Κατευθυντήριες γραμμές 4/2019 σύμφωνα με το άρθρο 25

Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

Έκδοση 2.0

Εκδόθηκε στις 20 Οκτωβρίου 2020

Ιστορικό έκδοσης

Έκδοση 1.0	13 Νοεμβρίου 2019	Έγκριση κατευθυντήριων γραμμών για δημόσια διαβούλευση
Έκδοση 2.0	20 Οκτωβρίου 2020	Έγκριση των κατευθυντήριων γραμμών από το ΕΣΠΔ μετά από δημόσια διαβούλευση

Πίνακας περιεχομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (εφεξής «ΓΚΠΔ»),

Έχοντας υπόψη τη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο και ιδίως το παράρτημα XI και το πρωτόκολλο 37 αυτής, όπως τροποποιήθηκαν με την απόφαση της Μικτής Επιτροπής του ΕΟΧ αριθ. 154/2018, της 6ης Ιουλίου 2018,

Έχοντας υπόψη το άρθρο 12 και το άρθρο 22 του εσωτερικού κανονισμού του

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

<u>Περίληψη</u>

Σε έναν ολοένα και πιο ψηφιακό κόσμο, η τήρηση των απαιτήσεων της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού διαδραματίζει καθοριστικό ρόλο στην προαγωγή της προστασίας της ιδιωτικής ζωής και των δεδομένων στην κοινωνία. Επιβάλλεται επομένως οι υπεύθυνοι επεξεργασίας να λάβουν σοβαρά υπόψη τους αυτήν την ευθύνη και να εφαρμόσουν τις υποχρεώσεις τους σε σχέση με τον ΓΚΠΔ κατά τον σχεδιασμό των πράξεων επεξεργασίας.

Οι παρούσες κατευθυντήριες γραμμές παρέχουν γενικές οδηγίες σχετικά με την υποχρέωση προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (εφεξής «ΠΔΣΕΟ»), όπως ορίζεται στο άρθρο 25 του ΓΚΠΔ. Η ΠΔΣΕΟ συνιστά υποχρέωση για όλους τους υπεύθυνους επεξεργασίας, ανεξαρτήτως μεγέθους και βαθμού πολυπλοκότητας της επεξεργασίας. Για να μπορεί ο υπεύθυνος επεξεργασίας να εφαρμόζει τις απαιτήσεις ΠΔΣΕΟ, είναι εξαιρετικά σημαντικό να κατανοεί τις αρχές της προστασίας δεδομένων και τα δικαιώματα και ελευθερίες του υποκειμένου των δεδομένων.

Η βασική υποχρέωση είναι η εφαρμογή των *κατάλληλων* μέτρων και των απαραίτητων εγγυήσεων που παρέχουν *αποτελεσματική εφαρμογή* των *αρχών της προστασίας δεδομένων και,* κατά συνέπεια*, των δικαιωμάτων και ελευθεριών των υποκειμένων ήδη από τον σχεδιασμό και εξ ορισμού*. Το άρθρο 25 ορίζει τόσο τα στοιχεία του σχεδιασμού όσο και εκείνα εξ ορισμού που πρέπει να λαμβάνονται υπόψη. Τα εν λόγω στοιχεία εξετάζονται περαιτέρω στις παρούσες κατευθυντήριες γραμμές.

Το άρθρο 25 παράγραφος 1 ορίζει ότι οι υπεύθυνοι επεξεργασίας πρέπει να εξετάζουν την ΠΔΣΕΟ νωρίς ενόσω σχεδιάζουν μια νέα πράξη επεξεργασίας. Οι υπεύθυνοι επεξεργασίας εφαρμόζουν την ΠΔΣΕΟ *πριν από* την επεξεργασία αλλά και κατά την διάρκεια της επεξεργασίας, ελέγχοντας τακτικά την αποτελεσματικότητα των επιλεχθέντων μέτρων και εγγυήσεων. Η ΠΔΣΕΟ ισχύει επίσης και για τα υφιστάμενα συστήματα τα οποία επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

Οι κατευθυντήριες γραμμές περιλαμβάνουν επίσης οδηγίες σχετικά με την αποτελεσματική εφαρμογή των αρχών της προστασίας των δεδομένων που προβλέπονται στο άρθρο 5, απαριθμώντας κύρια στοιχεία σχεδιασμού και εξ ορισμού, καθώς και πρακτικές περιπτώσεις ως ενδεικτικά παραδείγματα. Ο υπεύθυνος επεξεργασίας πρέπει να εξετάζει την καταλληλότητα των προτεινόμενων μέτρων στο πλαίσιο της εκάστοτε επεξεργασίας.

Το ΕΣΠΔ διατυπώνει συστάσεις σχετικά με τον τρόπο που οι υπεύθυνοι επεξεργασίας, οι εκτελούντες την επεξεργασία και οι παραγωγοί μπορούν να συνεργαστούν για την επίτευξη της ΠΔΣΕΟ. Ενθαρρύνει τους υπεύθυνους επεξεργασίας του κλάδου, τους εκτελούντες την επεξεργασία και τους παραγωγούς να χρησιμοποιούν την ΠΔΣΕΟ ως μέσο για την εξασφάλιση ενός ανταγωνιστικού πλεονεκτήματος κατά την εμπορική προώθηση των προϊόντων τους προς υπεύθυνους επεξεργασίας και υποκείμενα των δεδομένων. Ενθαρρύνει επίσης όλους τους υπεύθυνους επεξεργασίας να χρησιμοποιούν πιστοποιήσεις και κώδικες δεοντολογίας.

1 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

1. Οι κατευθυντήριες γραμμές εστιάζουν στην εφαρμογή της ΠΔΣΕΟ από τους υπεύθυνους επεξεργασίας, με βάση την υποχρέωση του άρθρου 25 του ΓΚΠΔ.[1] Άλλοι φορείς, όπως οι εκτελούντες την επεξεργασία και οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών (εφεξής «παραγωγοί»), οι οποίοι δεν ρυθμίζονται άμεσα στο άρθρο 25, μπορούν επίσης να θεωρήσουν χρήσιμες τις παρούσες κατευθυντήριες γραμμές κατά τη δημιουργία προϊόντων και υπηρεσιών συμβατών με τον ΓΚΠΔ, τα οποία επιτρέπουν στους υπεύθυνους επεξεργασίας να εκπληρώνουν τις υποχρεώσεις τους σε σχέση με την προστασία των δεδομένων.[2] Η αιτιολογική σκέψη 78 του ΓΚΠΔ προσθέτει ότι η ΠΔΣΕΟ θα πρέπει να λαμβάνεται υπόψη στο πλαίσιο των δημόσιων διαγωνισμών. Παρά το γεγονός ότι όλοι οι υπεύθυνοι επεξεργασίας έχουν το καθήκον να ενσωματώσουν την ΠΔΣΕΟ στις δραστηριότητες επεξεργασίας τους, η διάταξη αυτή ενθαρρύνει την εφαρμογή των αρχών της προστασίας δεδομένων, όπου οι δημόσιες διοικήσεις θα πρέπει να δίνουν το παράδειγμα. Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για την εκπλήρωση των υποχρεώσεων ΠΔΣΕΟ σε ό,τι αφορά την επεξεργασία που διενεργείται από τους εκτελούντες και υπο-εκτελούντες την επεξεργασία, γεγονός που πρέπει να λαμβάνεται υπόψη κατά τη σύναψη σύμβασης με αυτούς.

2. Η απαίτηση που περιγράφεται στο άρθρο 25 προϋποθέτει τη μέριμνα των υπευθύνων επεξεργασίας για συμπερίληψη της προστασίας των δεδομένων ήδη από τον σχεδιασμό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα αλλά και ως εξ ορισμού ρύθμιση, και αυτό ισχύει για το σύνολο του κύκλου ζωής της επεξεργασίας. Η ΠΔΣΕΟ αποτελεί επίσης απαίτηση για συστήματα επεξεργασίας που προϋπήρχαν της έναρξης ισχύος του ΓΚΠΔ. Οι υπεύθυνοι επεξεργασίας πρέπει να φροντίζουν για τη συνεπή επικαιροποίηση της επεξεργασίας σύμφωνα με τον ΓΚΠΔ. Για περισσότερες πληροφορίες σχετικά με τη διατήρηση ενός υφιστάμενου συστήματος το οποίο να είναι σύμφωνο προς την ΠΔΣΕΟ, βλ. υποκεφάλαιο 2.1.4 των παρουσών κατευθυντήριων γραμμών.

[1] Οι ερμηνείες που προβλέπονται στο παρόν ισχύουν εξίσου για το άρθρο 20 της οδηγίας (ΕΕ) 2016/680, και το άρθρο 27 του κανονισμού 2018/1725.

[2] Η αιτιολογική σκέψη 78 του ΓΚΠΔ αναφέρει σαφώς αυτή την ανάγκη: «*Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των «τελευταίων εξελίξεων», να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων*».

Η ουσία της διάταξης είναι η διασφάλιση *κατάλληλης* και *αποτελεσματικής* προστασίας δεδομένων τόσο ήδη από τον *σχεδιασμό* όσο και εξ *ορισμού*, γεγονός που σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να είναι σε θέση να αποδείξουν ότι εφαρμόζουν τα κατάλληλα μέτρα και εγγυήσεις κατά την επεξεργασία ώστε να διασφαλίζεται ότι οι αρχές προστασίας των δεδομένων και τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων είναι αποτελεσματικά.

3. Το δεύτερο κεφάλαιο των κατευθυντήριων γραμμών εστιάζει σε μια ερμηνεία των απαιτήσεων που καθορίζονται στο άρθρο 25 και διερευνά τις νομικές υποχρεώσεις που απορρέουν από τη διάταξη. Παραδείγματα όσον αφορά τον τρόπο της εφαρμογής της ΠΔΣΕΟ στο πλαίσιο συγκεκριμένων αρχών προστασίας των δεδομένων αναφέρονται στο τρίτο κεφάλαιο.

4. Οι κατευθυντήριες γραμμές εξετάζουν τη δυνατότητα θέσπισης ενός μηχανισμού πιστοποίησης για την απόδειξη της συμμόρφωσης προς το άρθρο 25, στο τέταρτο κεφάλαιο, καθώς και πώς μπορεί το άρθρο να επιβάλλεται από τις εποπτικές αρχές, στο πέμπτο κεφάλαιο. Τέλος, οι κατευθυντήριες γραμμές παρέχουν στους ενδιαφερόμενους φορείς περαιτέρω συστάσεις σχετικά με το πώς μπορούν να εφαρμόζουν επιτυχώς την ΠΔΣΕΟ. Το ΕΣΠΔ αναγνωρίζει τις προκλήσεις για τις μικρομεσαίες επιχειρήσεις (εφεξής «ΜΜΕ») προκειμένου να συμμορφώνονται πλήρως προς τις υποχρεώσεις της ΠΔΣΕΟ και παρέχει συμπληρωματικές συστάσεις ειδικά για τις ΜΜΕ στο έκτο κεφάλαιο.

