Ευρωπαϊκός Κανονισμός (ΕΕ) 2016/679

Νέο Νομικό Πλαίσιο

Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Δεκέμβριος 2017

1

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 (συμπεριλαμβανομένων των νομικών προσώπων δημοσίου δικαίου)
- Όταν γίνεται τακτική και συστηματική παρακολούθηση των υποκειμένων **σε μεγάλη κλίμακα**
- Όταν τυγχάνουν επεξεργασίας ειδικές κατηγορίες δεδομένων ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα **σε μεγάλη κλίμακα**

Μεγάλη κλίμακα:

- Γίνεται επεξεργασία σημαντικής ποσότητας δεδομένων ή για μεγάλη διάρκεια ή
- Επηρεάζεται μεγάλος αριθμός προσώπων ή
- Χρησιμοποιείται νέα τεχνολογία που ελλοχεύει ψηλούς κινδύνους
- Η επεξεργασία καλύπτει μεγάλη γεωγραφική περιοχή

2

Παραδείγματα

- Επεξεργασία δεδομένων ασθενών σε νοσοκομείο / κλινική
- Επεξεργασία δεδομένων πελατών τράπεζας / ασφαλιστικής εταιρείας
- Επεξεργασία δεδομένων πάροχων υπηρεσιών διαδικτύου
- Επεξεργασία δεδομένων για παροχή τηλεπικοινωνιακών υπηρεσιών
- Επεξεργασία δεδομένων μέσω μηχανής αναζήτησης για διαφημιστικούς σκοπούς π.χ. η Google διαφημίζει τον CEO και το ΔΣ εταιρείας στην Κύπρο
- Εξωτερικός συνεργάτης διαχειρίζεται την μισθοδοσία του προσωπικού μιας εταιρίας
- Εγκατάσταση και λειτουργία ΚΚΒΠ

3

- Επεξεργασία που καθορίζει την καταναλωτική συμπεριφορά και συνήθειες ατόμων για διαφημιστικούς σκοπούς (behavioural advertising)
- Δημιουργία προφίλ για εκτίμηση κινδύνων π.χ. αξιολόγηση ασφαλιστικού κινδύνου, για πάταξη ξεπλύματος βρώμικου χρήματος
- Επεξεργασία σε πραγματικό χρόνο των γεο-τοπογραφικών δεδομένων (Geo-Location Data) πελατών διεθνούς εταιρίας fast food για στατιστικούς σκοπούς

4

Ποια είναι τα καθήκοντα του ΥΠΔ;

- Συμβουλεύει την 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
- Ξεχωρίζει ποιες δραστηριότητες του οργανισμού είναι «κύριες» και ποιες «παρεπόμενες» (πρ. 97)
- Βοηθά τη διεύθυνση να καταρτίσει και να επικαιροποιεί το αρχείο δραστηριοτήτων *(σύμφωνα με το άρθρο 30)*
- Αναλύει και ελέγχει κατά πόσον οι επεξεργασίες είναι σύμφωνες με τον Κανονισμό και ενημερώνει τη διεύθυνση
- Συμβουλεύει τη διεύθυνση στη σύνταξη πολιτικών ασφάλειας και προστασίας προσωπικών δεδομένων

5

- Προτείνει τη λήψη εσωτερικών διαδικασιών ελέγχου και επαλήθευσης της αποτελεσματικής εφαρμογής των μέτρων ελέγχου
- **Συμβουλεύει** την διεύθυνση, <u>εάν του ζητηθεί πριν τη διενέργεια Εκτίμησης Αντικτύπου (ΕΑ):</u>

1. Τη μεθοδολογία που θα ακολουθηθεί
2. Κατά πόσον η ΕΑ θα διενεργηθεί από τον οργανισμό ή τρίτο (outsourcing)
3. Τις δικλίδες ασφαλείας για μετριασμό του κινδύνου
4. Κατά πόσον πρέπει να γίνει διαβούλευση με την ΑΠΔΠΧ *(ελλείψει μέτρων μετριασμού του κινδύνου)*

