια υπηρεσίας της κοινωνίας της πληροφορίας (Άρθρο 8 § 1)

- Εάν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα, έχει υποχρέωση να ενημερώσει όλους όσους τα έχουν αναδημοσιεύσει ότι το υποκείμενο ζήτησε τη διαγραφή τους

- **Το δικαίωμα διαγραφής (λήθη) ΔΕΝ εφαρμόζεται όταν:**

- Ισχύει ελευθερία έκφρασης και πληροφόρησης π.χ. το κοινό έχει ενδιαφέρον να γνωρίζει για ένα έγκλημα που είναι σε εξέλιξη
- Υπάρχει υποχρέωση από νόμο ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας
- Για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας
- Για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς
- Για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων

Το δικαίωμα διαγραφής (δικαίωμα στη λήθη) αφορά και στη διαγραφή δεδομένων στο διαδίκτυο
π.χ. από αποτελέσματα μηχανών αναζήτησης όπως Google και από μέσα κοινωνικής δικτύωσης όπως Facebook, Twitter και LinkedIn

Προστατεύει την ιδιωτική ζωή του ατόμου από τις συνέπειες του διαδικτύου που «δεν ξεχνά ποτέ»: ένα σφάλμα δεν πρέπει να στιγματίσει το άτομο για το υπόλοιπο της ζωής του

Παραδείγματα:

1. Το υποκείμενο μπορεί να ζητήσει τη διαγραφή από το διαδίκτυο περιεχομένου που το αφορά, το οποίο δημοσιεύτηκε σε κοινωνικό δίκτυο όταν ήταν παιδί και δεν είχε πλήρη επίγνωση των κινδύνων του διαδικτύου
2. Το υποκείμενο μπορεί να ζητήσει τη διαγραφή από το διαδίκτυο οδυνηρών και δυσάρεστων υποθέσεων του παρελθόντος του
3. Το υποκείμενο μπορεί να ζητήσει την απομάκρυνση ενός βίντεο σεξουαλικού περιεχομένου που τον θίγει
4. Δικαστήριο της Ευρωπαϊκής Ένωσης: Υπόθεση **Google Spain** SL και Google Inc. κατά Agencia Española de Protección de Datos (AEPD) και Mario Costeja González (C-131/12)

- **Δικαίωμα περιορισμού** (Right to restriction) (Άρθρο 18)

  Στην Οδηγία προϋπήρχε ο «περιορισμός» ως **προσωρινό «κλείδωμα» των δεδομένων**

  Μέθοδοι περιορισμού της επεξεργασίας είναι:

  (α) η προσωρινή μετακίνηση επιλεγμένων δεδομένων σε άλλο σύστημα,

  (β) η αφαίρεση της προσβασιμότητας των επιλεγμένων δεδομένων από τους χρήστες,

  (γ) η προσωρινή αφαίρεση δημοσιευμένων δεδομένων από ιστοσελίδα

  Σε συστήματα αυτοματοποιημένης αρχειοθέτησης:

  - Ο περιορισμός διασφαλίζεται με τεχνικά μέσα έτσι ώστε τα δεδομένα να μην υπόκεινται σε περαιτέρω επεξεργασία και να μην μπορούν να αλλάξουν
  - Αναγράφεται στο σύστημα ότι η επεξεργασία είναι περιορισμένη

Μπορεί να ασκηθεί όταν:

- το άτομο αμφισβητεί την ακρίβεια των δεδομένων του και ζητά να περιοριστεί η επεξεργασία μέχρι ο υπεύθυνος επεξεργασίας να επαληθεύσει την ακρίβεια τους, ή
- η επεξεργασία είναι παράνομη και το άτομο ζητά να περιοριστούν τα δεδομένα του αντί να διαγραφούν, ή
- τα δεδομένα δεν είναι πλέον απαραίτητα αλλά ζητούνται από το υποκείμενο για νομική αξίωση, ή
- το άτομο εναντιώνεται στην επεξεργασία (Άρθρο 21) και ζητά τον περιορισμό της επεξεργασίας εν αναμονή της επαλήθευσης του κατά πόσο οι λόγοι του υπεύθυνου επεξεργασίας υπερισχύουν έναντι των δικών του

Όταν γίνει περιορισμός, επεξεργασία, εκτός της αποθήκευσης, επιτρέπεται μόνο με συγκατάθεση ή για νομική αξίωση ή για την προστασία δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους δημοσίου συμφέροντος

Παράδειγμα: φυσικό πρόσωπο ισχυρίζεται ότι είναι παράνομη η αποστολή διαφημιστικού μηνύματος από εμπορικό κατάστημα. Αντί να ζητήσει τη διαγραφή τους ζητά τον προσωρινό περιορισμό τους

- **Δικαίωμα στη φορητότητα των δεδομένων** (Right to data portability) (Άρθρο 20)

  Είναι το δικαίωμα του υποκειμένου των δεδομένων να λαμβάνει τα προσωπικά δεδομένα που το αφορούν και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε ψηφιακή μορφή (σε δομημένη, κοινώς χρησιμοποιούμενη και αναγνώσιμη από μηχανήματα μορφή) και να αποθηκεύει τα δεδομένα αυτά για περαιτέρω δική του χρήση ή να διαβιβάζονται, χωρίς αντίρρηση, σε άλλον υπεύθυνο επεξεργασίας

  Η αποθήκευση μπορεί να γίνεται σε ιδιωτική συσκευή ή ιδιωτικό υπολογιστικό σύννεφο, χωρίς, κατ' ανάγκη, διαβίβαση των δεδομένων σε άλλον υπεύθυνο επεξεργασίας

  Η φορητότητα των δεδομένων δεν μπορεί να χρησιμοποιείται από τον υπεύθυνο επεξεργασίας ως δικαιολογία για την καθυστέρηση ή την άρνηση της διαγραφής (Άρθρο 17)

Το δικαίωμα φορητότητας εφαρμόζεται όταν:

- ✓ η επεξεργασία είναι αυτοματοποιημένη ΚΑΙ
- ✓ το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεση του για την επεξεργασία ή η επεξεργασία βασίζεται σε σύμβαση ΚΑΙ
- ✓ τα προσωπικά δεδομένα έχουν δοθεί στον υπεύθυνο επεξεργασίας από το <u>ίδιο</u> το άτομο, αφορούν στο ίδιο ΚΑΙ
- ✓ δεν επηρεάζονται δυσμενώς τα δικαιώματα και οι ελευθερίες άλλων (π.χ. εμπορικά μυστικά, πνευματική ιδιοκτησία, ιδίως δημιουργού λογισμικού)

Το δικαίωμα φορητότητας ΔΕΝ εφαρμόζεται 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 (Αιτ. Σκέψη 68)

Στο πεδίο αιτήματος φορητότητας εμπίπτουν:

- Τα ψευδώνυμα δεδομένα τα οποία μπορούν να συνδεθούν αδιαμφισβήτητα με υποκείμενο των δεδομένων
- Δεδομένα που σχετίζονται με τη δραστηριότητα του υποκειμένου ή προέρχονται από την παρατήρηση της συμπεριφοράς του

Στο πεδίο αιτήματος φορητότητας ΔΕΝ εμπίπτουν:

- Δεδομένα που προκύπτουν από τη μετέπειτα ανάλυση της συμπεριφοράς
- Δεδομένα τα οποία δημιουργεί ο υπεύθυνος επεξεργασίας στο πλαίσιο της επεξεργασίας των δεδομένων π.χ. μέσω διαδικασίας εξατομίκευσης (customisation), δηλαδή αποτελούν δεδομένα που παράγονται ή συνάγονται από τα δεδομένα που παρέχει το υποκείμενο των δεδομένων

Στα δεδομένα που παρέχει το υποκείμενο των δεδομένων περιλαμβάνονται τα δεδομένα προσωπικού χαρακτήρα που παρατηρούνται από τις δραστηριότητες των χρηστών όπως, π.χ., μη επεξεργασμένα δεδομένα που υποβάλλονται σε επεξεργασία από έξυπνο μετρητή ή άλλα είδη συνδεδεμένων αντικειμένων, αρχεία καταγραφής δραστηριοτήτων, το ιστορικό χρήσης δικτυακών τόπων ή το ιστορικό αναζητήσεων [wp242rev01]

Το δικαίωμα στη φορητότητα δεν συνεπάγεται αυτόματη διαγραφή των δεδομένων από το σύστημα του υπεύθυνου επεξεργασίας

Το υποκείμενο των δεδομένων μπορεί να ζητήσει τη διαγραφή δεδομένων που το αφορούν και μετά την άσκηση του δικαιώματος της φορητότητας

Παραδείγματα δικαιώματος φορητότητας:

- **Οι χρήστες θα μπορούν να μεταφέρουν τα δεδομένα τους από μια ιστοσελίδα κοινωνικής δικτύωσης σε άλλη**
- **Οι ασφαλιζόμενοι από μια ασφαλιστική εταιρεία σε άλλη**
- Άτομα θα μπορούν να ανακτήσουν τον κατάλογο επαφών τους από την εφαρμογή webmail που χρησιμοποιούν, π.χ. με σκοπό την κατάρτιση του καταλόγου των καλεσμένων σε έναν γάμο
- Άτομα θα μπορούν να λάβουν και να μεταφέρουν δεδομένα κίνησης και θέσης

Ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίζει ότι:

- τα δεδομένα διαβιβάζονται με ασφάλεια (μέσω κρυπτογράφησης)
- τα δεδομένα διαβιβάζονται στον σωστό προορισμό (μέσω αξιόπιστων μέτρων επαλήθευσης ταυτότητας),
- τα δεδομένα που παραμένουν στο σύστημά του είναι προστατευμένα
- θεσπίζει διαφανείς διαδικασίες για την αντιμετώπιση πιθανών παραβιάσεων δεδομένων

Ο παραλήπτης υπεύθυνος επεξεργασίας πρέπει να περιορίζει την επεξεργασία στα δεδομένα που είναι συναφή και αναγκαία για τους νέους σκοπούς και να διαγράφει το ταχύτερο δυνατό τα μη αναγκαία

Όταν υπάρχουν διάφοροι μορφότυποι, πρέπει να επιλέγονται με στόχο την επίτευξη της διαλειτουργικότητας και την παροχή στο υποκείμενο των δεδομένων ενός υψηλού βαθμού φορητότητας

Το δικαίωμα της φορητότητας ασκείται δωρεάν *(εκτός αν ασκείται προδήλως αβάσιμα ή υπερβολικά, ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα των αιτημάτων)*

Μέσα σε ένα μήνα από την παραλαβή του αιτήματος φορητότητας, ο υπεύθυνος επεξεργασίας οφείλει

- **Να ικανοποιήσει το αίτημα** ή
- Να ενημερώσει το υποκείμενο ότι θα καθυστερήσει (έως τρεις μήνες από την παραλαβή) να ικανοποιήσει το αίτημα ή
- Να ενημερώσει το υποκείμενο ότι δεν θα ικανοποιήσει το αίτημα, τους λόγους για αυτό, και ότι το υποκείμενο των δεδομένων έχει δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή και άσκησης δικαστικής προσφυγής

Ο υπεύθυνος επεξεργασίας δεν μπορεί να σιωπά όταν καλείται να απαντήσει σε αίτημα φορητότητας δεδομένων

- **Δικαίωμα εναντίωσης** (Right to object) (Άρθρο 21)

Το υποκείμενο έχει το δικαίωμα να εναντιωθεί στην επεξεργασία προσωπικών του δεδομένων, μόνο όταν:

(α) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, ή
(β) η επεξεργασία είναι απαραίτητη για εξυπηρέτηση του έννομου συμφέροντος του υπεύθυνου επεξεργασίας ή τρίτου, ή
(γ) γίνεται επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, ή
(δ) η επεξεργασία γίνεται για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

Στο πλαίσιο της χρήσης υπηρεσιών της κοινωνίας της πληροφορίας, η εναντίωση μπορεί να ασκηθεί και με αυτοματοποιημένα μέσα

Σταματά η επεξεργασία μετά την εναντίωση, εκτός αν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς νόμιμους λόγους για την επεξεργασία ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων

Αν η επεξεργασία εκτελείται για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, η εναντίωση δεν μπορεί να ασκηθεί εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος

- **Δικαίωμα εναντίωσης σε αυτοματοποιημένη απόφαση περιλαμβανομένης της κατάρτισης προφίλ** (Right to object to automated decision-making, including profiling) (Άρθρο 22)

➢ Το υποκείμενο των δεδομένων έχει δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται με αυτοματοποιημένα μέσα, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά

Ο υπεύθυνος επεξεργασίας πρέπει να εξασφαλίζει ότι ενημέρωσε το υποκείμενο για την ύπαρξη, τον τρόπο σύστασης προφίλ και τον τρόπο λήψης αυτοματοποιημένης απόφασης (Άρθρο 13 και 14) [wp251rev01 D.1]

Το δικαίωμα εναντίωσης ισχύει και για απόφαση που λαμβάνεται με μερικώς αυτοματοποιημένα μέσα [wp251rev01 D.1]

π.χ. το υποκείμενο δικαιούται να αντιταχθεί

σε αυτοματοποιημένη επεξεργασία για την απόφαση χορήγησης δανείου, η οποία λαμβάνεται αυτοματοποιημένα ή

για δοκιμασία επάρκειας πρόσληψης που χρησιμοποιεί προεπιλεγμένους αλγορίθμους και κριτήρια

ΔΕΝ μπορεί να ασκηθεί το δικαίωμα, όταν η απόφαση:

(α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης* , ή

(β) επιτρέπεται από νόμο, π.χ. για την πάταξη της απάτης και της φοροδιαφυγής, ή

(γ) βασίζεται σε ρητή συγκατάθεση*

** ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, ελευθεριών και έννομων συμφερόντων του υποκειμένου των δεδομένων, τουλάχιστον του δικαιώματος εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης*

- **Η λήψη αυτοματοποιημένης απόφασης βάσει δεδομένων ειδικών κατηγοριών επιτρέπεται μόνο αν η επεξεργασία τους βασίστηκε στη ρητή συγκατάθεση ή είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος**

  π.χ. Δημόσια αρχή δικαιούται να λάβει αυτοματοποιημένη απόφαση για αιτούντες επίδομα βάσει των πληροφοριών που έδωσαν (περιλαμβανομένων των δεδομένων υγείας π.χ. ανικανότητα για εργασία, ψυχολογική υγεία)

Υποχρέωση διορισμού Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)
(designation of a Data Protection Officer) (Άρθρα 37-39)

Πότε υπάρχει υποχρέωση διορισμού ΥΠΔ;

- **Όταν η επεξεργασία εκτελείται από δημόσια αρχή ή φορέα** (συμπεριλαμβανομένων των ΝΠΔΔ), εκτός από τα δικαστήρια, όταν ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας, ή
- **Όταν οι βασικές δραστηριότητες επεξεργασίας απαιτούν**

  τακτική και συστηματική **παρακολούθηση** των υποκειμένων **σε μεγάλη κλίμακα** ή

  μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων **ή** δεδομένων προσωπικού χαρακτήρα που αφορούν **ποινικές καταδίκες και αδικήματα**

Μεγάλη κλίμακα:

- Επηρεάζεται μεγάλος αριθμός προσώπων (ως συγκεκριμένος αριθμός ή ως ποσοστό επί του συναφούς πληθυσμού), ή
- Γίνεται επεξεργασία μεγάλου όγκου ή εύρους δεδομένων, ή
- Γίνεται επεξεργασία δεδομένων για μεγάλη διάρκεια ή με μόνιμο χαρακτήρα, ή
- Η επεξεργασία καλύπτει μεγάλη γεωγραφική έκταση [wp243rev01 2.1.3]

Παραδείγματα μεγάλης κλίμακας

- Επεξεργασία δεδομένων ασθενών σε **νοσοκομείο/κλινική**
- Επεξεργασία δεδομένων πελατών **τράπεζας / ασφαλιστικής εταιρείας**
- Επεξεργασία δεδομένων (περιεχόμενο, κίνηση, θέση) από **παρόχους υπηρεσιών τηλεφωνίας ή διαδικτύου**
- Επεξεργασία δεδομένων μετακίνησης φυσικών προσώπων που χρησιμοποιούν το σύστημα δημόσιων μεταφορών μιας πόλης (π.χ. παρακολούθηση μέσω καρτών πολλαπλών διαδρομών)
- Εξωτερικός συνεργάτης διαχειρίζεται τη μισθοδοσία του προσωπικού ομίλου εταιριών

Παραδείγματα μεγάλης κλίμακας

- Επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς συμπεριφορικής διαφήμισης από μηχανή αναζήτησης
- Επεξεργασία οικονομικής – καταναλωτικής συμπεριφοράς με **κάρτες «επιβράβευσης** πίστης» (“loyalty cards”)
- Επεξεργασία σε πραγματικό χρόνο δεδομένων γεωγραφικού εντοπισμού πελατών διεθνούς αλυσίδας ταχυφαγείων για στατιστικούς σκοπούς από εκτελούντα την επεξεργασία που ειδικεύεται στην παροχή τέτοιου είδους υπηρεσιών

Σύμφωνα με τις «Κατευθυντήριες γραμμές σχετικά με τους Υπευθύνους Προστασίας Δεδομένων» της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ, στην έννοια της δημόσιας αρχής ή δημόσιου φορέα που υποχρεούται να ορίσει υπεύθυνο προστασίας δεδομένων εμπίπτουν και άλλα **φυσικά ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου που εκπληρώνουν δημόσια καθήκοντα ή ασκούν δημόσια εξουσία**, όπως υπηρεσίες δημοσίων μεταφορών, παροχής ενέργειας και ύδρευσης, οδικές υποδομές, δημόσια ραδιοτηλεόραση, κατασκευή εργατικών κατοικιών (π.χ. ΟΛΠ, ΣΤΑΣΥ, ΕΥΔΑΠ, ΔΕΔΔΗΕ, ΕΡΤ), **ή πειθαρχικά όργανα για νομοθετικά κατοχυρωμένα επαγγέλματα** (π.χ. Δικηγορικός Σύλλογος Καρδίτσας, Τεχνικό Επιμελητήριο Καρδίτσας, Ιατρικός Σύλλογος Καρδίτσας)

Η δραστηριότητα του ΥΠΔ καλύπτει όλες τις πράξεις επεξεργασίας που διενεργούνται, περιλαμβανομένων και όσων δεν σχετίζονται με την εκπλήρωση δημόσιου καθήκοντος ή άσκηση επίσημης αρμοδιότητας (π.χ. διαχείριση βάσης δεδομένων υπαλλήλων) [wp243rev01 2.1.1]

Ποια είναι τα καθήκοντα του ΥΠΔ (Άρθρο 39 παρ. 1);