2 ΑΝΑΛΥΣΗ ΤΟΥ ΑΡΘΡΟΥ 25 ΠΑΡΑΓΡΑΦΟΣ 1 ΚΑΙ ΠΑΡΑΓΡΑΦΟΣ 2 ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΗΔΗ ΑΠΟ ΤΟ ΣΧΕΔΙΑΣΜΟ ΚΑΙ ΕΞ ΟΡΙΣΜΟΥ

5. Σκοπός του παρόντος κεφαλαίου είναι η διερεύνηση και η παροχή καθοδήγησης σχετικά με τις απαιτήσεις προστασίας των δεδομένων ήδη από τον σχεδιασμό, στο άρθρο 25 παράγραφος 1, και προστασίας των δεδομένων εξ ορισμού, στο άρθρο 25 παράγραφος 2, αντίστοιχα. Η προστασία των δεδομένων ήδη από τον σχεδιασμό και η προστασία των δεδομένων εξ ορισμού είναι αλληλοσυμπληρούμενες έννοιες, οι οποίες και αλληλοενισχύονται αμοιβαία. Τα υποκείμενα των δεδομένων ωφελούνται περισσότερο από την προστασία των δεδομένων εξ ορισμού εφόσον ταυτόχρονα εφαρμόζεται και η προστασία των δεδομένων ήδη από τον σχεδιασμό και αντίστροφα.

6. Η ΠΔΣΕΟ συνιστά απαίτηση για όλους τους υπεύθυνους επεξεργασίας, συμπεριλαμβανομένων των μικρομεσαίων επιχειρήσεων, όπως και των πολυεθνικών εταιρειών. Με δεδομένη αυτή την απαίτηση, η πολυπλοκότητα της εφαρμογής της ΠΔΣΕΟ ενδέχεται να ποικίλλει ανάλογα με την εκάστοτε πράξη επεξεργασίας. Ωστόσο, ανεξαρτήτως μεγέθους, η εφαρμογή της ΠΔΣΕΟ μπορεί σε κάθε περίπτωση να αποβαίνει προς όφελος τόσο του υπεύθυνου επεξεργασίας όσο και του υποκειμένου των δεδομένων.

2.1 Άρθρο 25 παράγραφος 1: Προστασία των δεδομένων ήδη από τον σχεδιασμό

2.1.1 Υποχρέωση του υπεύθυνου επεξεργασίας να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, καθώς και τις αναγκαίες εγγυήσεις κατά την επεξεργασία

7. Σύμφωνα με το άρθρο 25 παράγραφος 1, ο υπεύθυνος επεξεργασίας εφαρμόζει *κατάλληλα* τεχνικά και οργανωτικά *μέτρα* σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων και την ενσωμάτωση των *απαραίτητων εγγυήσεων* στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις και να προστατεύονται τα δικαιώματα και οι ελευθερίες των υποκειμένων των

δεδομένων. Τα κατάλληλα μέτρα καθώς και οι απαραίτητες εγγυήσεις αποσκοπούν στην εξυπηρέτηση του ίδιου σκοπού της προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων και της εξασφάλισης ότι η προστασία των δεδομένων προσωπικού χαρακτήρα τους είναι ενσωματωμένη στην επεξεργασία.

8. *Τα τεχνικά και οργανωτικά μέτρα* και οι απαραίτητες *εγγυήσεις* μπορούν να λογίζονται υπό μια ευρεία έννοια ως οποιαδήποτε μέθοδος ή μέσο που μπορεί να χρησιμοποιήσει ένας υπεύθυνος επεξεργασίας κατά την επεξεργασία. *Κατάλληλα* σημαίνει ότι τα μέτρα και οι απαραίτητες εγγυήσεις πρέπει να ενδείκνυνται προκειμένου να επιτυγχάνεται ο επιδιωκόμενος σκοπός, ήτοι πρέπει να υλοποιούν τις αρχές προστασίας των δεδομένων *αποτελεσματικά*[3]. Η απαίτηση της καταλληλότητας συνδέεται επομένως στενά με την απαίτηση της αποτελεσματικότητας.

9. Ένα τεχνικό ή οργανωτικό μέτρο και εγγύηση μπορεί να είναι οτιδήποτε, από τη χρήση προηγμένων τεχνικών λύσεων έως τη βασική εκπαίδευση του προσωπικού. Παραδείγματα που μπορεί να είναι κατάλληλα, αναλόγως του πλαισίου και των κινδύνων που συνδέονται με την εκάστοτε επεξεργασία, είναι: η ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα[4]· η αποθήκευση διαθέσιμων δεδομένων προσωπικού χαρακτήρα σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο· η παροχή δυνατότητας των υποκειμένων των δεδομένων να παρεμβαίνουν στην επεξεργασία· η παροχή πληροφοριών σχετικά με την αποθήκευση δεδομένων προσωπικού χαρακτήρα· η πρόβλεψη συστημάτων ανίχνευσης κακόβουλου λογισμικού· η κατάρτιση υπαλλήλων σχετικά με τη βασική «υγιεινή στον κυβερνοχώρο»· η καθιέρωση συστημάτων διαχείρισης απορρήτου και ασφάλειας των πληροφοριών, τα οποία υποχρεώνουν συμβατικά τους εκτελούντες την επεξεργασία να εφαρμόζουν συγκεκριμένες πρακτικές ελαχιστοποίησης δεδομένων κλπ.

10. Στον προσδιορισμό των κατάλληλων μέτρων μπορούν να βοηθούν πρότυπα, βέλτιστες πρακτικές και κώδικες δεοντολογίας που αναγνωρίζονται από ενώσεις και άλλους φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας. Ωστόσο, ο υπεύθυνος επεξεργασίας πρέπει να ελέγχει την καταλληλότητα των μέτρων στο πλαίσιο της εκάστοτε επεξεργασίας.

2.1.2 Τα μέτρα είναι σχεδιασμένα για την εφαρμογή των αρχών της προστασίας των δεδομένων με αποτελεσματικό τρόπο και για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων.

11. Οι *αρχές προστασίας των δεδομένων* περιέχονται στο άρθρο 5 (εφεξής «οι αρχές»). Τα *δικαιώματα και ελευθερίες των υποκειμένων των δεδομένων* είναι τα θεμελιώδη δικαιώματα των φυσικών προσώπων, και ιδιαίτερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα, η προστασία του οποίου μνημονεύεται στο άρθρο 1 παράγραφος 2 ως ο στόχος του ΓΚΠΔ (εφεξής «τα δικαιώματα»)[5]. Η ακριβής διατύπωσή τους περιέχεται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Είναι σημαντικό για τον υπεύθυνο επεξεργασίας να κατανοεί το νόημα *των αρχών* και *των δικαιωμάτων* ως τη βάση για την προστασία που παρέχεται από τον ΓΚΠΔ και ειδικά από την υποχρέωση ΠΔΣΕΟ.

[3] Η «αποτελεσματικότητα» εξετάζεται παρακάτω στο υποκεφάλαιο 2.1.2
[4] Ορίζεται στο άρθρο 4 παράγραφος 5 του ΓΚΠΔ.
[5] Βλ. αιτιολογική σκέψη 4 του ΓΚΠΔ.

12. Κατά την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων, τα μέτρα και οι εγγυήσεις πρέπει να *σχεδιάζονται* λαμβανομένης υπόψη της αποτελεσματικής εφαρμογής κάθε μίας από τις προαναφερθείσες αρχές και της απορρέουσας προστασίας των δικαιωμάτων.

Εξέταση της αποτελεσματικότητας

13. Η αποτελεσματικότητα βρίσκεται στο επίκεντρο της έννοιας της προστασίας των δεδομένων ήδη από τον σχεδιασμό. Η απαίτηση περί εφαρμογής των αρχών με αποτελεσματικό τρόπο σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να εφαρμόζουν τα αναγκαία μέτρα και εγγυήσεις ώστε να προστατεύουν αυτές τις αρχές, προκειμένου να διασφαλίζονται τα δικαιώματα των υποκειμένων των δεδομένων. Κάθε εφαρμοζόμενο μέτρο θα πρέπει να παράγει τα επιδιωκόμενα αποτελέσματα για την επεξεργασία που προβλέπεται από τον υπεύθυνο επεξεργασίας. Αυτή η παρατήρηση έχει δύο συνέπειες.

14. Πρώτον, σημαίνει ότι το άρθρο 25 δεν απαιτεί την εφαρμογή συγκεκριμένων τεχνικών και οργανωτικών μέτρων, αλλά ότι τα επιλεγόμενα μέτρα και εγγυήσεις θα πρέπει να αφορούν ειδικά την εφαρμογή των αρχών προστασίας των δεδομένων στο πλαίσιο της εκάστοτε επεξεργασίας. Ως εκ τούτου, τα μέτρα και οι εγγυήσεις θα πρέπει να σχεδιάζονται με τρόπο ώστε να είναι άρτια και ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να εφαρμόζει περαιτέρω μέτρα ώστε να έχει τη δυνατότητα να προσαρμόζεται σε τυχόν αύξηση του κινδύνου[6]. Ο βαθμός αποτελεσματικότητας των μέτρων θα εξαρτάται, κατά συνέπεια, από το πλαίσιο της εκάστοτε επεξεργασίας και από μια αξιολόγηση ορισμένων στοιχείων που πρέπει να λαμβάνονται υπόψη κατά τον προσδιορισμό των μέσων επεξεργασίας. Τα προαναφερθέντα στοιχεία εξετάζονται κατωτέρω στο υποκεφάλαιο 2.1.3.

15. Δεύτερον, οι υπεύθυνοι επεξεργασίας θα πρέπει να μπορούν να αποδείξουν ότι οι αρχές έχουν τηρηθεί.

16. Τα εφαρμοζόμενα μέτρα και εγγυήσεις θα πρέπει να επιτυγχάνουν το επιθυμητό αποτέλεσμα από πλευράς προστασίας δεδομένων και ο υπεύθυνος επεξεργασίας θα πρέπει να διαθέτει τεκμηρίωση των εφαρμοζόμενων τεχνικών και οργανωτικών μέτρων.[7] Για να το επιτύχει αυτό, ο υπεύθυνος επεξεργασίας μπορεί να καθορίζει τους κατάλληλους δείκτες επιδόσεων για την απόδειξη της αποτελεσματικότητας. Ένας δείκτης επίδοσης συνιστά μετρήσιμη τιμή που επιλέγεται από τον υπεύθυνο επεξεργασίας, η οποία καταδεικνύει το πόσο αποτελεσματικά επιτυγχάνει ο υπεύθυνος επεξεργασίας τον στόχο του σε ό,τι αφορά την προστασία των δεδομένων. Οι δείκτες επιδόσεων μπορούν να είναι *ποσοτικοί*, όπως το ποσοστό των ψευδώς θετικών ή ψευδώς αρνητικών αποτελεσμάτων, η μείωση των καταγγελιών, η μείωση του χρόνου απάντησης όταν τα υποκείμενα των δεδομένων ασκούν τα δικαιώματά τους, ή να είναι *ποιοτικοί*, όπως αξιολογήσεις επιδόσεων, χρήση κλιμάκων βαθμολόγησης ή αξιολόγηση από εμπειρογνώμονες. Εναλλακτικά προς τους δείκτες επιδόσεων, οι υπεύθυνοι επεξεργασίας μπορούν ενδεχομένως να αποδεικνύουν την αποτελεσματική εφαρμογή των αρχών δηλώνοντας το σκεπτικό τους πίσω από την αξιολόγηση της αποτελεσματικότητας των επιλεγόμενων μέτρων και εγγυήσεων.