- Εκπαιδεύει και συμβουλεύει το προσωπικό του οργανισμού για ορθή εφαρμογή του Κανονισμού
- Βοηθά τα υποκείμενα των δεδομένων να ασκούν τα δικαιώματα τους
- Συνεργάζεται με την ΑΠΔΠΧ

6

Κατά την εκτέλεση των καθηκόντων του ο ΥΠΔ:

- Λαμβάνει μέρος στις συναντήσεις της ανώτερης και ανώτατης διοίκησης
- Υπερέχει η γνώμη του στις αποφάσεις που έχουν αντίκτυπο στην προστασία προσωπικών δεδομένων: τεκμηρίωση από τη διοίκηση τυχόν αντίθετης γνώμης
- Του παρέχεται ικανοποιητικός χρόνος, η κατάλληλη υποδομή και απαραίτητοι οικονομικοί πόροι
- Έχει πρόσβαση σε κάθε είδους δεδομένα και λαμβάνει μέρος σε κάθε σχεδιαζόμενη πράξη επεξεργασίας από την αρχή
- Έχει πρόσβαση στις εγκαταστάσεις του οργανισμού
- Ενεργεί ως σημείο επικοινωνίας για την ΑΠΔΠΧ ιδίως για τις ΕΑ

7

- δεσμεύεται με την τήρηση του απορρήτου / εμπιστευτικότητας
- δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του
- δεν απολύεται ούτε υφίσταται κυρώσεις επειδή έκανε τη δουλειά του. π.χ. εάν μία επεξεργασία ενέχει υψηλό κίνδυνο και ο ΥΠΔ συμβουλεύσει τον υπεύθυνο επεξεργασίας για τη διενέργεια ΕΑ αλλά η διοίκηση διαφωνήσει, ο ΥΠΔ δεν θα απολυθεί. Απολύεται για άλλους λόγους π.χ. κλοπή, ανάρμοστη συμπεριφορά, άσκηση ψυχολογικής βίας κλπ
- λογοδοτεί απευθείας στο ανώτατο επίπεδο της διοίκησης
- έχει ως προτεραιότητα τα καθήκοντα του ΥΠΔ και δεν αναλαμβάνει άλλα καθήκοντα που έρχονται σε σύγκρουση συμφέροντος με τα καθήκοντά του ως ΥΠΔ

8

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.

- Γενικός Διευθυντής, Προϊστάμενος Τμήματος Πληροφορικής / Ανθρώπινου Δυναμικού / Λογιστηρίου / Ελεγκτικού οίκου
- Κατώτερες θέσεις, των οποίων οι κάτοχοι τους καθορίζουν 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)*

9

Δημοσίευση και ανακοίνωση των στοιχείων επικοινωνίας του ΥΠΔ

Ο Οργανισμός δημοσιεύει τα στοιχεία επικοινωνίας του 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 όνομα του) δημοσιεύονται στην εσωτερική σελίδα του οργανισμού
- Όλες οι πιο πάνω πληροφορίες ανακοινώνονται στην ΑΠΔΠΧ

10

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, mobile banking
- 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

11

Πεδίο εφαρμογής

- Στο έδαφος της Κυπριακής Δημοκρατίας
- Όταν εφαρμόζεται το κυπριακό δίκαιο δυνάμει διεθνούς δικαίου
- Διασυνοριακές υποθέσεις που αφορούν πρόσωπα σε περισσότερα κράτη μέλη (συνδεδεμένες εταιρείες)
- Σε επεξεργασία εκτός ΕΕ για υποκείμενα που βρίσκονται εντός ΕΕ
- Σε επεξεργασία που εκτελείται στην ΕΕ για υποκείμενα που βρίσκονται εκτός ΕΕ
- **Κύρια εγκατάσταση:** ορίζεται, όταν μια εταιρεία έχει εγκαταστάσεις σε πολλά κράτη μέλη

❖ **Για υπεύθυνο επεξεργασίας:** κύρια εγκατάσταση = η εγκατάσταση όπου λαμβάνονται οι αποφάσεις