- **Συμβουλεύει τη διεύθυνση για τα αναγκαία τεχνικά και οργανωτικά μέτρα που πρέπει να ληφθούν για συμμόρφωση με τον Κανονισμό**
- Συλλέγει πληροφορίες από τα διάφορα τμήματα για να αναγνωρίσει τις δραστηριότητες του οργανισμού (IT, Marketing, HR, νομικό κ.λ.π.)
- Ξεχωρίζει για ποιες δραστηριότητες ο Οργανισμός ενεργεί ως υπεύθυνος επεξεργασίας και για ποιες ως εκτελών την επεξεργασία
- Ξεχωρίζει ποιες δραστηριότητες του οργανισμού είναι «κύριες» και ποιες «παρεπόμενες» (Αιτιολογική Σκέψη 97)
- Βοηθά τη διεύθυνση να καταρτίσει και να επικαιροποιεί το αρχείο δραστηριοτήτων (σύμφωνα με το Άρθρο 30)
- **Αναλύει και ελέγχει κατά πόσο οι επεξεργασίες είναι σύμφωνες με τον Κανονισμό και ενημερώνει τη Διεύθυνση**
- Συμβουλεύει τη Διεύθυνση για τη σύνταξη πολιτικών ασφάλειας και προστασίας προσωπικών δεδομένων

- Προτείνει τη λήψη εσωτερικών διαδικασιών ελέγχου και επαλήθευσης της αποτελεσματικής εφαρμογής των μέτρων ελέγχου
- Συμβουλεύει τη Διεύθυνση όταν του ζητείται, για:

1. Το εάν πρέπει ή όχι να διενεργηθεί Εκτίμηση Αντικτύπου
2. Τη μεθοδολογία που θα ακολουθηθεί
3. Το κατά πόσο η Εκτίμηση Αντικτύπου θα διενεργηθεί από τον Οργανισμό ή τρίτο (outsourcing)
4. Τις δικλίδες ασφαλείας για μετριασμό του κινδύνου
5. Εάν διενεργήθηκε σωστά ή όχι η εκτίμηση αντικτύπου και εάν τα συμπεράσματά της είναι σύμφωνα με τις απαιτήσεις περί προστασίας δεδομένων
6. Το κατά πόσο πρέπει να γίνει διαβούλευση με την ΑΠΔΠΧ *(ελλείψει επαρκών μέτρων μετριασμού του κινδύνου)*

- **Εκπαιδεύει και συμβουλεύει το προσωπικό του οργανισμού για την ορθή εφαρμογή του Κανονισμού**
- **Ενεργεί ως μεσολαβητής μεταξύ των υποκειμένων των δεδομένων και του οργανισμού**
- **Συνεργάζεται με την ΑΠΔΠΧ**

Ποια είναι τα προσόντα του ΥΠΔ (Άρθρο 37 παρ. 5);

- **Εμπειρογνωσία στο δίκαιο προστασίας προσωπικών δεδομένων και στις πρακτικές περί προστασίας δεδομένων** ανάλογα με
  - τις πράξεις επεξεργασίας δεδομένων
  - τον βαθμό απαιτούμενης προστασίας
- Ικανότητα εκπλήρωσης των καθηκόντων του (Αιτ. Σκέψη 97)
- **Να εκτελεί τα καθήκοντα του με ανεξάρτητο τρόπο**
- Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι **μέλος του προσωπικού** του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία **ή** να ασκεί τα καθήκοντά του **βάσει σύμβασης παροχής υπηρεσιών**

Κατά την εκτέλεση των καθηκόντων του ο ΥΠΔ (Άρθρο 38)

- **Λαμβάνει μέρος τακτικά στις συναντήσεις των ανώτερων και μεσαίων στελεχών διοίκησης**
- **Συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων**
- **Η γνώμη του έχει τη δέουσα βαρύτητα στις αποφάσεις που έχουν αντίκτυπο στην προστασία προσωπικών δεδομένων**: καταγραφή από τη διοίκηση των λόγων απόκλισης από τις συμβουλές
- **Του παρέχεται ικανοποιητικός χρόνος, η κατάλληλη υποδομή και απαραίτητοι οικονομικοί πόροι**
- Έχει ελεύθερη πρόσβαση σε κάθε είδους δεδομένα και λαμβάνει μέρος σε κάθε σχεδιαζόμενη πράξη επεξεργασίας από την αρχή
- Έχει πρόσβαση σε άλλα τμήματα, όπως π.χ. το τμήμα ανθρωπίνων πόρων, το τμήμα ασφάλειας, νομικό τμήμα, τμήμα πληροφορικής
- **Ενεργεί ως σημείο επικοινωνίας με την ΑΠΔΠΧ**, ιδίως για τις Εκτιμήσεις Αντικτύπου

- Δεσμεύεται με την **τήρηση απορρήτου** / εμπιστευτικότητας
- **Δεν λαμβάνει εντολές** για την άσκηση καθηκόντων του
- **Δεν απολύεται, ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του**. π.χ. εάν μία επεξεργασία ενέχει υψηλό κίνδυνο και ο ΥΠΔ συμβουλεύσει τον υπεύθυνο επεξεργασίας για τη διενέργεια Εκτίμησης Αντικτύπου αλλά η διοίκηση διαφωνήσει, ο ΥΠΔ δεν θα απολυθεί. Απολύεται για άλλους λόγους π.χ. κλοπή, ανάρμοστη συμπεριφορά, άσκηση ψυχολογικής βίας κ.λπ.
- **Λογοδοτεί απευθείας στο ανώτατο επίπεδο της διοίκησης**
- Έχει ως προτεραιότητα τα καθήκοντά του ως ΥΠΔ και δεν αναλαμβάνει άλλα καθήκοντα που έρχονται σε σύγκρουση συμφέροντος με τα καθήκοντά του
- Τα υποκείμενα δεδομένων **επικοινωνούν απευθείας μαζί του**
- **Δεν φέρει προσωπική ευθύνη** για μη συμμόρφωση με τις απαιτήσεις του Κανονισμού στην προστασία των δεδομένων

Σύγκρουση συμφέροντος στα καθήκοντα που εκτελεί υπάρχει όταν:

Ο ΥΠΔ κατέχει μία θέση στον Οργανισμό, με την οποία μπορεί να καθορίσει το σκοπό και τα μέσα της επεξεργασίας προσωπικών δεδομένων π.χ. ---wp p32

- Γενικός Διευθυντής, Προϊστάμενος Τμήματος Πληροφορικής / Ανθρώπινου Δυναμικού / Οικονομικός Διευθυντής / Αρχίατρος
- Κατώτερες θέσεις, των οποίων οι κάτοχοι είναι δυνατό να καθορίσουν το σκοπό και τα μέσα της επεξεργασίας προσωπικών δεδομένων
- Σημ.: Ο Υπεύθυνος Ασφάλειας Πληροφοριών είναι ξεχωριστή θέση από τον ΥΠΔ *(Κατευθυντήριες Γραμμές Ομάδας Εργασίας Άρθρου 29 για τη Διενέργεια Εκτίμησης Αντικτύπου)*

Δημοσίευση και ανακοίνωση των στοιχείων επικοινωνίας του ΥΠΔ

Ο Οργανισμός δημοσιεύει τα στοιχεία επικοινωνίας του ΥΠΔ και τα ανακοινώνει στην ΑΠΔΠΧ.

Η Ομάδα Εργασίας του Άρθρου 29 προτείνει:

- Πληροφορίες που αφορούν στον ΥΠΔ (ταχ. διεύθυνση, υπηρεσιακό τηλ. και/ή email) δημοσιεύονται στην ιστοσελίδα του Οργανισμού. Η δημοσίευση του ονόματος εναπόκειται στην κρίση του Οργανισμού και του ΥΠΔ
- Οι εν λόγω πληροφορίες (ΚΑΙ το όνομά του) δημοσιεύονται στην εσωτερική σελίδα του Οργανισμού
- Όλες οι πιο πάνω πληροφορίες ανακοινώνονται στην ΑΠΔΠΧ

Δικηγορικός Σύλλογος Καρδίτσας

Τηλ: 2441021646

E-mail: dskarditsas@gmail.com

www.dskard.gr

Δημήτρης Τζέλλης

Δικηγορικός Σύλλογος Καρδίτσας

GDPR και DPO:
Γενικός Κανονισμός για την Προστασία Δεδομένων
και
Υπεύθυνος Προστασίας Δεδομένων

Μέρος 2ο (Υποχρεώσεις – Καλές πρακτικές) Ιούλιος 2018

Αυστηρότατες Υποχρεώσεις Υπεύθυνου Επεξεργασίας

1. Φέρει το βάρος της απόδειξης όσον αφορά στην παροχή συγκατάθεσης (Άρθρο 7)

Η δήλωση συγκατάθεσης για επεξεργασία προσωπικών δεδομένων πρέπει να είναι διατυπωμένη σε απλή και κατανοητή γλώσσα

Ο υπεύθυνος επεξεργασίας πρέπει να αποδείξει ότι έλαβε τη συγκατάθεση του ατόμου

Το άτομο μπορεί να ανακαλέσει τη συγκατάθεση του ανά πάσα στιγμή

2. Λήψη συγκατάθεσης για ανήλικους κάτω των 16 σε σχέση με τις υπηρεσίες της κοινωνίας της πληροφορίας (Άρθρο 8)