---

[6] «Οι θεμελιώδεις αρχές που ισχύουν για τους υπεύθυνους επεξεργασίας (δηλαδή νομιμότητα, ελαχιστοποίηση δεδομένων, περιορισμός του σκοπού, διαφάνεια, ακεραιότητα δεδομένων, ακρίβεια δεδομένων) θα πρέπει να παραμείνουν οι ίδιες, ανεξάρτητα από το είδος της επεξεργασίας και τους κινδύνους για τα υποκείμενα των δεδομένων. Ωστόσο, η φύση και το εύρος της εν λόγω επεξεργασίας αποτελούν πάντα αναπόσπαστο μέρος της εφαρμογής αυτών των αρχών, ώστε να είναι εγγενώς κλιμακούμενες.» Δήλωση της ομάδας εργασίας του άρθρου 29 σχετικά με τον ρόλο μιας προσέγγισης βασισμένης στους κινδύνους στα νομικά πλαίσια για την προστασία των δεδομένων. WP 218, 30 Μαΐου 2014, σ. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Βλ. αιτιολογικές σκέψεις 74 και 78.

2.1.3 Στοιχεία που πρέπει να λαμβάνονται υπόψη

17. Το άρθρο 25 παράγραφος 1 απαριθμεί τα στοιχεία που πρέπει να λαμβάνει υπόψη ο υπεύθυνος επεξεργασίας κατά τον καθορισμό των μέτρων μιας συγκεκριμένης πράξης επεξεργασίας. Στη συνέχεια, παρέχεται καθοδήγηση σχετικά με τον τρόπο εφαρμογής αυτών των στοιχείων στη διαδικασία σχεδιασμού, η οποία περιλαμβάνει και τον σχεδιασμό των προεπιλεγμένων ρυθμίσεων. Όλα τα εν λόγω στοιχεία συνεισφέρουν στο να διαπιστώνεται εάν ένα μέτρο είναι κατάλληλο για την αποτελεσματική εφαρμογή των αρχών. Ως εκ τούτου, κάθε ένα από τα εν λόγω στοιχεία δεν αποτελεί αυτοσκοπό αλλά παράγοντα που πρέπει να συνυπολογίζεται για την επίτευξη του στόχου.

2.1.3.1 «τελευταίες εξελίξεις»

18. Η έννοια «τελευταίες εξελίξεις» είναι παρούσα σε διάφορα κεκτημένα της ΕΕ, π.χ. προστασία του περιβάλλοντος και ασφάλεια των προϊόντων. Στον ΓΚΠΔ, η αναφορά στις «τελευταίες εξελίξεις»[8] δεν γίνεται μόνο στο άρθρο 32 για τα μέτρα ασφαλείας,[9][10] αλλά και στο άρθρο 25, επεκτείνοντας έτσι αυτό το σημείο αναφοράς σε όλα τα τεχνικά και οργανωτικά μέτρα που ενσωματώνονται στην επεξεργασία.

19. Στο πλαίσιο του άρθρου 25, η αναφορά στις «τελευταίες εξελίξεις» επιβάλλει στους υπεύθυνους επεξεργασίας, κατά τον καθορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων, **να λαμβάνουν υπόψη την τρέχουσα πρόοδο της τεχνολογίας** που είναι διαθέσιμη στην αγορά. Η απαίτηση συνεπάγεται ότι οι υπεύθυνοι επεξεργασίας πρέπει να γνωρίζουν και να ενημερώνονται σχετικά με τις τεχνολογικές εξελίξεις, τους τρόπους με τους οποίους η τεχνολογία μπορεί να παρουσιάζει κινδύνους ή ευκαιρίες για την προστασία των δεδομένων κατά την πράξη επεξεργασίας, καθώς και τον τρόπο εφαρμογής και επικαιροποίησης των μέτρων και εγγυήσεων *που εξασφαλίζουν την αποτελεσματική εφαρμογή* των αρχών και των δικαιωμάτων των υποκειμένων των δεδομένων, λαμβανομένου υπόψη του εξελισσόμενου τεχνολογικού τοπίου.

20. Οι «τελευταίες εξελίξεις» αποτελούν μια δυναμική έννοια που δεν μπορεί να οριστεί στατικά σε καθορισμένο χρονικό σημείο, αλλά θα πρέπει να αξιολογείται *συνεχώς* στο πλαίσιο της τεχνολογικής προόδου. Ενόψει των τεχνολογικών εξελίξεων, ο υπεύθυνος επεξεργασίας θα μπορούσε να διαπιστώσει ότι ένα μέτρο που παρείχε κατάλληλο επίπεδο προστασίας δεν το παρέχει πλέον. Η μη παρακολούθηση των τεχνολογικών αλλαγών θα μπορούσε συνεπώς να οδηγήσει σε μη συμμόρφωση με το άρθρο 25.

21. Το κριτήριο των «τελευταίων εξελίξεων» δεν ισχύει μόνο για τα τεχνολογικά, αλλά και για τα οργανωτικά μέτρα. Η έλλειψη κατάλληλων οργανωτικών μέτρων μπορεί να μειώσει ή και να υπονομεύσει εντελώς την αποτελεσματικότητα μιας επιλεγμένης τεχνολογίας. Παραδείγματα οργανωτικών μέτρων μπορούν να είναι η έγκριση εσωτερικών πολιτικών, η επικαιροποιημένη κατάρτιση σε θέματα τεχνολογίας, ασφάλειας και προστασίας των δεδομένων, καθώς και οι πολιτικές διακυβέρνησης και διαχείρισης της ασφάλειας ΤΠ.

---

[8] Βλ. απόφαση «Kalkar» του γερμανικού Ομοσπονδιακού Συνταγματικού Δικαστηρίου του 1978: https://germanlawarchive.iuscomp.org/?p=67 μπορεί να αποτελέσει τη βάση μιας μεθοδολογίας για έναν αντικειμενικό ορισμό της έννοιας. Σε αυτή τη βάση, το τεχνολογικό επίπεδο των «τελευταίων εξελίξεων» θα προσδιορίζεται μεταξύ του τεχνολογικού επιπέδου των «υφιστάμενων επιστημονικών γνώσεων και έρευνας» και των πιο καθιερωμένων «γενικά αποδεκτών κανόνων της τεχνολογίας». Οι «τελευταίες εξελίξεις» μπορούν ως εκ τούτου να προσδιοριστούν ως το επίπεδο τεχνολογίας μιας υπηρεσίας ή τεχνολογίας ή προϊόντος που υπάρχει στην αγορά και είναι πιο αποτελεσματικό για την επίτευξη των επιδιωκόμενων στόχων.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

22. Υφιστάμενα και αναγνωρισμένα πλαίσια, πρότυπα, πιστοποιήσεις, κώδικες δεοντολογίας κλπ. σε διαφορετικά πεδία ενδέχεται να διαδραματίζουν κάποιον ρόλο στον προσδιορισμό των τρεχουσών «τελευταίων εξελίξεων» εντός του δεδομένου πεδίου χρήσης. Εκεί όπου υπάρχουν τέτοια πρότυπα και παρέχουν υψηλό βαθμό προστασίας για το υποκείμενο των δεδομένων σύμφωνα με τις νομικές απαιτήσεις –ή και πέραν αυτών–, οι υπεύθυνοι επεξεργασίας θα πρέπει να τα λαμβάνουν υπόψη κατά τον σχεδιασμό και την εφαρμογή των μέτρων προστασίας των δεδομένων.

2.1.3.2 «κόστος εφαρμογής»

23. Ο υπεύθυνος επεξεργασίας δύναται να λαμβάνει υπόψη το κόστος εφαρμογής κατά την επιλογή και εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων και των αναγκαίων εγγυήσεων για την αποτελεσματική εφαρμογή των αρχών ώστε να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. Το κόστος αναφέρεται γενικά στους πόρους, συμπεριλαμβανομένου του χρόνου και των ανθρώπινων πόρων.

24. Το στοιχείο του κόστους δεν απαιτεί από τον υπεύθυνο επεξεργασίας να δαπανά δυσανάλογη ποσότητα πόρων, όταν υπάρχουν εναλλακτικά αποτελεσματικά μέτρα λιγότερο απαιτητικά από άποψη πόρων. Ωστόσο, το κόστος εφαρμογής αποτελεί παράγοντα που πρέπει να λαμβάνεται υπόψη για την εφαρμογή της προστασίας των δεδομένων ήδη από τον σχεδιασμό και όχι παράγοντα για τη μη εφαρμογή της προστασίας.

25. Ως εκ τούτου, τα επιλεγόμενα μέτρα διασφαλίζουν ότι η δραστηριότητα επεξεργασίας που προβλέπεται από τον υπεύθυνο επεξεργασίας δεν αφορά δεδομένα προσωπικού χαρακτήρα κατά παράβαση των αρχών, ανεξαρτήτως κόστους. Οι υπεύθυνοι επεξεργασίας πρέπει να είναι σε θέση να διαχειρίζονται τα συνολικά έξοδα ώστε να μπορούν να εφαρμόζουν αποτελεσματικά όλες τις αρχές και, κατά συνέπεια, να προστατεύουν τα δικαιώματα.

2.1.3.3 «φύση, πεδίο εφαρμογής, πλαίσιο και σκοπός της επεξεργασίας»

26. Οι υπεύθυνοι επεξεργασίας πρέπει να λαμβάνουν υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τον σκοπό της επεξεργασίας κατά τον προσδιορισμό των αναγκαίων μέτρων.

27. Οι εν λόγω παράγοντες πρέπει να ερμηνεύονται σύμφωνα με τον ρόλο τους σε άλλες διατάξεις του ΓΚΠΔ, όπως τα άρθρα 24, 32 και 35, με σκοπό τον σχεδιασμό των αρχών προστασίας των δεδομένων κατά την επεξεργασία.

28. Συνοπτικά, η έννοια της **φύσης** μπορεί να γίνει κατανοητή ως τα εγγενή[11] χαρακτηριστικά της επεξεργασίας. Το **πεδίο εφαρμογής** αναφέρεται στο μέγεθος και στο εύρος της επεξεργασίας. Το **πλαίσιο** σχετίζεται με τις συνθήκες της επεξεργασίας, οι οποίες ενδέχεται να επηρεάζουν τις προσδοκίες του υποκειμένου των δεδομένων, ενώ ο **σκοπός** αφορά τους σκοπούς της επεξεργασίας.

2.1.3.4 «κίνδυνοι διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία»

29. Ο ΓΚΠΔ υιοθετεί μια συνεκτική προσέγγιση βάσει των κινδύνων σε πολλές από τις διατάξεις του, στα άρθρα 24, 25, 32 και 35, με σκοπό τον καθορισμό των κατάλληλων τεχνικών και οργανωτικών

[11] Σχετικά παραδείγματα είναι οι ειδικές κατηγορίες δεδομένων, η αυτόματη λήψη αποφάσεων, οι άνισες σχέσεις εξουσίας, η απρόβλεπτη επεξεργασία, οι δυσκολίες του υποκειμένου των δεδομένων να ασκήσει τα δικαιώματά του κλπ.

μέτρων για την προστασία των ατόμων και των προσωπικών τους δεδομένων, καθώς και για τη συμμόρφωση προς τις απαιτήσεις του ΓΚΠΔ. Τα αγαθά που προστατεύονται είναι πάντα τα ίδια (τα άτομα, μέσω της προστασίας των προσωπικών τους δεδομένων), έναντι των ίδιων κινδύνων (για τα δικαιώματα των ατόμων), λαμβανομένων υπόψη των ίδιων προϋποθέσεων (φύση, πεδίο εφαρμογής, πλαίσιο και σκοποί επεξεργασίας).