❖ **Για εκτελών την επεξεργασία:** κύρια εγκατάσταση = η εγκατάσταση όπου εκτελείται η επεξεργασία

12

Καινοτομίες του Κανονισμού

(α) Ομοιόμορφη μεταφορά και εφαρμογή:

- 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 και δημιουργία νέων

(γ) Ενίσχυση υφιστάμενων αρχών προστασίας των 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 μπορεί να συναλλάσσεται με μία μόνο ΑΠΔΠΧ)

(η) Διενέργεια ελέγχων before the event

(θ) Πρόσβαση από την ΑΠΔΠΧ στις κτιριακές εγκαταστάσεις και στον εξοπλισμό του οργανισμού

(ι) Επιβολή αυστηρότερων κυρώσεων

(κ) Κατάργηση Γνωστοποιήσεων και Αδειών Διασύνδεσης / Διαβίβασης, όπως τις γνωρίζουμε σήμερα

(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

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 από ανάλυση βιολογικού δείγματος και παρέχουν μοναδικές πληροφορίες για την υγεία ή φυσιολογία π.χ. DNA
- **βιομετρικά δεδομένα:** δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία και επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου π.χ. εικόνες προσώπου, δακτυλοσκοπικά δεδομένα

15

- **ψευδωνυμοποίηση:** επεξεργασία που εκτελείται ώστε τα δεδομένα δεν 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 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 Αντρέου γεννήθηκε στις 25 Ιανουαρίου 1970, διαμένει στη Λεμεσό και εργάζεται σε τράπεζα», μπορεί να καταστεί ψευδώνυμη ως εξής:

    « Ο Π.Α. 1970 διαμένει στη Λεμεσό και εργάζεται σε τράπεζα» ή

    « Ο 48 διαμένει στη Λεμεσό και εργάζεται σε τράπεζα» ή

    «Ο ΒΦΓ43ΓΑ διαμένει στη Λεμεσό και εργάζεται σε τράπεζα» (έχει περισσότερη ασφάλεια)

16

- **παραβίαση προσωπικών δεδομένων:** παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, παράνομη διαβίβαση, κοινοποίηση κ.λ.π.
- **κύρια εγκατάσταση:** όταν πρόκειται για υπεύθυνο επεξεργασίας με εγκαταστάσεις σε περισσότερα κμ - κύρια εγκατάσταση είναι ο τόπος της κεντρικής διοίκησης στην ΕΕ. Αν όμως οι αποφάσεις λαμβάνονται σε άλλη εγκατάσταση στην ΕΕ, θεωρείται αυτή η κύρια εγκατάσταση
- **διασυνοριακή επεξεργασία:**
  - η επεξεργασία που εκτελείται όταν ο υπεύθυνος επεξεργασίας ή εκτελών είναι εγκατεστημένος σε περισσότερα του ενός κμ της ΕΕ
  - η επεξεργασία που εκτελείται στη μία μόνο εγκατάσταση του υπεύθυνου επεξεργασίας ή εκτελούντα αλλά επηρεάζει υποκείμενα των δεδομένων σε περισσότερα κμ
- **υπηρεσία της κοινωνίας των πληροφοριών:** 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

17

Διεύρυνση εννοιών (άρθρα 4, 7, 8)

- **Απλά δεδομένα** – δεδομένα θέσης και επιγραμμικά (on line) αναγνωριστικά στοιχεία ταυτότητας τα οποία παρέχονται από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα τους και διευκολύνουν τον εντοπισμό του φυσικού προσώπου π.χ.