Όταν προσφέρεται μία υπηρεσία της κοινωνίας της πληροφορίας απευθείας σε παιδί κάτω των 16 ετών, δεν αρκεί η συγκατάθεσή του για την επεξεργασία προσωπικών του δεδομένων αλλά χρειάζεται και η συγκατάθεση του γονέα / κηδεμόνα του

3. Εφαρμογή μέτρων προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (privacy by default and by design) (Άρθρο 25)

- Κατά τον αρχικό σχεδιασμό κάθε υπηρεσίας ή προϊόντος, ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα (τεχνολογία και διαδικασίες):
  - όπως η ψευδωνυμοποίηση των δεδομένων
  - σχεδιασμένα με τρόπο που να εφαρμόζονται οι αρχές προστασίας προσωπικών δεδομένων π.χ. ελαχιστοποίηση *(όσον αφορά το εύρος των δεδομένων, το βαθμό της επεξεργασίας, την προσβασιμότητα και την αποθήκευση)*
  - σχεδιασμένα ώστε να προάγουν τη διαφάνεια όσον αφορά στην επεξεργασία, με τρόπο που τα άτομα να μπορούν να παρακολουθούν την επεξεργασία και ο οργανισμός να δημιουργεί και να βελτιώνει τα μέτρα ασφαλείας
- Εγκεκριμένος μηχανισμός πιστοποίησης (άρθρο 42) αποδεικνύει τη συμμόρφωση με τις εν λόγω απαιτήσεις (Αιτ. Σκέψη 78)

- **Παράδειγμα:** οι κατασκευαστές έξυπνων συσκευών διασφαλίζουν ότι διατηρείται η ανωνυμία των προσώπων που αγοράζουν τις συσκευές και οι σχεδιαστές εφαρμογών (applications) συλλέγουν πληροφορίες για τους χρήστες, μόνο στον βαθμό που επιτρέπει ο Κανονισμός

4. Από κοινού υπεύθυνοι επεξεργασίας (Άρθρο 26)

- Μπορεί να υπάρχουν 2 ή περισσότεροι συν-υπεύθυνοι επεξεργασίας
- Καθορίζουν με μεταξύ τους συμφωνία και με διαφάνεια τις αντίστοιχες ευθύνες τους
- Η συμφωνία καθορίζει και τις ευθύνες τους για ικανοποίηση των δικαιωμάτων των υποκειμένων
- Η ουσία της συμφωνίας τίθεται στη διάθεση του υποκειμένου
- Στη συμφωνία δύναται να αναφέρεται ένα σημείο επικοινωνίας
- Το υποκείμενο μπορεί να ασκήσει τα δικαιώματα του σε κάθε υπεύθυνο επεξεργασίας

5. Υποχρέωση εκπροσώπησης υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση (Άρθρο 27)

- Υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία που ΔΕΝ είναι εγκατεστημένος στην ΕΕ ορίζει γραπτώς εκπρόσωπο του στην ΕΕ, που ενεργεί κατ' εντολή του υπεύθυνου/ εκτελούντα
- Ο εκπρόσωπος ενεργεί ως σημείο επαφής με την ΑΠΔΠΧ και με υποκείμενα των δεδομένων (one stop shop)
- ΔΕΝ ορίζεται εκπρόσωπος όταν:

  (α) η επεξεργασία είναι περιστασιακή, δεν περιλαμβάνει, σε μεγάλο βαθμό, επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα

  (β) η επεξεργασία εκτελείται από δημόσια αρχή ή φορέα
- Ο εκπρόσωπος πρέπει να είναι εγκατεστημένος σε Κράτος Μέλος όπου βρίσκονται τα υποκείμενα των δεδομένων, των οποίων επεξεργάζεται τα δεδομένα τους (για προσφορά αγαθών ή υπηρεσιών ή των οποίων παρακολουθεί τη συμπεριφορά τους)

6. Επιλογή εκτελούντων την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων (Άρθρο 28)

- Η σχετική **ανάθεση γίνεται ΥΠΟΧΡΕΩΤΙΚΑ ΓΡΑΠΤΩΣ**
- Επιλογή του κατάλληλου εκτελούντος την επεξεργασία ο οποίος θα πρέπει να παρέχει εχέγγυα απορρήτου και ασφάλειας των δεδομένων γίνεται με ιδιαίτερη μέριμνα
- Εκτελών την επεξεργασία που επεξεργάζεται τα δεδομένα για δικούς του σκοπούς καθίσταται υπεύθυνος επεξεργασίας

7. Τήρηση αρχείου των δραστηριοτήτων επεξεργασίας (record of processing activities) (Άρθρο 30)

- Ο υπεύθυνος επεξεργασίας και ο εκτελών **έχουν υποχρέωση να τηρούν εγγράφως ή ηλεκτρονικά** αρχείο δραστηριοτήτων
- Η τήρηση του αρχείου καταγραφής των δραστηριοτήτων επεξεργασιών είναι υποχρεωτική όταν:

  (α) ο οργανισμός απασχολεί πάνω από 250 άτομα

  (β) όταν η επεξεργασία δημιουργεί κινδύνους για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων

  (γ) η επεξεργασία δεν είναι περιστασιακή

  (δ) η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων ή ποινικές καταδίκες και αδικήματα

- Οι πληροφορίες στο εν λόγω αρχείο είναι αντίστοιχες με αυτές που περιλαμβάνει το προηγούμενο έντυπο Γνωστοποίησης
- Το αρχείο τίθεται στη διάθεση της ΑΠΔΠΧ κατόπιν αιτήματός της για άσκηση των αρμοδιοτήτων της

8. Υποχρέωση τήρησης της ασφάλειας της επεξεργασίας (security of processing) (Άρθρο 32)

- Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία αξιολογεί τους κινδύνους της επεξεργασίας και εφαρμόζει μέτρα για τον μετριασμό τους π.χ. μέσω κρυπτογράφησης

- Γίνεται εκτίμηση του ενδεδειγμένου επιπέδου ασφαλείας, λαμβάνοντας υπόψη τους κινδύνους που απορρέουν από την επεξεργασία (π.χ. από παράνομη καταστροφή, απώλεια κ.λ.π.)

- Η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης είναι στοιχείο συμμόρφωσης

9. Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας στην Αρχή (**notification of a personal data breach**) (Άρθρο 33)

- Ο υπεύθυνος επεξεργασίας σε περίπτωση παραβίασης προσωπικών δεδομένων γνωστοποιεί την παραβίαση **στην ΑΠΔΠΧ**, **αμέσως** και όχι πέραν των **72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος, εκτός αν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο. Μετά τις 72 ώρες, λογοδοτεί στην ΑΠΔΠΧ

- Ο εκτελών ενημερώνει τον υπεύθυνο επεξεργασίας μόλις αντιληφθεί παραβίαση

- Η γνωστοποίηση περιλαμβάνει τουλάχιστον:
  (α) τη φύση της παραβίασης και αριθμό των επηρεαζόμενων
  (β) στοιχεία επικοινωνίας ΥΠΔ ή άλλου για πληροφορίες
  (γ) ενδεχόμενες συνέπειες της παραβίασης
  (δ) ληφθέντα ή προτεινόμενα μέτρα

- Οι πληροφορίες μπορούν να παρέχονται στην ΑΠΔΠΧ σταδιακά, χωρίς όμως καθυστέρηση

10. Υποχρέωση ανακοίνωσης παραβιάσεων ασφάλειας (communication of a personal data breach) (Άρθρο 34)

- Η παραβίαση ανακοινώνεται αμέσως **στο επηρεαζόμενο άτομο** όταν υπάρχει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες του

- Περιγράφεται η φύση της παραβίασης και τα ληφθέντα μέτρα

- Η ανακοίνωση δεν απαιτείται, εάν:

  (α) είχαν ήδη εφαρμοστεί κατάλληλα μέτρα προστασίας στα δεδομένα που αφορά η παραβίαση όπως π.χ. κρυπτογράφηση

  (β) λήφθηκαν στη συνέχεια μέτρα που διασφαλίζουν ότι δεν υπάρχει κίνδυνος πλέον

  (γ) προϋποθέτει δυσανάλογες προσπάθειες (γίνεται όμως δημόσια ανακοίνωση ή παρόμοιο μέτρο για ενημέρωση των επηρεαζόμενων προσώπων)

- Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων στο επηρεαζόμενο άτομο, η ΑΠΔΠΧ μπορεί να του ζητήσει να το πράξει ή μπορεί να αποφασίσει ότι πληρούται οποιαδήποτε από τις εξαιρέσεις

11. Εκτίμηση Αντικτύπου (ΕΑ) (Impact Assessment - DPIA) (Άρθρο 35) **και Προηγούμενη Διαβούλευση** (Άρθρο 36)

- Σημαντικό εργαλείο συμμόρφωσης με την Αρχή της Λογοδοσίας
- Εντοπίζει τους κινδύνους της επεξεργασίας και καθορίζει τα μέτρα που θα ληφθούν για αντιμετώπιση/ελαχιστοποίηση τους

- **Διενεργείται από τον υπεύθυνο επεξεργασίας με τη βοήθεια/συμβουλή του ΥΠΔ:**

- Δεν απαιτείται σε κάθε πράξη επεξεργασίας **αλλά μόνο όταν υπάρχει υψηλός κίνδυνος (ιδίως με τη χρήση νέων τεχνολογιών) για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων** *(περιλαμβανομένων και επεξεργασιών πριν τις 25-05-2018, δεδομένου ότι, ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων. Π.χ. χρησιμοποιείται πλέον μια νέα τεχνολογία ή επειδή τα προσωπικά δεδομένα χρησιμοποιούνται για διαφορετικό σκοπό*
- Πριν από την επεξεργασία **(δηλ. στο σχεδιασμό της πράξης επεξεργασίας)** και ενημερώνεται κάθε φορά που αλλάζει ο κίνδυνος ή κάθε 3 χρόνια