30. Κατά τη διενέργεια της ανάλυσης κινδύνων για τη συμμόρφωση προς το άρθρο 25, ο υπεύθυνος επεξεργασίας οφείλει να εντοπίζει τους κινδύνους που ενέχει για τα δικαιώματα του υποκειμένου των δεδομένων τυχόν παραβίαση των αρχών και να προσδιορίζει την πιθανότητα επέλευσης και τη σοβαρότητά τους ώστε να εφαρμόζει μέτρα για τον αποτελεσματικό μετριασμό των εντοπιζόμενων κινδύνων. Η συστηματική και διεξοδική αξιολόγηση της επεξεργασίας είναι εξαιρετικά σημαντική κατά τη διενέργεια της αξιολόγησης των κινδύνων. Για παράδειγμα, ένας υπεύθυνος επεξεργασίας αξιολογεί τους ιδιαίτερους κινδύνους που σχετίζονται με τυχόν έλλειψη ελεύθερης συγκατάθεσης, γεγονός που συνιστά παραβίαση της αρχής της νομιμότητας, κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα παιδιών και νεαρών ατόμων ηλικίας κάτω των 18 ετών ως ευάλωτης ομάδας, εφόσον δεν υφίσταται κανένας άλλος νομικός λόγος, και εφαρμόζει κατάλληλα μέτρα για την αντιμετώπιση και τον αποτελεσματικό μετριασμό των εντοπιζόμενων κινδύνων που σχετίζονται με την εν λόγω ομάδα υποκειμένων των δεδομένων.

31. Οι «Κατευθυντήριες γραμμές του ΕΣΠΔ για την εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ)»,[12] οι οποίες επικεντρώνονται στον καθορισμό του εάν μια πράξη επεξεργασίας είναι πιθανό να έχει ως αποτέλεσμα υψηλό κίνδυνο για το υποκείμενο των δεδομένων, παρέχουν επίσης καθοδήγηση σχετικά με τον τρόπο αξιολόγησης των κινδύνων για την προστασία των δεδομένων, καθώς και τον τρόπο διενέργειας μιας αξιολόγησης κινδύνου για την προστασία των δεδομένων. Οι εν λόγω κατευθυντήριες γραμμές μπορεί επίσης να είναι χρήσιμες κατά την αξιολόγηση κινδύνου με βάση όλα τα προαναφερθέντα άρθρα, συμπεριλαμβανομένου του άρθρου 25.

32. Η προσέγγιση βάσει των κινδύνων δεν αποκλείει τη χρήση σεναρίων αναφοράς, βέλτιστων πρακτικών και προτύπων. Αυτά μπορεί να παράσχουν ένα χρήσιμο εργαλείο για τους υπεύθυνους επεξεργασίας για την αντιμετώπιση παρόμοιων κινδύνων σε παρόμοιες καταστάσεις (φύση, πεδίο εφαρμογής, πλαίσιο και σκοπός της επεξεργασίας). Ωστόσο, παραμένει η υποχρέωση του άρθρου 25 (καθώς και των άρθρων 24, 32 και 35 παράγραφος 7 στοιχείο γ) να λαμβάνονται υπόψη «*κίνδυνοι διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία*». Επομένως, οι υπεύθυνοι επεξεργασίας, αν και υποστηρίζονται από τα εν λόγω εργαλεία, πρέπει πάντα να διενεργούν αξιολόγηση των κινδύνων για την προστασία των δεδομένων για την εκάστοτε πράξη επεξεργασίας και να επαληθεύουν την αποτελεσματικότητα των προτεινόμενων κατάλληλων μέτρων και εγγυήσεων. Ενδέχεται τότε να απαιτείται επιπλέον μια ΕΑΠΔ ή η επικαιροποίηση μιας υφιστάμενης ΕΑΠΔ.

2.1.4 Χρονική πτυχή

2.1.4.1 Τη στιγμή του καθορισμού των μέσων επεξεργασίας

33. Η προστασία των δεδομένων ήδη από τον σχεδιασμό πρέπει να εφαρμόζεται «*τη στιγμή του προσδιορισμού των μέσων επεξεργασίας*».

[12] «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία "ενδέχεται να επιφέρει υψηλό κίνδυνο" για τους σκοπούς του κανονισμού 2016/679» της ομάδας εργασίας του άρθρου 29. WP 248, αναθ.01, 4 Οκτωβρίου 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 - οι οποίες εγκρίθηκαν από το ΕΣΠΔ

34. Τα «*μέσα επεξεργασίας*» ποικίλλουν από γενικά έως αναλυτικά στοιχεία σχεδιασμού της επεξεργασίας, συμπεριλαμβανομένης της αρχιτεκτονικής, των διαδικασιών, των πρωτοκόλλων, της διάταξης και της εμφάνισης.

35. Η «*στιγμή του προσδιορισμού των μέσων επεξεργασίας*» αναφέρεται στο χρονικό διάστημα κατά το οποίο ο υπεύθυνος επεξεργασίας αποφασίζει πώς θα διενεργηθεί η επεξεργασία, τον τρόπο με τον οποίο θα γίνει και τους μηχανισμούς που θα χρησιμοποιηθούν για τη διενέργεια της επεξεργασίας. Κατά τη διαδικασία λήψης των εν λόγω αποφάσεων, ο υπεύθυνος επεξεργασίας πρέπει να αξιολογήσει τα κατάλληλα μέτρα και εγγυήσεις για την αποτελεσματική εφαρμογή των αρχών και των δικαιωμάτων των υποκειμένων των δεδομένων κατά την επεξεργασία και να λάβει υπόψη του στοιχεία όπως οι τελευταίες εξελίξεις, το κόστος εφαρμογής, η φύση, το πεδίο εφαρμογής, το πλαίσιο και ο σκοπός, καθώς και οι κίνδυνοι. Αυτό περιλαμβάνει και τη στιγμή της παροχής και εφαρμογής λογισμικού, υλισμικού και υπηρεσιών για την επεξεργασία των δεδομένων.

36. Η έγκαιρη εξέταση του ζητήματος της ΠΔΣΕΟ είναι εξαιρετικά σημαντική για την επιτυχή εφαρμογή των αρχών και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Επιπλέον, από την άποψη κόστους/οφέλους, θα ήταν επίσης προς το συμφέρον των υπεύθυνων επεξεργασίας να λαμβάνουν υπόψη την ΠΔΣΕΟ το συντομότερο δυνατόν, καθώς οι μετέπειτα αλλαγές σε σχέδια που έχουν ήδη πραγματοποιηθεί και σε πράξεις επεξεργασίας που έχουν ήδη σχεδιαστεί θα συνιστούσαν πρόκληση και θα ήταν δαπανηρές.

2.1.4.2 Τη στιγμή της ίδιας της επεξεργασίας (διατήρηση και επανεξέταση των απαιτήσεων προστασίας δεδομένων)

37. Εφόσον η επεξεργασία έχει ξεκινήσει, ο υπεύθυνος επεξεργασίας έχει συνεχή υποχρέωση να διατηρεί την ΠΔΣΕΟ, ήτοι τη συνεχιζόμενη αποτελεσματική εφαρμογή των αρχών με σκοπό την προστασία των δικαιωμάτων, την ευθυγράμμιση με τις τελευταίες εξελίξεις, την επαναξιολόγηση του επιπέδου του κινδύνου κλπ. Η φύση, το πεδίο εφαρμογής και το πλαίσιο των πράξεων επεξεργασίας, όπως και ο κίνδυνος, ενδέχεται να αλλάζουν κατά τη διάρκεια της επεξεργασίας, γεγονός που σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να επαναξιολογεί τις πράξεις επεξεργασίας του μέσω τακτικής επανεξέτασης και αξιολογήσεων της αποτελεσματικότητας των μέτρων και εγγυήσεων που έχει επιλέξει.

38. Η υποχρέωση διατήρησης, επανεξέτασης και επικαιροποίησης της πράξης επεξεργασίας, στο μέτρο του αναγκαίου, ισχύει και για τα προϋπάρχοντα συστήματα. Αυτό σημαίνει ότι τα παλαιότερα συστήματα που σχεδιάστηκαν προτού ο ΓΚΠΔ τεθεί σε ισχύ, πρέπει να υπόκεινται σε επανεξέταση και συντήρηση ώστε να διασφαλίζεται η εφαρμογή των μέτρων και των εγγυήσεων που, με τη σειρά τους, διασφαλίζουν την εφαρμογή των αρχών και των δικαιωμάτων των υποκειμένων με αποτελεσματικό τρόπο, όπως περιγράφεται εν γένει στις παρούσες κατευθυντήριες γραμμές.

39. Η υποχρέωση αυτή επεκτείνεται επίσης σε κάθε επεξεργασία που πραγματοποιείται μέσω εκτελούντων την επεξεργασία. Οι πράξεις των εκτελούντων την επεξεργασία θα πρέπει να ελέγχονται και να αξιολογούνται τακτικά από τους υπεύθυνους επεξεργασίας, ώστε να διασφαλίζεται η συνεχής συμμόρφωση προς τις αρχές και να μπορεί ο υπεύθυνος επεξεργασίας να εκπληρώνει τις σχετικές του υποχρεώσεις.

2.2 Άρθρο 25 παράγραφος 2: Προστασία δεδομένων εξ ορισμού

2.2.1 Εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας

40. Ο όρος «εξ ορισμού», όπως ορίζεται συνήθως στην επιστήμη υπολογιστών, αναφέρεται στην προϋπάρχουσα ή προεπιλεγμένη τιμή μιας διαμορφώσιμης ρύθμισης που αντιστοιχεί σε μια εφαρμογή λογισμικού, ένα πρόγραμμα ηλεκτρονικού υπολογιστή ή συσκευή. Οι εν λόγω ρυθμίσεις ονομάζονται επίσης «προκαθορισμένες ρυθμίσεις» ή «εργοστασιακές προκαθορισμένες ρυθμίσεις», ειδικά για τις ηλεκτρονικές συσκευές.

41. Ως εκ τούτου, ο όρος «εξ ορισμού» κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, αναφέρεται σε επιλογές που αφορούν τιμές ρύθμισης παραμέτρων ή σε επιλογές επεξεργασίας που ορίζονται ή προβλέπονται σε ένα σύστημα επεξεργασίας, όπως μια εφαρμογή λογισμικού, υπηρεσία ή συσκευή, ή μια χειροκίνητη διαδικασία επεξεργασίας, οι οποίες επηρεάζουν την ποσότητα των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, την έκταση της επεξεργασίας τους, το διάστημα αποθήκευσης και την προσβασιμότητά τους.

42. Ο υπεύθυνος επεξεργασίας πρέπει να επιλέγει και να λογοδοτεί σχετικά με την εφαρμογή των εξ ορισμού ρυθμίσεων και επιλογών επεξεργασίας με τρόπο ώστε να διενεργείται εξ ορισμού μόνο η επεξεργασία που είναι αυστηρά αναγκαία για την επίτευξη του καθορισμένου νόμιμου σκοπού. Εδώ, οι υπεύθυνοι επεξεργασίας πρέπει να βασίζονται στην εκτίμησή τους σχετικά με την αναγκαιότητα της επεξεργασίας όσον αφορά τους νομικούς λόγους του άρθρου 6 παράγραφος 1. Αυτό σημαίνει ότι εξ ορισμού ο υπεύθυνος επεξεργασίας δεν συλλέγει περισσότερα δεδομένα από όσα είναι αναγκαία, δεν επεξεργάζεται τα δεδομένα περισσότερο από όσο είναι αναγκαίο για τους σκοπούς του και δεν αποθηκεύει τα δεδομένα για διάστημα μεγαλύτερο από το αναγκαίο. Η βασική απαίτηση είναι η ενσωμάτωση της προστασίας δεδομένων στην επεξεργασία εξ ορισμού.