  IP address, εντοπισμός θέσης μέσω GPS)

- **Ειδικές κατηγορίες δεδομένων** *(πρώην ευαίσθητα δεδομένα)* – γενετικά και βιομετρικά

18

➢ **Συγκατάθεση:** δεν υπήρχε αντίστοιχη πρόνοια 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 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

19

➢ **Συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών**

π.χ. e-government, e-commerce, eBay, Amazon, gambling

- Η επεξεργασία προσωπικών δεδομένων παιδιού είναι σύννομη εάν το παιδί είναι τουλάχιστον 16 χρονών. Εάν το παιδί είναι κάτω των 16 ετών, απαιτείται η συγκατάθεση του προσώπου που έχει τη γονική μέριμνά του
- Τα ΚΜ μπορούν να μειώσουν το όριο ηλικίας, όχι όμως κάτω των 13, με εφαρμοστική διάταξη
- Ο υπεύθυνος επεξεργασίας επαληθεύει ότι η συγκατάθεση παρέχεται από το πρόσωπο που έχει τη γονική μέριμνα, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία

20

Αρχές νόμιμης επεξεργασίας (άρθρο 5)

- Εισάγεται η **Αρχή της Λογοδοσίας:**
  Ο οργανισμός 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. Τα μέτρα αυτά επανεξετάζονται και επικαιροποιούνται κάθε 3 χρόνια ή όταν αυξάνεται ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των ατόμων (κατευθυντήριες γραμμές της Ομάδας Εργασίας του Άρθρου 29)

- 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 πως αυτά ασκούνται

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
Σημ.: 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 (δεν απαιτείται Άδεια από την ΑΠΔΠΧ για την περαιτέρω επεξεργασία)

3. Αρχή της ελαχιστοποίησης των δεδομένων (data minimisation): Τα δεδομένα που τυγχάνουν επεξεργασίας είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους έχουν αρχικά συλλεγεί

4. Αρχή της ακρίβειας (accuracy): Λαμβάνονται μέτρα που διασφαλίζουν ότι τα προσωπικά δεδομένα είναι ακριβή, διαγράφονται ή διορθώνονται χωρίς καθυστέρηση

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 την πραγματοποίηση του σκοπού. 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 ασφάλεια τους

23

Πότε είναι νόμιμη η επεξεργασία απλών προσωπικών δεδομένων (άρθρο 6 – Πρ. 40-50)

- Έχει δοθεί η συναίνεση του ατόμου
- Για εκτέλεση σύμβασης
- Για έννομη υποχρέωση του οργανισμού
- Για διαφύλαξη ζωτικού συμφέροντος του ατόμου (ανθρωπιστικοί σκοποί π.χ. επιδημίες, ανταπόκριση σε καταστροφές)
- Για δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας
- Για το έννομο συμφέρον του οργανισμού ή του τρίτου

24

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

Κατά κανόνα απαγορεύεται η επεξεργασία τους

- Επιτρέπεται όταν:

(α) υπάρχει συγκατάθεση

(β) στον τομέα του εργατικού δικαίου (και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας – *νέα πρόνοια*)

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

(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 πρόνοια)* ή πρόσωπα που έχουν τακτική επικοινωνία μαζί του και τα δεδομένα δεν κοινοποιούνται σε τρίτους

(ε) για δεδομένα που έχουν δημοσιοποιηθεί από το άτομο

(στ) για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων

(ζ) για λόγους ουσιαστικού δημόσιου συμφέροντος

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

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

(ι) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ***(νέα πρόνοια),*** 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 επαγγέλματα που επιβάλλει ο νόμος π.χ. για αποφυγή εργοδότησης ατόμων σε σχολεία που καταδικάστηκαν για αδικήματα σεξουαλικής φύσης / ατόμων που καταδικάστηκαν για ξέπλυμα βρώμικου χρήματος σε τράπεζα
- Ο εργοδότης μπορεί να ζητήσει από τον υπάλληλο Πιστοποιητικό Λευκού Ποινικού Μητρώου ακόμα και όταν δεν προβλέπεται από νόμο, δεδομένου ότι έχει συνάφεια με το σκοπό που επιδιώκει
- Ο εργοδότης δεν μπορεί να ζητήσει Πιστοποιητικό Λευκού Ποινικού Μητρώου χωρίς τη συγκατάθεση του ατόμου, η οποία πρέπει να δίνεται ελεύθερα
- Αρχείο προηγούμενων καταδικών τηρείται μόνο από την Αστυνομία