- Εάν η επεξεργασία εν όλω ή εν μέρει εκτελείται **από εκτελούντα την επεξεργασία**, ο εκτελών την επεξεργασία θα πρέπει να συνδράμει τον υπεύθυνο επεξεργασίας στη διενέργεια της ΕΑ και να παράσχει κάθε αναγκαία πληροφορία

- Όπου ενδείκνυται, **ζητείται η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους** για τη σχεδιαζόμενη επεξεργασία

  π.χ. μέσω (α) μελέτης/έρευνας σχετικά με το σκοπό και τα μέσα της επεξεργασίας, (β) γραπτού ερωτήματος προς τις συνδικαλιστικές οργανώσεις, (γ) ερωτηματολόγιου προς τους πελάτες του υπεύθυνου επεξεργασίας

- Εάν η τελική απόφαση του υπεύθυνου επεξεργασίας διαφέρει από τις απόψεις των υποκειμένων των δεδομένων ή δεν έχει ζητηθεί καν γνώμη των υποκειμένων (*π.χ. κάτι τέτοιο θα διακινδύνευε την εμπιστευτικότητα των επιχειρηματικών σχεδίων της εταιρείας*), τότε οι λόγοι για τη συνέχιση της επεξεργασίας θα πρέπει να τεκμηριώνονται γραπτώς

- Στο πλαίσιο της αρχής της λογοδοσίας, ο υπεύθυνος επεξεργασίας τηρεί «αρχείο των δραστηριοτήτων επεξεργασίας» και πρέπει να αξιολογεί αν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο
  <250 εργαζόμενοι: Αρχεία επεξεργασιών με διακινδύνευση
  >= 250 εργαζόμενοι: Εσωτερικά αρχεία κάθε επεξεργασίας
- Ο υπεύθυνος επεξεργασίας είναι αρμόδιος να **επιλέξει τη μεθοδολογία της Εκτίμησης Αντικτύπου** (*παραδείγματα παρατίθενται στο Παράρτημα 1 των Κατευθυντήριων Γραμμών της Ομάδας Εργασίας του Άρθρου 29 για τη διενέργεια ΕΑ*), **η οποία θα πρέπει να συνάδει με τα κριτήρια του Παραρτήματος 2 των εν λόγω Κατευθυντήριων Γραμμών**
- Ο υπεύθυνος επεξεργασίας αποφασίζει κατά πόσο θα δημοσιεύσει την ΕΑ – η δημοσίευση μιας σύνοψης θα μπορούσε να προαγάγει την εμπιστοσύνη και διαφάνεια

- **Επεξεργασίες που ενδέχεται να επιφέρουν υψηλό κίνδυνο:**

- συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία λαμβάνονται αποφάσεις που επηρεάζουν σημαντικά το φυσικό πρόσωπο
- επεξεργασία που μπορεί να δημιουργήσει διακρίσεις
- διαβιβάσεις δεδομένων εκτός ΕΕ
- συστηματική παρακολούθηση δημόσιων χώρων σε **μεγάλη κλίμακα***

  * *ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού, όγκος δεδομένων, διάρκεια, γεωγραφική έκταση, ειδικές κατηγορίες δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα*

Παραδείγματα επεξεργασιών που επιφέρουν υψηλό κίνδυνο: Αξιολόγηση (Scoring)

- Τράπεζα που αξιολογεί / ελέγχει τους πελάτες της σε σχέση με μια βάση δεδομένων πιστοληπτικής ικανότητας ή μια βάση δεδομένων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας
- Εταιρεία συλλέγει δεδομένα από προφίλ κοινωνικής δικτύωσης που είναι δημόσια διαθέσιμα με σκοπό τη δημιουργία προφίλ για καταλόγους επαφών
- Εταιρεία βιοτεχνολογίας που προσφέρει γενετικές εξετάσεις απευθείας στους καταναλωτές προκειμένου να αξιολογήσει και να προβλέψει τους κινδύνους για την ασθένεια ή την υγεία
- Εταιρεία που καταρτίζει προφίλ συμπεριφοράς ή μάρκετινγκ βασισμένο στη χρήση ή πλοήγηση των ατόμων στην ιστοσελίδα της

Συστηματική παρακολούθηση

- Εταιρεία που παρακολουθεί τους εργοδοτούμενους: emails, πλοήγηση στο διαδίκτυο, ώρα προσέλευσης/αποχώρησης
- Drones ή ΚΚΒΠ (Κλειστά Κυκλώματα Βίντεο-Παρακολούθησης) σε δημόσιους / ιδιωτικούς χώρους

Ειδικές κατηγορίες προσωπικών δεδομένων

- Νοσοκομείο / κλινική που επεξεργάζεται γενετικά δεδομένα και δεδομένα υγείας των πελατών του
- Εταιρεία που σχεδιάζει λογισμικά για ιατρούς και νοσοκομεία/ κλινικές

Ευάλωτες κατηγορίες ατόμων

- Παιδιά που δεν είναι σε θέση να αντιταχθούν ενσυνείδητα και αντικειμενικά στην επεξεργασία των δεδομένων τους
- Ευάλωτα τμήματα του πληθυσμού που χρήζουν ειδικής προστασίας π.χ. ψυχικά ασθενείς, αιτούντες ασύλου, ηλικιωμένοι

Χρήση νέων τεχνολογιών

- Χρήση δακτυλικών αποτυπωμάτων / αναγνώριση προσώπου για έλεγχο φυσικής πρόσβασης
- Χρήση συστήματος ανάλυσης βίντεο για αναγνώριση των πινακίδων κυκλοφορίας

Τι περιλαμβάνει η Εκτίμηση Αντικτύπου

- **Παραδείγματα επεξεργασιών που ενδεχομένως να μην απαιτείται Εκτίμηση Αντικτύπου:**
- Ιδιώτης δικηγόρος που επεξεργάζεται δεδομένα των πελατών του
- Ιδιώτης ιατρός που επεξεργάζεται δεδομένα των πελατών του (Κατευθυντήριες γραμμές ΟΕ29 WP243/05-04-2017, σελ. 11)

- Εταιρεία που δραστηριοποιείται στο ηλεκτρονικό εμπόριο, διαφημίζει στην ιστοσελίδα της περιορισμένες πληροφορίες καταναλωτών με βάση τις προτιμήσεις / προηγούμενες αγορές τους

- Όταν μια επεξεργασία έχει νομική βάση το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, **όταν το εν λόγω δίκαιο ρυθμίζει τη συγκεκριμένη πράξη επεξεργασίας και έχει διενεργηθεί ήδη ΕΑ**

- Η ΑΠΔΠΧ καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία απαιτείται / δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων

- **Ζητείται η γνώμη της ΑΠΔΠΧ, πριν από την επεξεργασία (προηγούμενη διαβούλευση),** όταν ο υπεύθυνος επεξεργασίας δεν μπορεί να βρει επαρκή μέτρα για τη μείωση των κινδύνων σε αποδεκτό επίπεδο (δηλαδή οι υπολειπόμενοι κίνδυνοι παραμένουν υψηλοί)

- Εάν η ΑΠΔΠΧ κρίνει ότι η σχεδιαζόμενη επεξεργασία παραβαίνει τον Κανονισμό, ιδίως εάν ο οργανισμός δεν έχει επαρκώς μετριάσει τον κίνδυνο, συμβουλεύει γραπτώς τον υπεύθυνο/ εκτελούντα εντός 8 εβδομάδων – δυνατότητα παράτασης ακόμη 6 εβδομάδων

- Κατά τη διαβούλευση υποβάλλονται στην ΑΠΔΠΧ, μεταξύ άλλων:
  - αρμοδιότητες του υπεύθυνου / συνυπεύθυνων επεξεργασίας
  - σκοποί και τα μέσα της σχεδιαζόμενης επεξεργασίας
  - η εκτίμηση αντίκτυπου και τα μέτρα μετριασμού κινδύνων

12. Τήρηση κώδικα δεοντολογίας (code of conduct)
(Άρθρα 40 – 41)

- Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπεύθυνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν εθελοντικά να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν υφιστάμενους

- **Σκοπός:** για συμμόρφωση με τον Κανονισμό όσον αφορά στη θεμιτή και διαφανή επεξεργασία και στην άσκηση των δικαιωμάτων των υποκειμένων

- Το σχέδιο κώδικα δεοντολογίας υποβάλλεται στην ΑΠΔΠΧ για απόψεις και τελική έγκριση. Όταν εγκριθεί, η ΑΠΔΠΧ τον δημοσιεύει

- Ανεξάρτητος φορέας, διαπιστευμένος από την ΑΠΔΠΧ, μπορεί να παρακολουθεί τη συμμόρφωση με τον Κώδικα

- Ο Φορέας θεωρείται ότι είναι διαπιστευμένος εφόσον πληροί συγκεκριμένα κριτήρια που θέτει το άρθρο 41 του Κανονισμού

- Ο Φορέας ενημερώνει την ΑΠΔΠΧ σε περίπτωση παράβασης του κώδικα

- Ο Κώδικας μπορεί να αποτελέσει νομική βάση για διαβίβαση δεδομένων σε τρίτη χώρα/ διεθνή οργανισμό

13. Πιστοποίηση (Certification) (Άρθρα 42-43)