43. Ο υπεύθυνος επεξεργασίας υποχρεούται να καθορίζει εκ των προτέρων για ποιους συγκεκριμένους, σαφείς και νόμιμους σκοπούς συλλέγονται και υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα.[13] Τα μέτρα πρέπει εξ ορισμού να είναι κατάλληλα ώστε να εξασφαλίζεται ότι υποβάλλονται σε επεξεργασία μόνο δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας. Οι κατευθυντήριες γραμμές του ΕΕΠΔ για την αξιολόγηση της αναγκαιότητας και της αναλογικότητας των μέτρων που περιορίζουν το δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα μπορούν επίσης να είναι χρήσιμες για να αποφασίζεται ποια δεδομένα είναι απαραίτητο να υποβληθούν σε επεξεργασία προκειμένου να επιτευχθεί ένας συγκεκριμένος σκοπός.[14] [15] [16]

44. Εάν ο υπεύθυνος επεξεργασίας χρησιμοποιεί λογισμικό τρίτων ή λογισμικό του εμπορίου, πρέπει να διενεργεί αξιολόγηση κινδύνων του προϊόντος και να διασφαλίζει ότι οι λειτουργίες που δεν έχουν

[13] Άρθρο 5 παράγραφος 1 στοιχεία β), γ), δ), ε) του ΓΚΠΔ.
[14] ΕΕΠΔ. «Κατευθυντήριες γραμμές για την αξιολόγηση της αναγκαιότητας και της αναλογικότητας των μέτρων που περιορίζουν το δικαίωμα της προστασίας των δεδομένων». 25 Φεβρουαρίου 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf
[15] Βλ. επίσης ΕΕΠΔ. «Εκτίμηση της αναγκαιότητας μέτρων που περιορίζουν το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα: μια εργαλειοθήκη» https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
[16] Για περισσότερες πληροφορίες σχετικά με την αναγκαιότητα, βλ. ομάδα εργασίας του άρθρου 29. «Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ». WP 217, 9 Απριλίου 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf

νομική βάση ή δεν είναι συμβατές με τους επιδιωκόμενους σκοπούς της επεξεργασίας απενεργοποιούνται.

45. Το ίδιο ισχύει για τα οργανωτικά μέτρα που συνοδεύουν τις πράξεις επεξεργασίας. Πρέπει να σχεδιάζονται για την επεξεργασία, εξ αρχής, μόνο της ελάχιστης ποσότητας των δεδομένων προσωπικού χαρακτήρα που απαιτούνται για τις συγκεκριμένες πράξεις. Αυτό θα πρέπει να λαμβάνεται ιδιαίτερα υπόψη κατά την εκχώρηση πρόσβασης στα δεδομένα σε προσωπικό με διαφορετικούς ρόλους και διαφορετικές ανάγκες πρόσβασης.

46. Τα κατάλληλα «τεχνικά και οργανωτικά μέτρα» στο πλαίσιο της προστασίας των δεδομένων εξ ορισμού ερμηνεύονται ως εκ τούτου με τον τρόπο που αναφέρεται ανωτέρω στο υποκεφάλαιο 2.1.1 αλλά εφαρμόζονται ειδικά στην εφαρμογή της αρχής της ελαχιστοποίησης δεδομένων.

47. Η προαναφερθείσα υποχρέωση επεξεργασίας μόνο των δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό ισχύει για τα ακόλουθα στοιχεία.

2.2.2 Διαστάσεις της υποχρέωσης ελαχιστοποίησης των δεδομένων

48. Το άρθρο 25 παράγραφος 2 απαριθμεί τις διαστάσεις της υποχρέωσης ελαχιστοποίησης των δεδομένων για την εξ ορισμού επεξεργασία, αναφέροντας ότι η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους.

2.2.2.1 «εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται»

49. Οι υπεύθυνοι επεξεργασίας πρέπει να εξετάζουν τόσο τον όγκο των δεδομένων προσωπικού χαρακτήρα, όσο και τους τύπους, τις κατηγορίες και το επίπεδο λεπτομέρειας των δεδομένων προσωπικού χαρακτήρα που απαιτούνται για τους σκοπούς της επεξεργασίας. Οι επιλογές τους όσον αφορά τον σχεδιασμό θα πρέπει να λαμβάνουν υπόψη τους αυξημένους κινδύνους για τις αρχές της ακεραιότητας και της εμπιστευτικότητας, της ελαχιστοποίησης δεδομένων και του περιορισμού της αποθήκευσης κατά τη συλλογή μεγάλου όγκου λεπτομερών δεδομένων προσωπικού χαρακτήρα, καθώς και να τους συγκρίνουν με τη μείωση των κινδύνων όταν συλλέγονται μικρότερες ποσότητες ή/και λιγότερο λεπτομερείς πληροφορίες σχετικά με τα υποκείμενα των δεδομένων. Σε κάθε περίπτωση, η προεπιλεγμένη ρύθμιση δεν πρέπει να περιλαμβάνει συλλογή δεδομένων προσωπικού χαρακτήρα που δεν είναι απαραίτητα για τον συγκεκριμένο σκοπό επεξεργασίας. Με άλλα λόγια, εάν ορισμένες κατηγορίες δεδομένων προσωπικού χαρακτήρα δεν είναι απαραίτητες ή εάν δεν απαιτούνται λεπτομερή δεδομένα, εφόσον αρκούν τα λιγότερο λεπτομερή δεδομένα, τότε δεν θα συλλέγονται τυχόν επιπλέον δεδομένα προσωπικού χαρακτήρα.

50. Οι ίδιες εξ ορισμού απαιτήσεις ισχύουν και για τις υπηρεσίες ανεξαρτήτως της χρησιμοποιούμενης πλατφόρμας ή συσκευής, ενώ μόνο τα απαραίτητα δεδομένα για τον εκάστοτε σκοπό μπορούν να συλλέγονται.

2.2.2.2 «ο βαθμός της επεξεργασίας τους»

51. Οι πράξεις επεξεργασίας[17] δεδομένων προσωπικού χαρακτήρα πρέπει να περιορίζονται σε ό,τι είναι απαραίτητο. Πολλές πράξεις επεξεργασίας μπορούν να συμβάλουν σε έναν σκοπό επεξεργασίας.

[17] Σύμφωνα με το άρθρο 4 παράγραφος 2 του ΓΚΠΔ, αυτό περιλαμβάνει, τη συλλογή, την καταχώριση, την οργάνωση, τη διάρθρωση, την αποθήκευση, την προσαρμογή ή τη μεταβολή, την ανάκτηση, την αναζήτηση

Ωστόσο, το γεγονός ότι ορισμένα δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα για την εκπλήρωση ενός σκοπού δεν σημαίνει ότι μπορούν να εφαρμοστούν όλοι οι τύποι και οι συχνότητες των πράξεων επεξεργασίας στα δεδομένα. Οι υπεύθυνοι επεξεργασίας πρέπει επίσης να προσέχουν να μην επεκτείνουν τα όρια των «συμβατών σκοπών» του άρθρου 6 παράγραφος 4 και να έχουν υπόψη τους ποιο είδος επεξεργασίας θα βρίσκεται εντός των εύλογων προσδοκιών των υποκειμένων των δεδομένων.

2.2.2.3 «περίοδος αποθήκευσης»

52. Τα δεδομένα προσωπικού χαρακτήρα δεν αποθηκεύονται εάν αυτό δεν είναι απαραίτητο για τον σκοπό της επεξεργασίας και δεν υπάρχει άλλος συμβατός σκοπός και νομικός λόγος σύμφωνα με το άρθρο 6 παράγραφος 4. Οποιαδήποτε διατήρηση θα πρέπει να μπορεί να αιτιολογείται αντικειμενικά στον βαθμό που είναι αναγκαίο από τον υπεύθυνο επεξεργασίας σύμφωνα με την αρχή της λογοδοσίας.

53. Ο υπεύθυνος επεξεργασίας περιορίζει το διάστημα διατήρησης σε αυτό που είναι αναγκαίο για τον επιδιωκόμενο σκοπό. Εάν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα για τον σκοπό της επεξεργασίας, τότε θα πρέπει εξ ορισμού να διαγράφονται ή να ανωνυμοποιούνται. Η διάρκεια του διαστήματος διατήρησης εξαρτάται κατά συνέπεια από τον σκοπό της εκάστοτε επεξεργασίας. Η υποχρέωση αυτή συνδέεται άμεσα με την αρχή του περιορισμού της περιόδου αποθήκευσης στο άρθρο 5 παράγραφος 1 στοιχείο ε), και εφαρμόζεται εξ ορισμού, δηλαδή ο υπεύθυνος επεξεργασίας πρέπει να έχει ενσωματώσει στην επεξεργασία συστηματικές διαδικασίες για τη διαγραφή ή την ανωνυμοποίηση των δεδομένων.

54. Η ανωνυμοποίηση[18] δεδομένων προσωπικού χαρακτήρα αποτελεί εναλλακτική λύση για τη διαγραφή, εφόσον λαμβάνονται υπόψη όλα τα εκάστοτε σχετικά στοιχεία και αξιολογείται τακτικά η πιθανότητα και η σοβαρότητα του κινδύνου, συμπεριλαμβανομένου του κινδύνου εκ νέου ταυτοποίησης[19].

2.2.2.4 «η προσβασιμότητά τους»

55. Ο υπεύθυνος επεξεργασίας πρέπει να επιβάλλει περιορισμούς όσον αφορά το ποιος μπορεί να έχει πρόσβαση και τι είδους πρόσβαση σε δεδομένα προσωπικού χαρακτήρα με βάση μια εκτίμηση αναγκαιότητας και, επίσης, να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα είναι πράγματι προσβάσιμα σε όσους τα χρειάζονται εφόσον απαιτείται, π.χ. σε κρίσιμες καταστάσεις. Οι έλεγχοι πρόσβασης πρέπει να τηρούνται για το σύνολο της ροής δεδομένων κατά την επεξεργασία.

56. Το άρθρο 25 παράγραφος 2 αναφέρει επιπλέον ότι τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων. Ο υπεύθυνος επεξεργασίας περιορίζει εξ ορισμού την προσβασιμότητα και

πληροφοριών, τη χρήση, την κοινολόγηση με διαβίβαση, τη διάδοση ή κάθε άλλη μορφή διάθεσης, τη συσχέτιση ή τον συνδυασμό, τον περιορισμό, τη διαγραφή ή την καταστροφή.

[18] «Γνωμοδότηση 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης», της ομάδας εργασίας του άρθρου 29. WP 216, 10 Απριλίου 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[19] Βλ. άρθρο 4 παράγραφος 1 του ΓΚΠΔ, αιτιολογική σκέψη 26 του ΓΚΠΔ, «Γνωμοδότηση 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης», της ομάδας εργασίας του άρθρου 29. Βλ. επίσης το υποτμήμα «περιορισμός αποθήκευσης» στο τμήμα 3 του παρόντος εγγράφου, σχετικά με την υποχρέωση του υπεύθυνου επεξεργασίας να διασφαλίζει την αποτελεσματικότητα της ισχύουσας τεχνικής/των ισχυουσών τεχνικών ανωνυμοποίησης.

παρέχει στο υποκείμενο των δεδομένων τη δυνατότητα να παρεμβαίνει πριν δημοσιεύσει ή καταστήσει διαθέσιμα με άλλο τρόπο δεδομένα προσωπικού χαρακτήρα που αφορούν το υποκείμενο των δεδομένων σε αόριστο αριθμό φυσικών προσώπων.