27

Ενδυνάμωση Δικαιωμάτων

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

Η ενημέρωση πρέπει να γίνεται σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται 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 δικαιούται να λάβει πληροφορίες που το αφορούν τις οποίες το ίδιο ή άλλο πρόσωπο έδωσε στον υπεύθυνο επεξεργασίας – Καταργείται το τέλος των €17

- ❖ Έντυπη ή ηλεκτρονική μορφή
- ❖ Πληροφορίες για αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ
- ❖ Δικαίωμα παροχής αντιγράφου, νοουμένου ότι δεν επηρεάζει δυσμενώς τα δικαιώματα άλλων προσώπων

28

- **Δικαίωμα διόρθωσης (Right to rectification) (Άρθρο 16)**

➢ Το υποκείμενο έχει δικαίωμα να ζητήσει τη διόρθωση των ανακριβών δεδομένων που το αφορούν, χωρίς αδικαιολόγητη καθυστέρηση

➢ Δικαίωμα συμπλήρωσης ελλειπών προσωπικών δεδομένων, μεταξύ άλλων, μέσω συμπληρωματικής δήλωσης (Πρ. 65)

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

➢ Το υποκείμενο έχει δικαίωμα διαγραφής των δεδομένων όταν:

- δεν είναι πλέον απαραίτητα
- ανάκληση συγκατάθεσης από το υποκείμενο
- το υποκείμενο αντιτίθεται στην επεξεργασία (Άρθρο 21)
- παράνομη επεξεργασία
- υποχρέωση από νόμο
- το υποκείμενο των δεδομένων ήταν παιδί όταν συναίνεσε

29

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

➢ **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
- Υπερέχει δημόσιο συμφέρον στον τομέα της υγείας
- Για επιστημονικούς, στατιστικούς σκοπούς & αρχειοθέτησης
- Για άσκηση νομικών αξιώσεων

30

- **Το δικαίωμα στη λήθη** ενισχύει το δικαίωμα διαγραφής:
- Αφορά στο δικαίωμα διαγραφής δεδομένων στο διαδίκτυο*, που το άτομο δεν επιθυμεί τη δημοσίευση τους διότι του προκαλούν βλάβη και δεν είναι πλέον χρήσιμα για την ενημέρωση του κοινού
  * *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 μπορεί 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. Υπόθεση Google Spain

31

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

➢ Στην Οδηγία προϋπήρχε ο «περιορισμός» ως «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 αυτοματοποιημένη επεξεργασία:

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

32

➢ **Μπορεί να ασκηθεί όταν:**

- το άτομο αμφισβητεί την ακρίβεια των δεδομένων του και ζητά να περιοριστούν τα δεδομένα του μέχρι ο οργανισμός να επαληθεύσει την ακρίβεια τους
- η επεξεργασία είναι παράνομη και το άτομο ζητά να περιοριστούν τα δεδομένα του αντί να διαγραφούν
- τα δεδομένα δεν είναι πλέον απαραίτητα αλλά ζητούνται από το υποκείμενο για νομική αξίωση
- το άτομο έχει αντιρρήσεις για την επεξεργασία (άρθρο 21) και ζητά τον περιορισμό των δεδομένων του εις αναμονή της επαλήθευσης του κατά πόσο οι λόγοι του οργανισμού υπερισχύουν έναντι των δικών του

➢ Όταν γίνει περιορισμός, επεξεργασία επιτρέπεται μόνο με συγκατάθεση ή για νομική αξίωση 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

33

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

➢ Είναι το δικαίωμα του υποκειμένου των δεδομένων να λαμβάνει ένα υποσύνολο των προσωπικών δεδομένων που το αφορούν και έχουν υποβληθεί σε επεξεργασία από υπεύθυνο επεξεργασίας, σε ψηφιακή μορφή (σε μορφή αναγνώσιμη, τόσο από τον άνθρωπο όσο και από το μηχανογραφημένο σύστημα του άλλου οργανισμού) και να αποθηκεύει τα δεδομένα αυτά για περαιτέρω προσωπική χρήση

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

34

➢ **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

35

- **Το δικαίωμα φορητότητας μπορεί να εφαρμοστεί 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 οργανισμό από το ΙΔΙΟ το άτομο ΚΑΙ