- Εάν επιθυμεί, ο υπεύθυνος επεξεργασίας / εκτελών την επεξεργασία θεσπίζει μηχανισμούς πιστοποίησης της προστασίας δεδομένων με σκοπό την απόδειξη συμμόρφωσης με τον Κανονισμό

- Μπορεί να είναι σφραγίδα ή σήμα προστασίας

- Η πιστοποίηση χορηγείται από τους φορείς πιστοποίησης (certification bodies) ή την ΑΠΔΠΧ, για μέγιστη περίοδο 3 ετών και μπορεί να ανανεωθεί

- Ο φορέας πιστοποίησης διαπιστεύεται από την ΑΠΔΠΧ ή από τον εθνικό οργανισμό πιστοποίησης για μέγιστη περίοδο 5 ετών και μπορεί να ανανεωθεί

- Η πιστοποίηση ανακαλείται αν δεν πληρούνται οι προϋποθέσεις πιστοποίησης

- Η πιστοποίηση μπορεί να αποτελέσει νομική βάση για διαβίβαση σε τρίτη χώρα / διεθνή οργανισμό

- **Διαδικασία πιστοποίησης:**
  Ο ενδιαφερόμενος οργανισμός
  υποβάλλει στο φορέα πιστοποίησης ή στην ΑΠΔΠΧ κάθε πληροφορία και
  παρέχει πρόσβαση στα αρχεία του που απαιτούνται για τη διεξαγωγή της διαδικασίας πιστοποίησης

14. Υποχρέωση διορισμού Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ) (designation of a Data Protection Officer) (Άρθρα 37-39)

Υποχρεώσεις και ευθύνες εκτελούντα την επεξεργασία

- Συνάπτεται συμφωνία/σύμβαση μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντα, η οποία καθορίζει τις υποχρεώσεις/ευθύνες του (άρθρο 28)
- Η συμφωνία/σύμβαση υφίσταται και σε ηλεκτρονική μορφή και είναι στη διάθεση των υποκειμένων (άρθρο 28)
- Ο εκτελών επεξεργάζεται τα δεδομένα μόνο βάσει καταγεγραμμένων εντολών του υπεύθυνου (άρθρο 28)
- Θέτει στη διάθεση του υπεύθυνου κάθε απαραίτητη πληροφορία προς απόδειξη συμμόρφωσης (άρθρο 28)
- Τηρεί αρχείο καταγραφής δραστηριοτήτων επεξεργασίας (άρθρο 30)
- Συνεργάζεται με την ΑΠΔΠΧ (άρθρο 31)

- Λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της επεξεργασίας (άρθρο 32)
- Ενημερώνει τον υπεύθυνο επεξεργασίας σε περίπτωση παραβίασης δεδομένων (άρθρο 33)
- Διορίζει ΥΠΔ (άρθρο 37)
- Υπόκειται στον έλεγχο της εποπτικής αρχής (άρθρα 57-58)
- Υπόκειται σε κυρώσεις (άρθρα 82-84)
- Προσλαμβάνει άλλον εκτελούντα ΜΟΝΟ με προηγούμενη άδεια του υπευθύνου επεξεργασίας. Οι ίδιες υποχρεώσεις βαραίνουν και αυτόν (άρθρο 28)
- Η τήρηση εγκεκριμένου κώδικα δεοντολογίας (άρθρο 40) ή εγκεκριμένου μηχανισμού πιστοποίησης (άρθρο 42), είναι στοιχείο ότι παρέχει επαρκείς διαβεβαιώσεις (Αιτ. Σκέψη 79, 81.)

Τι καταργείται!

- Γνωστοποιήσεις Σύστασης και Λειτουργίας Αρχείου/Εναρξης Επεξεργασίας – αντικαθίστανται με την τήρηση Αρχείου Δραστηριοτήτων της επεξεργασίας
- Άδεια για επεξεργασία ευαίσθητων δεδομένων *(νυν ειδικών κατηγοριών προσωπικών δεδομένων)*
- Άδεια για διασύνδεση αρχείων
- Έκδοση Απόφασης από την ΑΠΔΠΧ για άρση της υποχρέωσης ενημέρωσης των υποκειμένων των δεδομένων
- Καταβολή τέλους από τα υποκείμενα για άσκηση του δικαιώματος πρόσβασης και αντίρρησης

Τι αλλάζει!

- Καθεστώς αδειών διαβίβασης σε τρίτες χώρες – όμως η ΑΠΔΠΧ εγκρίνει τη νομική βάση της διαβίβασης π.χ. τυποποιημένες συμβατικές ρήτρες, δεσμευτικούς εταιρικούς κανόνες, κώδικα δεοντολογίας, μηχανισμό πιστοποίησης

- Με εφαρμοστικές διατάξεις, η ΑΠΔΠΧ μπορεί να περιορίσει την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων και δεδομένων που αφορούν στην υγεία

Διαβιβάσεις σε τρίτες χώρες – διεθνείς οργανισμούς
(Άρθρα 44-49)

Επιτρέπεται η διαβίβαση με Άδεια της ΑΠΔΠΧ:

- Εάν ο Οργανισμός επιλέξει ως νομική βάση για τη διαβίβαση συμβατικές ρήτρες που θα ετοιμάσει **και θα εγκριθούν από την ΑΠΔΠΧ**

Εάν από τη διαβίβαση επηρεάζονται και πολίτες κρατών μελών, οι συμβατικές ρήτρες θα εγκριθούν στα πλαίσια του μηχανισμού συνεκτικότητας*

* *Θεσπίζεται μηχανισμός συνεκτικότητας για τη συνεργασία μεταξύ των εποπτικών αρχών, ιδιαίτερα όταν μια εποπτική αρχή θεσπίζει μέτρο που επηρεάζει ουσιωδώς σημαντικό αριθμό υποκειμένων των δεδομένων σε περισσότερα κράτη μέλη.*

➢ **Επιτρέπεται η διαβίβαση <u>χωρίς Άδεια</u>** όταν τρίτη χώρα:

- **Εξασφαλίζει ικανοποιητικό επίπεδο προστασίας** (με Απόφαση της Ευρωπαϊκής Επιτροπής ή δυνάμει του Privacy Shield για εταιρείες των ΗΠΑ που έχουν καταχωρηθεί στο FTC [Federal Trade Commission], DoT [Department of Transport] και DoC [Commerce])

- **Δεν εξασφαλίζει** μεν ικανοποιητικό επίπεδο προστασίας **αλλά** υπάρχουν επαρκείς εγγυήσεις:

  (α) νομικά δεσμευτικό μέσο μεταξύ δημόσιων αρχών π.χ. πολυμερής συμφωνία, FATCA (Foreign Account Tax Compliance Act) ή

  (β) δεσμευτικούς εταιρικούς κανόνες (για ομίλους επιχειρήσεων) **που εγκρίνονται από την αρμόδια εποπτική αρχή** ή

  (γ) τυποποιημένες ρήτρες που εκδίδονται από την Επιτροπή ή

  (δ) τυποποιημένες ρήτρες που **<u>εκδίδονται από την ΑΠΔΠΧ και εγκρίνονται από την Επιτροπή</u>** ή

  (ε) κώδικα δεοντολογίας, **<u>ο οποίος εγκρίνεται από την ΑΠΔΠΧ</u>** ή από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, εάν αφορά διάφορα κράτη μέλη

  (στ) μηχανισμό πιστοποίησης, **<u>ο οποίος εγκρίνεται από την ΑΠΔΠΧ</u>** ή τον εθνικό οργανισμό πιστοποίησης ή και από τους δύο

- **Επιτρέπεται η διαβίβαση <u>χωρίς Άδεια</u>** όταν τρίτη χώρα:

- **ΔΕΝ** εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, **ΔΕΝ** υπάρχουν επαρκείς εγγυήσεις, **αλλά** πληρούνται συγκεκριμένες προϋποθέσεις

  π.χ. για λόγους δημοσίου συμφέροντος, για άσκηση νομικών αξιώσεων, για προστασία ζωτικού συμφέροντος κ.λπ.

  ΣΗΜ: Όταν η διαβίβαση ελλοχεύει κινδύνους για τα υποκείμενα των δεδομένων, ο Οργανισμός διενεργεί Εκτίμηση Αντικτύπου και αν δεν υπάρχουν μέτρα μετριασμού του κινδύνου ή αν τα προβλεπόμενα μέτρα δεν μετριάζουν τον κίνδυνο επαρκώς, ο οργανισμός διαβουλεύεται τη διαβίβαση με την ΑΠΔΠΧ

- **Επικεφαλής εποπτική αρχή**

  Είναι η εποπτική αρχή της κύριας ή της μόνης εγκατάστασης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία

- **Αρμόδια εποπτική αρχή**

  Κάθε εποπτική αρχή είναι αρμόδια, στο έδαφος του κράτους μέλους στο οποίο υπάγεται, να ασκεί τις εξουσίες και να εκτελεί τα καθήκοντά της βάσει του Κανονισμού

  Για παράδειγμα, εξέταση υποβολής παραπόνου, με την προϋπόθεση ότι αφορά μόνο εγκατάσταση στο οικείο κράτος μέλος ή επηρεάζει ουσιωδώς υποκείμενα των δεδομένων μόνο στο οικείο κράτος μέλος

- **Ενδιαφερόμενη εποπτική αρχή**

  Εποπτική αρχή την οποία αφορά η επεξεργασία διότι:

  (α) ο υπεύθυνος ή ο εκτελών είναι εγκατεστημένος στο έδαφος του κράτους μέλους της εν λόγω εποπτικής αρχής,

  (β) τα υποκείμενα που διαμένουν στο κράτος μέλος της εν λόγω εποπτικής αρχής επηρεάζονται ή ενδέχεται να επηρεαστούν ουσιωδώς από την επεξεργασία ή

  (γ) έχει υποβληθεί καταγγελία στην εν λόγω εποπτική αρχή

Εποπτική αρχή

- Ανεξάρτητη, χωρίς εξωτερικές επιρροές, δεν ζητεί ούτε λαμβάνει οδηγίες από κανέναν
- Τα μέλη της διορίζονται με διαφανή διαδικασία και απέχουν από κάθε πράξη ασυμβίβαστη προς τα καθήκοντά τους
- Διαθέτει τους απαραίτητους ανθρώπινους, τεχνικούς και οικονομικούς πόρους και τις αναγκαίες εγκαταστάσεις και υποδομές
- Διαθέτει δικούς της υπαλλήλους
- Υπόκειται σε οικονομικό έλεγχο ο οποίος δεν επηρεάζει την ανεξαρτησία της και διαθέτει δικό της ετήσιο προϋπολογισμό
- Τα μέλη και οι υπάλληλοι δεσμεύονται από το επαγγελματικό απόρρητο κατά τη διάρκεια της θητείας και μετά το πέρας αυτής
- Δια νόμου προβλέπεται η σύσταση της εποπτικής αρχής, τα προσόντα, η διάρκεια θητείας των μελών *(δεν πρέπει να είναι μικρότερη από 4 χρόνια)*

Εξουσίες Εποπτικής Αρχής (Άρθρο 58)

- Εισάγονται αυξημένες εξουσίες

- Εγκρίνει πιστοποιητικά και κριτήρια πιστοποίησης
- Προβαίνει σε επανεξέταση των πιστοποιήσεων
- Παρέχει διαπίστευση σε φορείς πιστοποίησης
- Εκδίδει γνώμες για σχέδια κωδίκων δεοντολογίας και τα εγκρίνει
- Εγκρίνει δεσμευτικούς εταιρικούς κανόνες
- Εγκρίνει τυποποιημένες ρήτρες

- Επιβάλλει αυξημένα διοικητικά πρόστιμα (Άρθρο 83)

Εγχειρίδιο - Λίστα Ελέγχου - Μέτρα που πρέπει να ληφθούν από τον οργανισμό για συμμόρφωση με τον Κανονισμό

1. Αντίληψη του οργανισμού ότι η προστασία των προσωπικών δεδομένων είναι ευθύνη της Διοίκησης π.χ.
   - Με την ύπαρξη πολιτικών/κανόνων για την επεξεργασία προσωπικών δεδομένων
   - Με την αντίληψη των κινδύνων που ενέχει η επεξεργασία
2. Ορισμός ΥΠΔ
   - Γιατί δεν έχει οριστεί;
   - Αν έχει οριστεί, είναι ξεκάθαρος ο ρόλος του;
   - Έχουν δηλωθεί τα στοιχεία επικοινωνίας του στην ΑΠΔΠΧ;

3. Έλεγχος των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας:
   - είναι σύμφωνα με το σκοπό για τον οποίο έχουν αρχικά συλλεχθεί;
   - είναι μόνο τα απαραίτητα;
   - είναι ορθά και ενημερωμένα;
   - διατηρούνται μόνο για όσο χρονικό διάστημα είναι απολύτως απαραίτητα;
   - λαμβάνονται τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφάλειας και προστασίας τους;
   - αυτά τα μέτρα αναθεωρούνται τακτικά για να λαμβάνουν υπόψη τις νέες τεχνολογικές εξελίξεις;
   - σε κάποια τουλάχιστον μέρη της επεξεργασίας, αντί να χρησιμοποιηθούν πραγματικά δεδομένα, θα μπορούσε να χρησιμοποιηθεί κρυπτογράφηση ή ψευδωνυμοποίηση;

4. Κατάρτιση διαδικασιών για τήρηση Αρχείου Δραστηριοτήτων της επεξεργασίας
5. Κατάρτιση εργαλείων και διαδικασιών που διασφαλίζουν ότι στη φάση σχεδιασμού του έργου/παροχής της υπηρεσίας:
   - συλλέγονται μόνο τα δεδομένα που είναι απαραίτητα για το συγκεκριμένο σκοπό που επιδιώκεται
   - αποφασίζεται το χρονικό διάστημα διατήρησης και τα οργανωτικά και τεχνικά μέτρα ασφάλειας
   - η προστασία των προσωπικών δεδομένων αποτελεί αναπόσπαστο μέρος της διαδικασίας ανάπτυξης του έργου/παροχής της υπηρεσίας
6. Εκπαίδευση και ευαισθητοποίηση του προσωπικού:
   - όσοι επεξεργάζονται προσωπικά δεδομένα μέσα στον οργανισμό γνωρίζουν πότε υπάρχει παραβίαση προσωπικών δεδομένων;

7. Υιοθέτηση:
    - εσωτερικής διαδικασίας αναφοράς της παραβίασης
    - εσωτερικού «πλάνου ανταπόκρισης» (response plan) σε περίπτωση παραβίασης
    - διαδικασία γνωστοποίησης ενδεχόμενης παράβασης στην ΑΠΔΠΧ, εντός 72 ωρών
8. Σύναψη συμφωνίας μεταξύ 2 υπεύθυνων επεξεργασίας, σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας

9. Αναθεώρηση των συμβολαίων/συμβάσεων που συνάπτονται με πελάτες, προμηθευτές, υπαλλήλους, εκτελούντες την επεξεργασία (βλ. άρθρο 28 του Κανονισμού για το τι πρέπει να περιλαμβάνει μία σύμβαση ανάθεσης εργασίας σε εκτελούντα)
    - Τι απογίνονται τα δεδομένα μετά τη λήξη της σύμβασης με τον εκτελούντα;

10. Διενέργεια εκτίμησης αντικτύπου εάν η επεξεργασία ενέχει υψηλό κίνδυνο / ρίσκο στα δικαιώματα, ελευθερίες και συμφέροντα των ατόμων:
    - έχει υιοθετηθεί μέθοδος που να αναγνωρίζει εάν υπάρχει υψηλός κίνδυνος;
    - έχει επιλεγεί διαδικασία για διενέργεια ΕΑ;
    - έχει υιοθετηθεί πολιτική με προκαθορισμένη διαδικασία για αντιμετώπιση του υψηλού κινδύνου;

11. Σε περίπτωση διασυνοριακής επεξεργασίας, εντός της ΕΕ, ορισμός του κράτους μέλους της κύριας εγκατάστασης, του οποίου η εποπτεύουσα αρχή θα είναι αρμόδια ως επικεφαλής αρχή, για την εποπτεία της νομιμότητας της επεξεργασίας εντός της Ε.Ε.

12. Αξιολόγηση των συγκαταθέσεων των υποκειμένων, εάν ανταποκρίνονται στις διατάξεις του άρθρου 5 του Κανονισμού

- Μπορεί πράγματι να αποδειχθεί ότι έχει δοθεί συγκατάθεση;

13. Υιοθέτηση των απαιτήσεων του άρθρου 32 (ασφάλεια):

- Έχουν αντικατασταθεί οι υφιστάμενες λίστες ελέγχου που αφορούν στους κινδύνους της επεξεργασίας λαμβάνοντας υπόψη τη φύση, πεδίο εφαρμογής, περιεχόμενο και σκοπό της επεξεργασίας;
- Έχει υιοθετηθεί σύστημα διοίκησης για τακτική αναθεώρηση, αξιολόγηση και βελτίωση των μέτρων ασφάλειας;
- Έχουν ληφθεί μέτρα (π.χ. ψευδωνυμοποίηση και κρυπτογράφηση) για προστασία από παράνομη επεξεργασία από εσωτερικούς και εξωτερικούς εισβολείς;

14. Αναθεώρηση των εντύπων που δίνονται στα υποκείμενα με τα οποία ενημερώνονται για τις πληροφορίες που προβλέπονται στα άρθρα 13 και 14. Για παράδειγμα:

- ✓ στοιχεία επικοινωνίας του ΥΠΔ
- ✓ νομική βάση για την επεξεργασία
- ✓ νομική βάση για διαβίβαση σε τρίτη χώρα (εάν ισχύει)
- ✓ χρονικό διάστημα διατήρησης των δεδομένων
- ✓ τα δικαιώματα που μπορούν να ασκήσουν
- ✓ δικαίωμα υποβολής παραπόνου στην ΑΠΔΠΧ
- ✓ σε περίπτωση που η νομική βάση της επεξεργασίας είναι η συγκατάθεση, να γνωρίζουν ότι μπορούν να την ανακαλέσουν ανά πάσα στιγμή
- ✓ σε περίπτωση αυτοματοποιημένης λήψης απόφασης (π.χ. κατάρτιση προφίλ), τη λογική, σημασία και επιπτώσεις τέτοιας επεξεργασίας στο υποκείμενο
- ✓ σε περίπτωση συλλογής των δεδομένων, όχι από το ίδιο το υποκείμενο, την πηγή/προέλευση τους

15. Εφαρμογή διαδικασιών για ικανοποίηση των δικαιωμάτων των υποκειμένων π.χ. φορητότητα των δεδομένων

16. Πριν το κλείσιμο λογαριασμού ενός ατόμου, να δίνεται το δικαίωμα στο άτομο να ασκήσει το δικαίωμα στη φορητότητα των δεδομένων του