57. Η διάθεση δεδομένων προσωπικού χαρακτήρα σε αόριστο αριθμό προσώπων ενδέχεται να οδηγήσει σε ακόμη περαιτέρω διάδοση των δεδομένων απ' ό,τι προοριζόταν αρχικά. Αυτό έχει ιδιαίτερη σημασία στο πλαίσιο του Διαδικτύου και των μηχανών αναζήτησης. Σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει εξ ορισμού να παρέχουν στα υποκείμενα των δεδομένων τη δυνατότητα να παρεμβαίνουν πριν από τη διάθεση δεδομένων προσωπικού χαρακτήρα στο ανοιχτό Διαδίκτυο. Αυτό είναι ιδιαίτερα σημαντικό όταν πρόκειται για παιδιά και ευάλωτες ομάδες.

58. Αναλόγως των νομικών λόγων της επεξεργασίας, η ευκαιρία παρέμβασης μπορεί να ποικίλλει βάσει του πλαισίου της επεξεργασίας. Για παράδειγμα, μπορεί να ζητείται συγκατάθεση για να καταστούν τα δεδομένα προσωπικού χαρακτήρα δημοσίως προσβάσιμα ή να προβλέπονται ρυθμίσεις απορρήτου ώστε τα υποκείμενα των δεδομένων να μπορούν μόνα τους να ελέγχουν τη δημόσια πρόσβαση.

59. Ακόμα και στην περίπτωση που τα δεδομένα προσωπικού χαρακτήρα δημοσιοποιούνται με την άδεια και την νόηση ενός υποκειμένου δεδομένων, αυτό δεν σημαίνει ότι οποιοσδήποτε υπεύθυνος επεξεργασίας με πρόσβαση στα δεδομένα προσωπικού χαρακτήρα μπορεί ελεύθερα να τα επεξεργαστεί ο ίδιος, για τους δικούς του σκοπούς – η εν λόγω επεξεργασία θα πρέπει να διαθέτει τη δική της νομική βάση.[20]

3 ΕΦΑΡΜΟΓΗ ΑΡΧΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΤΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΗΔΗ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ ΚΑΙ ΕΞ ΟΡΙΣΜΟΥ

60. Σε όλα τα στάδια σχεδιασμού των δραστηριοτήτων επεξεργασίας, συμπεριλαμβανομένων των προμηθειών, των διαγωνισμών, της εξωτερικής ανάθεσης, της ανάπτυξης, της υποστήριξης, της συντήρησης, των δοκιμών, της αποθήκευσης, της διαγραφής, κ.λπ., ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει υπόψη του και να εξετάζει τα διάφορα στοιχεία της ΠΔΣΕΟ, τα οποία επεξηγούνται με παραδείγματα στο παρόν κεφάλαιο στο πλαίσιο της εφαρμογής των αρχών.[21] [22] [23]

61. Οι υπεύθυνοι επεξεργασίας οφείλουν να εφαρμόζουν τις αρχές ώστε να επιτυγχάνεται η ΠΔΣΕΟ. Στις εν λόγω αρχές περιλαμβάνονται: η διαφάνεια, η νομιμότητα, η αντικειμενικότητα, ο περιορισμός του σκοπού, η ελαχιστοποίηση των δεδομένων, η ακρίβεια, ο περιορισμός της περιόδου αποθήκευσης, η ακεραιότητα, η εμπιστευτικότητα και η λογοδοσία. Οι εν λόγω αρχές περιγράφονται στο άρθρο 5 και στην αιτιολογική σκέψη 39 του ΓΚΠΔ. Για την πλήρη κατανόηση του

[20] Βλ. υπόθεση Satakunnan Markkinapörssi Oy και Satamedia Oy κατά Φινλανδίας αριθ. 931/13

[21] Περισσότερα παραδείγματα παρέχονται από την Υπηρεσία προστασίας δεδομένων της Νορβηγίας. «Ανάπτυξη λογισμικού στο πλαίσιο της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού.» 28 Νοεμβρίου 2017 www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

τρόπου εφαρμογής της ΠΔΣΕΟ, υπογραμμίζεται η σημασία της κατανόησης του νοήματος κάθε μίας από τις αρχές.

62. Κατά την παρουσίαση των παραδειγμάτων όσον αφορά το πώς μπορεί να καταστεί λειτουργική η ΠΔΣΕΟ, καταρτίστηκαν κατάλογοι **βασικών στοιχείων ΠΔΣΕΟ** για κάθε μία από τις αρχές. Τα παραδείγματα, αν και υπογραμμίζουν την εκάστοτε συγκεκριμένη αρχή προστασίας δεδομένων, ενδέχεται να αλληλοεπικαλύπτονται και με άλλες στενά συνδεόμενες αρχές. Το ΕΣΠΔ υπογραμμίζει ότι τα βασικά στοιχεία και παραδείγματα που παρουσιάζονται στη συνέχεια δεν είναι ούτε εξαντλητικά ούτε δεσμευτικά και πρέπει να εκλαμβάνονται ως καθοδηγητικά στοιχεία για κάθε μία από τις αρχές. Οι υπεύθυνοι επεξεργασίας οφείλουν να αξιολογούν τον τρόπο με τον οποίο μπορούν να εγγυώνται τη συμμόρφωση προς τις αρχές στο πλαίσιο της εκάστοτε πράξης επεξεργασίας.

63. Ενώ η παρούσα ενότητα επικεντρώνεται στην εφαρμογή των αρχών, ο υπεύθυνος επεξεργασίας θα πρέπει επίσης να εφαρμόζει *κατάλληλους* και *αποτελεσματικούς* τρόπους για την προστασία των υποκειμένων των δεδομένων, καθώς και σύμφωνα με το κεφάλαιο III του ΓΚΠΔ, στις περιπτώσεις όπου αυτό δεν προβλέπεται από τις ίδιες τις αρχές.

64. Η αρχή της λογοδοσίας έχει γενική εφαρμογή: απαιτεί από τον υπεύθυνο επεξεργασίας να είναι υπεύθυνος για την επιλογή των αναγκαίων τεχνικών και οργανωτικών μέτρων.

3.1 Διαφάνεια[24]

65. Ο υπεύθυνος επεξεργασίας πρέπει να είναι εξαρχής σαφής και ξεκάθαρος με το υποκείμενο των δεδομένων όσον αφορά τον τρόπο συλλογής, χρήσης και ανταλλαγής των δεδομένων προσωπικού χαρακτήρα. Η διαφάνεια αφορά την παροχή δυνατότητας στα υποκείμενα των δεδομένων να κατανοούν και, εφόσον κρίνεται αναγκαίο, να κάνουν χρήση των δικαιωμάτων τους σύμφωνα με τα άρθρα 15 έως 22. Η εν λόγω αρχή περιλαμβάνεται στα άρθρα 12, 13, 14 και 34. Τα μέτρα και οι εγγυήσεις που έχουν θεσπιστεί για την ενίσχυση της αρχής της διαφάνειας θα πρέπει επίσης να συνοδεύουν την εφαρμογή αυτών των άρθρων.

66. Τα βασικά στοιχεία εξ ορισμού και ήδη από τον σχεδιασμό για την αρχή της διαφάνειας μπορούν να περιλαμβάνουν:

- Σαφήνεια – Οι πληροφορίες πρέπει να διατυπώνονται σε σαφή και απλή γλώσσα, και να είναι συνοπτικές και κατανοητές.
- Σημασιολογία – Η σημασία της επικοινωνίας πρέπει να είναι σαφής για το εκάστοτε κοινό.
- Προσβασιμότητα – Το υποκείμενο των δεδομένων πρέπει να έχει εύκολη πρόσβαση στις πληροφορίες.
- Συνάφεια – Οι πληροφορίες πρέπει να παρέχονται τη σωστή στιγμή και με την κατάλληλη μορφή.
- Σχετικότητα – Οι πληροφορίες πρέπει να είναι σχετικές και να αφορούν το εκάστοτε υποκείμενο των δεδομένων.

[24] Ανάλυση του τρόπου κατανόησης της έννοιας της διαφάνειας περιλαμβάνεται στις «Κατευθυντήριες γραμμές για τη διαφάνεια σύμφωνα με τον κανονισμό 2016/679» της ομάδας εργασίας του άρθρου 29. WP 260, αναθ.01, 11 Απριλίου 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 - οι οποίες εγκρίθηκαν από το ΕΣΠΔ

- Καθολικός σχεδιασμός – Οι πληροφορίες πρέπει να είναι προσβάσιμες σε όλα τα υποκείμενα των δεδομένων, μεταξύ άλλων με τη χρήση μηχανικά αναγνώσιμων γλωσσών για τη διευκόλυνση και την αυτοματοποίηση της αναγνωσιμότητας και της σαφήνειας.
- Κατανοητές – Τα υποκείμενα των δεδομένων πρέπει να αντιλαμβάνονται πλήρως τι μπορούν να αναμένουν όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων, ιδίως όταν πρόκειται για παιδιά ή άλλες ευάλωτες ομάδες.
- Πολλαπλοί δίαυλοι πληροφόρησης – Οι πληροφορίες πρέπει να παρέχονται μέσω διαφορετικών διαύλων και μέσων, και όχι μόνο μέσω κειμένου, ώστε να αυξάνεται η πιθανότητα οι πληροφορίες να καταλήξουν στο υποκείμενο των δεδομένων.
- Πολυεπίπεδες – Οι πληροφορίες πρέπει να είναι πολυεπίπεδες, με τρόπο ώστε να αντιμετωπίζεται η ένταση μεταξύ πληρότητας και κατανόησης, λαμβάνοντας παράλληλα υπόψη τις εύλογες προσδοκίες των υποκειμένων των δεδομένων.

Παράδειγμα[25]

Ένας υπεύθυνος επεξεργασίας σχεδιάζει μια πολιτική απορρήτου στον διαδικτυακό του τόπο προκειμένου να συμμορφωθεί προς τις απαιτήσεις διαφάνειας. Η πολιτική απορρήτου δεν πρέπει να περιέχει μακροσκελές σώμα πληροφοριών το οποίο να είναι δύσκολο για το μέσο υποκείμενο δεδομένων να το διατρέξει και να το κατανοήσει. Πρέπει να είναι γραμμένο με σαφή και σύντομη διατύπωση και να διευκολύνει τον χρήστη του διαδικτυακού τόπου στο να κατανοεί τον τρόπο με τον οποίο τα προσωπικά του δεδομένα υποβάλλονται σε επεξεργασία. Ο υπεύθυνος επεξεργασίας παρέχει επομένως πληροφορίες με πολυεπίπεδο τρόπο, όπου επισημαίνονται τα πιο σημαντικά σημεία. Λεπτομερέστερες πληροφορίες καθίστανται εύκολα διαθέσιμες. Παρέχονται αναπτυσσόμενα μενού και σύνδεσμοι για την περαιτέρω εξήγηση των διαφόρων στοιχείων και εννοιών της πολιτικής. Ο υπεύθυνος επεξεργασίας βεβαιώνεται επίσης ότι οι πληροφορίες παρέχονται μέσω πολλαπλών διαύλων, παρέχοντας βίντεο κλιπ για να εξηγήσει τα πιο σημαντικά σημεία των γραπτών πληροφοριών. Η συνέργεια μεταξύ των διαφόρων σελίδων είναι ζωτικής σημασίας ώστε να διασφαλίζεται ότι η πολυεπίπεδη προσέγγιση δεν συντελεί στη σύγχυση αλλά τη μειώνει.