✓ δεν επηρεάζονται δυσμενώς τα δικαιώματα και οι ελευθερίες άλλων (περιλαμβάνουν επαγγελματικό απόρρητο, πνευματική ιδιοκτησία, προστασία λογισμικού)

36

Παραδείγματα:

- 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 ένα γάμο
- Άτομα θα μπορούν να λάβουν και να μεταφέρουν δεδομένα κίνησης και θέσης

37

- Ο υπεύθυνος επεξεργασίας δεν μπορεί να απορρίπτει αίτημα φορητότητας στη βάση της παραβίασης άλλου συμβατικού δικαιώματος (π.χ. ανεξόφλητο χρέος ή εμπορική διαφορά με το υποκείμενο των δεδομένων)
- Ένας οργανισμός δεν μπορεί να διατηρεί τα δεδομένα για περισσότερο χρονικό διάστημα από αυτό που χρειάζεται να πραγματοποιηθεί ο σκοπός της επεξεργασίας, απλά επειδή μεταγενέστερα μπορεί να ασκηθεί το δικαίωμα της φορητότητας
- 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, μετά την άσκηση του δικαιώματος της φορητότητας

38

- 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,
- Ο παραλήπτης υπεύθυνος επεξεργασίας έχει υποχρέωση να διασφαλίζει ότι τα δεδομένα που μεταφέρθηκαν είναι ανάλογα των δικών του σκοπών

39

- Όταν υπάρχουν διάφορες τεχνικές λύσεις για τη μεταφορά, πρέπει να επιλέγεται αυτή που ευνοεί το υποκείμενο
- Το δικαίωμα της φορητότητας ασκείται δωρεάν *(εκτός αν είναι επαναλαμβανόμενο)*
- Το δικαίωμα πρέπει να ικανοποιηθεί μέσα σε 1 μήνα από την ημερομηνία υποβολής του αιτήματος αλλιώς το υποκείμενο ενημερώνεται για τους λόγους που δεν μπορεί να το ικανοποιηθεί και έχει το δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή και άσκησης δικαστικής προσφυγής
- ΔΕΝ ισχύει όταν η επεξεργασία είναι απαραίτητη για δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας Πρ. 68

40

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

➢ Το υποκείμενο έχει το δικαίωμα να εναντιωθεί στην επεξεργασία προσωπικών του δεδομένων, ιδίως για σκοπούς απευθείας εμπορικής προώθησης, μόνο όταν:

(α) η επεξεργασία εκτελείται για σκοπούς δημοσίου συμφέροντος ή άσκησης δημόσιας εξουσίας ή

(β) η επεξεργασία εκτελείται για εξυπηρέτηση του έννομου συμφέροντος του υπεύθυνου επεξεργασίας ή τρίτου

➢ Η εναντίωση μπορεί να ασκηθεί και με αυτοματοποιημένα μέσα

➢ Σταματά η επεξεργασία μετά την εναντίωση, εκτός αν ο υπεύθυνος επεξεργασίας καταδείξει υπέρτερο έννομο συμφέρον

➢ Αν η επεξεργασία εκτελείται για επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς, η εναντίωση ασκείται μόνο όταν η επεξεργασία βασίζεται στο έννομο συμφέρον του υπεύθυνου επεξεργασίας ή του τρίτου

➢ **Παράδειγμα:** Πανεπιστήμιο έχει έννομο συμφέρον να διατηρεί προσωπικά δεδομένα φοιτητών για επιστημονικούς/ιστορικούς/στατιστικούς σκοπούς. Σε τέτοια περίπτωση πρώην φοιτητής έχει δικαίωμα να εναντιωθεί

41

- **Δικαίωμα αντίρρησης 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 το επηρεάζει σημαντικά

➢ Ισχύει και για απόφαση που λαμβάνεται με μη αυτοματοποιημένα μέσα (Κατευθυντήριες Γραμμές Άρθρου 29)