Άλλα σημαντικά θέματα
και
ορθές πρακτικές

Ηχογράφηση τηλεφωνικών συνδιαλέξεων

Ισχύουν οι διατάξεις για το Απόρρητο των Επικοινωνιών (άρθρο 4) του νόμου 3471/2006

Παρέμβαση στις επικοινωνίες επιτρεπτή αν:

- εξασφαλίζεται η συγκατάθεση των επικοινωνούντων ή
- προβλέπεται από νομοθεσία (πρωτογενή /δευτερογενή) και με άδεια του Δικαστηρίου ή
- αν πρόκειται για νόμιμη επαγγελματική πρακτική επιτρέπεται η καταγραφή συνδιαλέξεων με σκοπό την εξασφάλιση αποδεικτικών στοιχείων κάποιας εμπορικής συναλλαγής και/ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα

Ισχύουν και οι διατάξεις του νόμου 3471/2006, δυνάμει των οποίων:

- προτού αρχίσει η τηλεφωνική συνομιλία, υπάρχει προειδοποιητική σήμανση ότι η συνομιλία ηχογραφείται,
- στο περιεχόμενο της προειδοποιητικής σήμανσης, να αναφέρονται τα ακόλουθα:

- η ταυτότητα του υπεύθυνου επεξεργασίας,
- ο σκοπός της ηχογράφησης,
- εάν η ηχογραφημένη συνομιλία θα κοινοποιηθεί σε τρίτους και ότι
- το φυσικό πρόσωπο μπορεί να έχει πρόσβαση στο περιεχόμενο της ηχογραφημένης τηλεφωνικής συνομιλίας

Εγκατάσταση Κλειστού Κυκλώματος Βιντεοπαρακολούθησης (ΚΚΒΠ) στο χώρο εργασίας

- Επιτρέπεται μόνο αν δεν υπάρχει λιγότερο παρεμβατικός τρόπος για την πραγματοποίηση του σκοπού π.χ. για προστασία του χώρου από διαρρήξεις και κλοπές.
- Επιτρέπεται η εγκατάσταση και λειτουργία κάμερας στις εισόδους/ εξόδους /για τον έλεγχο των ταμείων / των ΑΤΜ / δωμάτια εξοπλισμού / έλεγχο θυρίδων / χώρων στάθμευσης / έξω από ανελκυστήρα μόνο για έλεγχο διερχομένων κλπ
- Απαραίτητη η σήμανση με ευδιάκριτα γράμματα για ενημέρωση των πελατών **πριν** από την είσοδό τους στην εταιρεία
- Οι υπάλληλοι ενημερώνονται μέσω εγκυκλίου
- Δεν επιτρέπεται η μυστική παρακολούθηση

- Δεν επιτρέπεται η εγκατάσταση ΚΚΒΠ σε:

- διαδρόμους
- μέσα στο ασανσέρ
- χώρο αναμονής
- τουαλέτες
- σε γραφεία όπου απασχολείται ένας ή μικρός αριθμός υπαλλήλων (Υπάρχουν σχετικές Αποφάσεις της ΑΠΔΠΧ για απεγκατάσταση των καμερών ή λειτουργία τους κατά τις μη εργάσιμες ώρες)
- καφετέρια

- Δεν επιτρέπεται να ελέγχεται η προσωπική συμπεριφορά, οι προσωπικές επαφές και η αποδοτικότητα / παραγωγικότητα των υπαλλήλων μέσω τέτοιων συστημάτων
- Τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται μέσω προειδοποιητικών πινακίδων, οι οποίες θα πρέπει να είναι:
- ευδιάκριτες
- επαρκείς σε αριθμό
- εμφανείς
- σε σημείο **πριν** τα υποκείμενα των δεδομένων εισέλθουν στο χώρο όπου γίνεται η οπτικογράφηση
- Σε περίπτωση που υπάρχει ΚΚΒΠ σε κάθε όροφο, η ενημέρωση θα πρέπει να γίνεται σε κάθε όροφο ξεχωριστά

Ορθή τηλεξυπηρέτηση κοινού

Δεν πρέπει να δίνονται δεδομένα μέσω τηλεφώνου αφού δεν επιβεβαιώνεται ότι τα δεδομένα ανακοινώνονται στα άτομα στα οποία αναφέρονται τα δεδομένα

Εγκατάσταση συστημάτων δακτυλικών αποτυπωμάτων για σκοπούς ελέγχου της ώρας προσέλευσης / αναχώρησης των υπαλλήλων από την εργασία

- **Είναι βιομετρικό δεδομένο:** καθολικό, μοναδικό, μόνιμο δεδομένο όπως είναι φωτογραφία, DNA, ίριδα, παλάμη, φωνή κτλ
- **Δεν επιτρέπεται**
- **Επιτρέπεται** σε κτίρια υψίστης ασφάλειας και χώρους με ιδιαίτερες απαιτήσεις ασφαλείας και εφόσον δεν υπάρχει άλλο λιγότερο επαχθές μέσο για την επίτευξη των **σκοπών ασφάλειας** των εγκαταστάσεων / εξοπλισμού /προσώπων (π.χ. στρατιωτικές /αμυντικές εγκαταστάσεις, εργαστήρια υψηλού κινδύνου, χώροι αεροδρομίων, κ.ά.)
- Ο υπεύθυνος επεξεργασίας θα πρέπει να σταθμίζει τους κινδύνους, την έκταση των κινδύνων αυτών και τις υπάρχουσες εναλλακτικές δυνατότητες αντιμετώπισης των κινδύνων και από την άλλη, τις προσβολές της προσωπικότητας και της ιδιωτικότητας του ατόμου από τη χρήση τέτοιων μεθόδων

Ορθή χρήση αρχείου του προσωπικού

- Οι προσωπικοί φάκελοι των υπαλλήλων (που περιέχουν προσόντα και ατομικές εκθέσεις), θα πρέπει να διατηρούνται σε ασφαλές μέρος (σε χώρους που κλειδώνουν)
- Πρόσβαση στους προσωπικούς φακέλους να έχει μόνο εξουσιοδοτημένο προσωπικό
- Απαγορεύεται η διάδοση προσωπικών δεδομένων που αφορούν ένα υπάλληλο σε άλλο

Ορθή χρήση αναρρωτικών αδειών και δεδομένων υγείας του προσωπικού

Νόμιμη επεξεργασία: Συγκατάθεση ή Άδεια ΑΠΔΠΧ

- Οι αναρρωτικές άδειες (περιλαμβάνουν ευαίσθητα δεδομένα) θα πρέπει να καταχωρούνται όχι στον προσωπικό φάκελο του υπαλλήλου αλλά σε ξεχωριστό φάκελο που να ονομάζεται «Φάκελος Αδειών». Σε αυτόν, μπορούν επίσης να καταχωρούνται οι άδειες ανάπαυσής του
- Περιορισμένη πρόσβαση: μόνο από άτομα που έχουν επιλεγεί και εξουσιοδοτηθεί ειδικά από τον εργοδότη.
- Αν τα δεδομένα υγείας ενός εργαζόμενου πρόκειται να κοινοποιηθούν σε τρίτους, ο εργαζόμενος πρέπει να ενημερώνεται εκ των προτέρων για τους σκοπούς και τους αποδέκτες της κοινοποίησης

- Η επεξεργασία δεδομένων υγείας πρέπει να περιορίζεται στις περιπτώσεις όπου αυτή είναι απαραίτητη για να ικανοποιηθούν συγκεκριμένοι σκοποί όπως π.χ.:
  - όταν η επεξεργασία είναι απαραίτητη για να κριθεί κατά πόσο ένας εργαζόμενος είναι ικανός να εκπληρώσει μία παρούσα ή μελλοντική εργασία
  - όταν η επεξεργασία είναι απαραίτητη για σκοπούς πρόληψης και προστασίας της υγείας των εργαζόμενων στους χώρους εργασίας
  - όταν η επεξεργασία είναι απαραίτητη, για να παρασχεθούν στον εργαζόμενο δικαιώματα ασθενείας ή κοινωνικών ασφαλίσεων
  - όταν τα καθήκοντα της θέσης επιβάλλουν την υποβολή του εργαζόμενο σε συγκεκριμένους υγειονομικούς ή ιατρικούς ελέγχους

Καταστροφή εγγράφων που περιέχουν προσωπικά δεδομένα

- Τα δεδομένα θα πρέπει να διατηρούνται **μόνο κατά τη διάρκεια της περιόδου που απαιτείται** για την πραγματοποίηση των σκοπών της συλλογής /επεξεργασίας

- Για εταιρείες που παρέχουν διοικητικές υπηρεσίες και

- Για εταιρείες που παρέχουν λογιστικές/ελεγκτικές υπηρεσίες

θα οριστεί από την ΑΠΔΠΧ και τη συμφωνημένη διεθνή και ελληνική καλή πρακτική κάθε κλάδου για πόσα χρόνια μετά τη λήξη της συμβατικής σχέσης και / ή της διευθέτησης οποιασδήποτε οικονομικής ή άλλης διαφοράς θα διατηρούνται τα δεδομένα

- Μετά την παρέλευση της περιόδου αυτής, η ΑΠΔΠΧ μπορεί να επιτρέψει τη διατήρησή τους για ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς

Δικηγορικός Σύλλογος Καρδίτσας

Τηλ: 2441021646

E-mail: dskarditsas@gmail.com

www.dskard.gr

Δημήτρης Τζέλλης