Η πρόσβαση των υποκειμένων των δεδομένων στην πολιτική απορρήτου δεν πρέπει να είναι δύσκολη. Η πολιτική απορρήτου καθίσταται έτσι διαθέσιμη και ορατή σε όλες τις εσωτερικές ιστοσελίδες του εκάστοτε διαδικτυακού τόπου, ώστε το υποκείμενο των δεδομένων να απέχει μόλις ένα κλικ από την πρόσβαση στις πληροφορίες. Οι πληροφορίες που παρέχονται σχεδιάζονται επίσης σύμφωνα με τις βέλτιστες πρακτικές και πρότυπα καθολικού σχεδιασμού προκειμένου να έχουν όλοι πρόσβαση σε αυτές.

Επιπλέον, οι απαραίτητες πληροφορίες πρέπει πάντα να παρέχονται στο σωστό πλαίσιο, την κατάλληλη στιγμή. Καθώς ο υπεύθυνος επεξεργασίας διενεργεί πολλές πράξεις επεξεργασίας χρησιμοποιώντας τα δεδομένα που συλλέγονται από τον διαδικτυακό τόπο, μια γενική πολιτική απορρήτου που αφορά μόνο τον διαδικτυακό τόπο δεν επαρκεί προκειμένου ο υπεύθυνος επεξεργασίας να πληροί τις απαιτήσεις διαφάνειας. Ο υπεύθυνος επεξεργασίας σχεδιάζει επομένως μια ροή πληροφοριών, θέτοντας στη διάθεση του υποκειμένου των δεδομένων σχετικές πληροφορίες εντός των κατάλληλων πλαισίων χρησιμοποιώντας για παράδειγμα αποσπάσματα πληροφοριών ή αναδυόμενα παράθυρα. Για παράδειγμα, όταν ζητείται από το υποκείμενο των δεδομένων να καταχωρίσει δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων για τον τρόπο επεξεργασίας των δεδομένων

[25] Η γαλλική αρχή προστασίας δεδομένων έχει δημοσιεύσει διάφορα παραδείγματα που καταδεικνύουν τις βέλτιστες πρακτικές ενημέρωσης των χρηστών και άλλες αρχές διαφάνειας: https://design.cnil.fr/en/

προσωπικού χαρακτήρα και τους λόγους για τους οποίους τα δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα για την επεξεργασία.

3.2 Νομιμότητα

67. Ο υπεύθυνος επεξεργασίας πρέπει να προσδιορίζει μια έγκυρη νομική βάση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Τα μέτρα και οι εγγυήσεις πρέπει να υποστηρίζουν την απαίτηση της εξασφάλισης ότι ο συνολικός κύκλος ζωής της επεξεργασίας συνάδει με τους σχετικούς νομικούς λόγους της επεξεργασίας.

68. Τα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού όσον αφορά τη νομιμότητα μπορούν να περιλαμβάνουν τα ακόλουθα:
    - Συνάφεια – Κατά την επεξεργασία πρέπει να εφαρμόζεται η σωστή νομική βάση.
    - Διαφοροποίηση[26] – Η νομική βάση που χρησιμοποιείται για κάθε δραστηριότητα επεξεργασίας πρέπει να διαφοροποιείται.
    - Καθορισμένος σκοπός - Η κατάλληλη νομική βάση πρέπει να συνδέεται σαφώς με τον ειδικό σκοπό της επεξεργασίας.[27]
    - Αναγκαιότητα – Για να είναι νόμιμος ο σκοπός, η επεξεργασία πρέπει να είναι αναγκαία και άνευ όρων.
    - Αυτονομία – Το υποκείμενο των δεδομένων πρέπει να διαθέτει τον υψηλότερο δυνατό βαθμό αυτονομίας όσον αφορά τον έλεγχο των δεδομένων προσωπικού χαρακτήρα εντός του πλαισίου της νομικής βάσης.
    - Εξασφάλιση συγκατάθεσης – Η συγκατάθεση πρέπει να παρέχεται ελεύθερα, να είναι συγκεκριμένη, εν επιγνώσει και σαφής.[28] Ιδιαίτερη προσοχή πρέπει να δίδεται σε ό,τι αφορά την ικανότητα των παιδιών και των νεαρών ατόμων να παρέχουν εν επιγνώσει συναίνεση.
    - Ανάκληση της συγκατάθεσης – Στις περιπτώσεις όπου η συγκατάθεση είναι η νομική βάση, η επεξεργασία πρέπει να διευκολύνει την ανάκληση της συγκατάθεσης. Η ανάκληση θα πρέπει να είναι όσο εύκολη είναι η συναίνεση. Σε διαφορετική περίπτωση, ο μηχανισμός συγκατάθεσης του υπεύθυνου επεξεργασίας δεν συμμορφώνεται προς τον ΓΚΠΔ.[29]
    - Εξισορρόπηση συμφερόντων – Στις περιπτώσεις όπου τα έννομα συμφέροντα είναι η νομική βάση, ο υπεύθυνος επεξεργασίας οφείλει να προβαίνει σε μια σταθμισμένη εξισορρόπηση των συμφερόντων, λαμβάνοντας ιδίως υπόψη την ανισορροπία ισχύος, ειδικά όταν πρόκειται για παιδιά ηλικίας κάτω των 18 ετών και άλλες ευάλωτες ομάδες. Υπάρχουν μέτρα και εγγυήσεις που μετριάζουν τον αρνητικό αντίκτυπο για τα υποκείμενα των δεδομένων.
    - Προκαθορισμός – Η νομική βάση πρέπει να έχει καθοριστεί πριν από τη διενέργεια της επεξεργασίας.

[26] ΕΣΠΔ. «Κατευθυντήριες γραμμές 2/2019 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ στο πλαίσιο της παροχής επιγραμμικών υπηρεσιών σε υποκείμενα δεδομένων». Έκδοση 2.0, 8 Οκτωβρίου 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[27] Βλ. ενότητα σχετικά με τον περιορισμό του σκοπού κατωτέρω.

[28] Βλ. κατευθυντήριες γραμμές 05/2020 σχετικά με τη συναίνεση δυνάμει του κανονισμού 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Βλ. κατευθυντήριες γραμμές 05/2020 σχετικά με τη συναίνεση δυνάμει του κανονισμού 2016/679, σ. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

- Παύση – Εάν η νομική βάση παύει να ισχύει, η επεξεργασία παύει αναλόγως.
- Προσαρμογή – Σε περίπτωση έγκυρης αλλαγής της νομικής βάσης για την επεξεργασία, η επεξεργασία πρέπει να προσαρμοστεί σύμφωνα με τη νέα νομική βάση.[30]
- Κατανομή ευθυνών – Όταν προβλέπεται κοινή ευθύνη επεξεργασίας, τα μέρη οφείλουν να κατανέμουν με σαφή και διαφανή τρόπο τις αντίστοιχες αρμοδιότητές τους έναντι του υποκειμένου των δεδομένων και να σχεδιάζουν τα μέτρα της επεξεργασίας σύμφωνα με αυτήν την κατανομή.

Παράδειγμα

Μια τράπεζα προτίθεται να παράσχει μια υπηρεσία για τη βελτίωση της αποτελεσματικότητας κατά τη διαχείριση αιτήσεων χορήγησης δανείων. Το σκεπτικό για τη δημιουργία της υπηρεσίας είναι ότι η τράπεζα, ζητώντας την άδεια του πελάτη, μπορεί να ανακτήσει στοιχεία σχετικά με τον πελάτη απευθείας από τις δημόσιες φορολογικές αρχές. Το παρόν παράδειγμα δεν εξετάζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα από άλλες πηγές.

Η απόκτηση δεδομένων προσωπικού χαρακτήρα σχετικά με την οικονομική κατάσταση του υποκειμένου των δεδομένων είναι απαραίτητη για την εκτέλεση ενεργειών κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη δανειακής σύμβασης[31] Ωστόσο, η συγκέντρωση δεδομένων προσωπικού χαρακτήρα προερχόμενων απευθείας από τη φορολογική διοίκηση δεν θεωρείται απαραίτητη, διότι ο πελάτης δύναται να συνάψει σύμβαση παρέχοντας ο ίδιος τις πληροφορίες από τη φορολογική διοίκηση. Παρότι η τράπεζα ενδέχεται να έχει έννομο συμφέρον να προμηθευτεί τα προβλεπόμενα έγγραφα απευθείας από τις φορολογικές αρχές, π.χ. για να διασφαλίσει την αποτελεσματικότητα της διεκπεραίωσης του δανείου, η παροχή στις τράπεζες μιας τέτοιας άμεσης πρόσβασης στα δεδομένα προσωπικού χαρακτήρα των αιτούντων ενέχει κινδύνους που σχετίζονται με τη χρήση ή τη δυνητική κατάχρηση των δικαιωμάτων πρόσβασης

Κατά την εφαρμογή της αρχής της νομιμότητας, ο υπεύθυνος επεξεργασίας διαπιστώνει ότι σε αυτό το πλαίσιο δεν μπορεί να χρησιμοποιήσει τη βάση σύμφωνα με την οποία τα δεδομένα είναι «απαραίτητα για τη σύναψη συμβάσεων» για το μέρος της επεξεργασίας που αφορά τη συλλογή δεδομένων προσωπικού χαρακτήρα απευθείας από τις φορολογικές αρχές. Το γεγονός ότι η συγκεκριμένη επεξεργασία ενέχει τον κίνδυνο για το υποκείμενο των δεδομένων να συμμετέχει λιγότερο στην επεξεργασία των δεδομένων του αποτελεί επίσης σημαντικό παράγοντα για την αξιολόγηση της νομιμότητας της ίδιας της επεξεργασίας. Η τράπεζα συμπεραίνει ότι αυτό το μέρος της επεξεργασίας πρέπει να βασίζεται σε κάποια άλλη νομική βάση επεξεργασίας. Στο κράτος μέλος όπου εδρεύει ο υπεύθυνος επεξεργασίας, υπάρχουν εθνικοί νόμοι που επιτρέπουν στην τράπεζα να συλλέγει πληροφορίες απευθείας από τις δημόσιες φορολογικές αρχές, εφόσον το υποκείμενο των δεδομένων έχει συναινέσει προς τούτο εκ των προτέρων.

Ως εκ τούτου, η τράπεζα παρουσιάζει πληροφορίες σχετικά με την επεξεργασία στην ηλεκτρονική πλατφόρμα υποβολής αιτήσεων με τρόπο τέτοιον ώστε να διευκολύνει τα υποκείμενα των δεδομένων να κατανοήσουν ποια επεξεργασία είναι υποχρεωτική και ποια προαιρετική. Οι επιλογές επεξεργασίας, εξ ορισμού, δεν επιτρέπουν την ανάκτηση δεδομένων απευθείας από άλλες πηγές

[30] Εάν η αρχική νομική βάση είναι η συναίνεση, βλ. Κατευθυντήριες γραμμές 05/2020 σχετικά με τη συναίνεση δυνάμει του κανονισμού 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[31] Βλ. άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ.

πλην του ίδιου του υποκειμένου των δεδομένων, και η επιλογή για άμεση ανάκτηση πληροφοριών παρουσιάζεται με τρόπο που δεν εμποδίζει το υποκείμενο των δεδομένων να απέχει. Κάθε συναίνεση που παρέχεται για τη συλλογή δεδομένων απευθείας από άλλους υπεύθυνους επεξεργασίας αποτελεί ένα προσωρινό δικαίωμα πρόσβασης σε ένα συγκεκριμένο σύνολο πληροφοριών.

Κάθε συγκατάθεση υποβάλλεται σε ηλεκτρονική επεξεργασία με τεκμηριωμένο τρόπο, στα δε υποκείμενα των δεδομένων προσφέρεται ένας εύκολος τρόπος να ελέγχουν τις πληροφορίες για τις οποίες έχουν συναινέσει και να ανακαλούν τη συγκατάθεση τους.