Π.χ. το υποκείμενο δικαιούται να αντιταχθεί σε αυτοματοποιημένη επεξεργασία για την αξιολόγηση προσωπικών πτυχών του όπως την υγεία, αξιοπιστία, τις προσωπικές του προτιμήσεις, επίδοση στην εργασία

Π.χ. το παιδί δικαιούται να μην υπόκειται σε απόφαση που λαμβάνεται με αυτοματοποιημένα ή μη μέσα π.χ. στο σχολείο ή σε εξωσχολικές δραστηριότητες

42

- ΔΕΝ μπορεί να ασκηθεί το δικαίωμα, όταν η απόφαση:

  (α) είναι αναγκαία για την εκτέλεση σύμβασης*. Π.χ. σύμβαση εργασίας, σύμβαση για παροχή υπηρεσιών από τράπεζα, ασφαλιστική εταιρεία

  (β) επιτρέπεται από νόμο

  (γ) βασίζεται σε συγκατάθεση για απλά δεδομένα*. Π.χ. φυσικό πρόσωπο δίνει τα στοιχεία επικοινωνίας σε πάροχο τηλεπικοινωνιακών υπηρεσιών για να γίνει συνδρομητής και λαμβάνεται απόφαση ότι η σύνδεση στο διαδίκτυο δεν καλύπτει τη γεωγραφική περιοχή του

* *σε τέτοια περίπτωση, ο υπεύθυνος επεξεργασίας εφαρμόζει άλλα μέτρα για την προστασία των δικαιωμάτων, ελευθεριών και συμφερόντων των υποκειμένων π.χ. έκφραση άποψης και αμφισβήτησης της απόφασης*

43

- Επιτρέπεται η λήψη αυτοματοποιημένης απόφασης που αφορά ειδικές κατηγορίες δεδομένων μόνο εάν η επεξεργασία τους βασίστηκε στη συγκατάθεση ή στο δημόσιο συμφέρον/δημόσια εξουσία

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

44

Αυστηρότατες Υποχρεώσεις Υπεύθυνων Επεξεργασίας

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

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

2. 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

45

3. Υποχρέωση κατασκευαστών στο στάδιο του σχεδιασμού 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 (Πρ. 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 στο βαθμό που επιτρέπει ο Κανονισμός

46

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

47

6. 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 ΚΜ όπου βρίσκονται τα υποκείμενα των δεδομένων, των οποίων επεξεργάζεται τα δεδομένα τους (για προσφορά αγαθών ή υπηρεσιών ή των οποίων παρακολουθεί τη συμπεριφορά τους)

48

7. Τήρηση αρχείων των δραστηριοτήτων επεξεργασίας (records of processing activities) (Άρθρο 30)

- Ο υπεύθυνος επεξεργασίας και ο εκτελών **έχουν υποχρέωση να τηρούν εγγράφως ή ηλεκτρονικά** αρχείο δραστηριοτήτων
- Οι πληροφορίες στο εν λόγω αρχείο είναι αντίστοιχες με αυτές που περιλαμβάνει το υφιστάμενο έντυπο Γνωστοποίησης
- Το αρχείο τίθεται στη διάθεση της ΑΠΔΠΧ κατόπιν αιτήματος της για άσκηση των αρμοδιοτήτων της
- 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

49

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

50

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

- Ο υπεύθυνος επεξεργασίας σε περίπτωση παραβίασης προσωπικών δεδομένων γνωστοποιεί αμέσως και όχι περάν των **72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος, την παραβίαση στην ΑΠΔΠΧ, 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 τουλάχιστο:
  (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

51

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

- Η παραβίαση ανακοινώνεται αμέσως στο επηρεαζόμενο άτομο όταν υπάρχει ψηλός 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

52

11. Εκτίμηση Αντικτύπου (ΕΑ) (impact assessment) (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

53

- 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

54

- 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

- Ο υπεύθυνος επεξεργασίας είναι αρμόδιος να **επιλέξει τη μεθοδολογία της ΕΑ** (*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

55

➢ **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*

56

➢ **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
- ΚΚΒΠ σε δημόσιους / ιδιωτικούς χώρους

57

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

58

Τι περιλαμβάνει η Εκτίμηση Αντικτύπου

59

➢ **Παραδείγματα επεξεργασιών που ενδεχομένως να μην απαιτείται ΕΑ:**

- Ιδιώτης δικηγόρος που επεξεργάζεται δεδομένα των πελατών του
- 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**

60

- 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 - παράταση 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

61

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

62

- 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

63

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

64

- 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 την επεξεργασία του στο φορέα πιστοποίησης ή στο Γραφείο μου κάθε πληροφορία και πρόσβαση στα αρχεία του που απαιτείται για τη διεξαγωγή της διαδικασίας πιστοποίησης

65

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)

66

- 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 Πρ. 79, 81.

67

Τι καταργείται!

- Γνωστοποιήσεις Σύστασης και Λειτουργίας Αρχείου/Έναρξης Επεξεργασίας – αντικαθίστανται με την τήρηση Αρχείου Δραστηριοτήτων της επεξεργασίας
- Άδεια για επεξεργασία ευαίσθητων δεδομένων *(νυν ειδικών κατηγοριών προσωπικών δεδομένων)* στον τομέα του εργατικού δικαίου
- Άδεια για διασύνδεση αρχείων
- Έκδοση Απόφασης από την Επίτροπο για άρση της υποχρέωσης ενημέρωσης των υποκειμένων των δεδομένων
- Καταβολή τέλους των €17 από τα υποκείμενα για άσκηση του δικαιώματος πρόσβασης και αντίρρησης

68

Τι αλλάζει!

- Άδειες 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

69

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 κμ, 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 κμ.*

70

- **Επιτρέπεται η διαβίβαση χωρίς Άδεια** όταν τρίτη χώρα:
- Εξασφαλίζει ικανοποιητικό επίπεδο προστασίας (με Απόφαση της Ευρωπαϊκής Επιτροπής)
- Δεν εξασφαλίζει μεν ικανοποιητικό επίπεδο προστασίας αλλά υπάρχουν επαρκείς εγγυήσεις:

(α) νομικά δεσμευτικό μέσο μεταξύ δημόσιων αρχών π.χ. πολυμερής συμφωνία, FATCA 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 **εκδίδονται από το Γραφείο μου** και **εγκρίνονται από την Επιτροπή** ή

(ε) κώδικα δεοντολογίας, **ο οποίος εγκρίνεται από το Γραφείο μου** ή από το Συμβούλιο Προστασίας Δεδομένων, εάν αφορά διάφορα κμ

(στ) μηχανισμό πιστοποίησης, **ο οποίος εγκρίνεται από το Γραφείο μου** ή τον εθνικό οργανισμό πιστοποίησης ή και από τους δύο

71

- **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 κλπ

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

72

Διοικητικά πρόστιμα

- Αυστηρότατα πρόστιμα, **με ανώτατο όριο: €10.000.000 ή 2% του παγκόσμιου κύκλου εργασιών** για παραβιάσεις που αφορούν, μεταξύ άλλων:
  - στις υποχρεώσεις σχετικά με την συγκατάθεση ανηλίκων
  - στις υποχρεώσεις του υπεύθυνου επεξεργασίας σχετικά με την εκτέλεση καθηκόντων του ΥΠΔ
  - στην προστασία των προσωπικών δεδομένων από τον σχεδιασμό και εξ ορισμού
- **Το ανώτατο όριο είναι €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,

73

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)*

74

Εξουσίες Επιτρόπου (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)

75

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;

76

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;

77

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;

78

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

79

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;

80

11. Σε περίπτωση διασυνοριακής επεξεργασίας, εντός της ΕΕ, ορισμός του κμ 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;

81

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;

82

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 συγκατάθεση είναι η νομική βάση της επεξεργασίας, 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

83

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

84

Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Ιάσονος 1, 1082 Λευκωσία
Τ.Θ. 23378, 1682 Λευκωσία

Τηλ: 22818456, Φαξ: 22304565
E-mail: commissioner@dataprotection.gov.cy

www.dataprotection.gov.cy

85