Ο υπεύθυνος επεξεργασίας έχει αξιολογήσει τις εν λόγω απαιτήσεις ΠΔΣΕΟ εκ των προτέρων και περιλαμβάνει όλα αυτά τα κριτήρια στις προδιαγραφές απαιτήσεων του διαγωνισμού για την προμήθεια της πλατφόρμας. Ο υπεύθυνος επεξεργασίας γνωρίζει ότι εάν δεν συμπεριλάβει τις απαιτήσεις ΠΔΣΕΟ στον διαγωνισμό, μπορεί να είναι πολύ αργά ή να είναι πολύ δαπανηρή η διαδικασία για την εφαρμογή της προστασίας των δεδομένων στη συνέχεια.

3.3 Αντικειμενικότητα

69. Η αντικειμενικότητα είναι μια θεμελιώδης αρχή σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που είναι αδικαιολόγητα επιζήμιος, εισάγει αθέμιτα διακρίσεις, είναι απρόβλεπτος ή παραπλανητικός για το υποκείμενο των δεδομένων. Τα μέτρα και οι εγγυήσεις για την εφαρμογή της αρχής της αντικειμενικότητας υποστηρίζουν επίσης τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ειδικότερα το δικαίωμα στην ενημέρωση (διαφάνεια), το δικαίωμα παρέμβασης (πρόσβαση, διαγραφή, φορητότητα των δεδομένων, διόρθωση) και το δικαίωμα περιορισμού της επεξεργασίας (το δικαίωμα να μην υπόκειται κάποιος σε αυτοματοποιημένη μεμονωμένη διαδικασία λήψης αποφάσεων και μη εισαγωγής διακρίσεων των υποκειμένων των δεδομένων στις εν λόγω διαδικασίες).

70. Τα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού όσον αφορά την αντικειμενικότητα μπορούν να περιλαμβάνουν τα ακόλουθα:
    - Αυτονομία – Το υποκείμενο των δεδομένων πρέπει να διαθέτει τον υψηλότερο δυνατό βαθμό αυτονομίας προκειμένου να καθορίζει τη χρήση των δεδομένων προσωπικού χαρακτήρα που το αφορούν, καθώς και το πεδίο εφαρμογής και τους όρους της εν λόγω χρήσης ή επεξεργασίας.
    - Αλληλεπίδραση – Τα υποκείμενα των δεδομένων πρέπει να είναι σε θέση να επικοινωνούν και να ασκούν τα δικαιώματά τους σε ό,τι αφορά τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία από τον υπεύθυνο επεξεργασίας.
    - Προσδοκίες – Η επεξεργασία πρέπει να ανταποκρίνεται στις εύλογες προσδοκίες των υποκειμένων των δεδομένων.
    - Μη εισαγωγή διακρίσεων – Ο υπεύθυνος επεξεργασίας δεν πρέπει να εισάγει αθέμιτα διακρίσεις εις βάρος των υποκειμένων των δεδομένων.
    - Μη εκμετάλλευση – Ο υπεύθυνος επεξεργασίας δεν πρέπει να εκμεταλλεύεται τις ανάγκες ή τις αδυναμίες των υποκειμένων των δεδομένων.
    - Επιλογή καταναλωτή – Ο υπεύθυνος επεξεργασίας δεν πρέπει να «δεσμεύει» τους χρήστες του με αθέμιτο τρόπο. Όταν μια υπηρεσία που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα καλύπτεται από δικαιώματα κυριότητας, μπορεί να συνεπάγεται ένα είδος δέσμευσης του χρήστη, το οποίο ενδέχεται να μην είναι θεμιτό, εάν περιορίζει τη

δυνατότητα των υποκειμένων των δεδομένων να ασκούν το δικαίωμά τους στη φορητότητα των δεδομένων σύμφωνα με το άρθρο 20.

- Ισορροπία ισχύος – Η ισορροπία ισχύος πρέπει να αποτελεί βασικό στόχο της σχέσης μεταξύ του υπεύθυνου επεξεργασίας και του υποκειμένου των δεδομένων. Οι ανισορροπίες ισχύος πρέπει να αποφεύγονται. Όταν αυτό δεν είναι εφικτό, πρέπει να αναγνωρίζονται και να συνυπολογίζονται με εφαρμογή των κατάλληλων αντίμετρων.
- Μη μεταβίβαση κινδύνων – Οι υπεύθυνοι επεξεργασίας δεν πρέπει να μεταβιβάζουν τους κινδύνους της επιχείρησης στα υποκείμενα των δεδομένων.
- Μη εξαπάτηση – Οι πληροφορίες και επιλογές σχετικά με την επεξεργασία δεδομένων πρέπει να παρέχονται με αντικειμενικό και ουδέτερο τρόπο, αποφεύγοντας τυχόν λόγο ή σχεδιασμό που υποδηλώνει εξαπάτηση ή χειραγώγηση.
- Σεβασμός των δικαιωμάτων – Ο υπεύθυνος επεξεργασίας οφείλει να σέβεται τα θεμελιώδη δικαιώματα των υποκειμένων των δεδομένων και να εφαρμόζει τα κατάλληλα μέτρα και εγγυήσεις, καθώς και να μη θίγει τα εν λόγω δικαιώματα παρά μόνο εφόσον αυτό δικαιολογείται ρητά από τον νόμο.
- Δεοντολογία – Ο υπεύθυνος επεξεργασίας θα πρέπει να βλέπει τις ευρύτερες επιπτώσεις της επεξεργασίας στα δικαιώματα και στην αξιοπρέπεια των ατόμων.
- Αληθείς πληροφορίες – Ο υπεύθυνος επεξεργασίας οφείλει να παρέχει πληροφορίες σχετικά με τον τρόπο με τον οποίο επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα και πρέπει να ενεργεί με τον τρόπο που δηλώνει και να μην παραπλανά τα υποκείμενα των δεδομένων.
- Ανθρώπινη παρέμβαση – Ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει *εξειδικευμένο* μηχανισμό ανθρώπινης παρέμβασης, ικανό να αποκαλύπτει τις διακρίσεις που ενδέχεται να δημιουργούν τα μηχανήματα σύμφωνα με το δικαίωμα των ατόμων να μην υπόκεινται σε αυτοματοποιημένες ατομικές αποφάσεις, όπως προβλέπεται στο άρθρο 22.[32]
- Σωστοί αλγόριθμοι – Τακτική αξιολόγηση του εάν οι αλγόριθμοι λειτουργούν σύμφωνα με τους επιδιωκόμενους σκοπούς και προσαρμογή των αλγορίθμων ώστε να μετριάζονται οι εντοπιζόμενες διακρίσεις και να εξασφαλίζεται η αντικειμενικότητα της επεξεργασίας. Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται σχετικά με τη λειτουργία της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα βάσει αλγορίθμων που αναλύουν ή κάνουν προβλέψεις που τα αφορούν, όπως οι επιδόσεις στην εργασία, η οικονομική κατάσταση, η υγεία, οι προσωπικές προτιμήσεις, η αξιοπιστία ή η συμπεριφορά, η τοποθεσία ή οι μετακινήσεις.[33]

Παράδειγμα 1

Ένας υπεύθυνος επεξεργασίας χρησιμοποιεί μια μηχανή αναζήτησης που επεξεργάζεται κυρίως προσωπικά δεδομένα που προκύπτουν από τον χρήστη. Ο υπεύθυνος επεξεργασίας επωφελείται από τον μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα και από το γεγονός ότι έχει τη δυνατότητα να χρησιμοποιεί τα εν λόγω δεδομένα προσωπικού χαρακτήρα για στοχοθετημένες διαφημίσεις. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας επιθυμεί να επηρεάσει τα υποκείμενα των δεδομένων ώστε

[32] Βλ Κατευθυντήριες γραμμές σχετικά με την αυτοματοποιημένη ατομική λήψη αποφάσεων και τη δημιουργία προφίλ για τους σκοπούς του κανονισμού 2016/679.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Βλ. αιτιολογική σκέψη 71 του ΓΚΠΔ.

να επιτρέψουν μια πιο εκτεταμένη συλλογή και χρήση των προσωπικών τους δεδομένων. Η συγκατάθεση πρόκειται να λαμβάνεται μέσω της παροχής επιλογών επεξεργασίας στο υποκείμενο των δεδομένων.

Κατά την εφαρμογή της αρχής της αντικειμενικότητας, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τον σκοπό της επεξεργασίας, ο υπεύθυνος επεξεργασίας διαπιστώνει ότι δεν μπορεί να παρουσιάσει τις επιλογές κατά τρόπο που ωθεί το υποκείμενο των δεδομένων προς την κατεύθυνση που επιτρέπει στον υπεύθυνο επεξεργασίας να συλλέξει περισσότερα δεδομένα προσωπικού χαρακτήρα σε σχέση με αυτά που θα είχε συλλέξει εάν οι επιλογές είχαν παρουσιαστεί με ισότιμο και ουδέτερο τρόπο. Αυτό σημαίνει ότι οι επιλογές επεξεργασίας δεν μπορούν να παρουσιαστούν κατά τρόπο που καθιστά δύσκολο για τα υποκείμενα των δεδομένων να μην υποβάλουν τα προσωπικά τους δεδομένα ή να μην προσαρμόσουν τις ρυθμίσεις απορρήτου τους και να περιορίσουν την επεξεργασία. Αυτά συνιστούν παραδείγματα σκοτεινών πρακτικών, οι οποίες αντιβαίνουν στο πνεύμα του άρθρου 25. Οι προεπιλεγμένες επιλογές επεξεργασίας δεν πρέπει να είναι επεμβατικές και η επιλογή για περαιτέρω επεξεργασία πρέπει να παρουσιάζεται κατά τρόπο που να μην ασκεί πίεση στο υποκείμενο των δεδομένων προκειμένου να δώσει τη συναίνεσή του. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας παρουσιάζει τις επιλογές συναίνεσης και απόρριψης ως δύο εξίσου ορατές επιλογές, υποδεικνύοντας επακριβώς τις συνέπειες κάθε επιλογής στο υποκείμενο των δεδομένων.

Παράδειγμα 2

Ένας άλλος υπεύθυνος επεξεργασίας, επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για μια υπηρεσία μετάδοσης (streaming) όπου οι χρήστες μπορούν να επιλέξουν μεταξύ μιας κανονικής συνδρομής τυπικής ποιότητας και μιας premium συνδρομής υψηλής ποιότητας. Στο πλαίσιο της premium συνδρομής, οι συνδρομητές λαμβάνουν μια κατά προτεραιότητα εξυπηρέτηση πελατών.

Όσον αφορά την αρχή της αντικειμενικότητας, η κατά προτεραιότητα υπηρεσία εξυπηρέτησης πελατών η οποία παρέχεται στους premium συνδρομητές δεν μπορεί να εισάγει διακρίσεις σε σχέση με τα δικαιώματα των κανονικών συνδρομητών σύμφωνα με το άρθρο 12 του ΓΚΠΔ. Αυτό σημαίνει ότι παρόλο που οι premium συνδρομητές λαμβάνουν υπηρεσίες κατά προτεραιότητα, αυτή η προτεραιότητα δεν μπορεί να οδηγήσει στη μη λήψη των κατάλληλων μέτρων για την ανταπόκριση σε αιτήματα κανονικών συνδρομητών χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός ενός μήνα από τη λήψη των αιτήσεων.

Οι κατά προτεραιότητα πελάτες μπορούν να πληρώνουν για να λαμβάνουν καλύτερες υπηρεσίες, αλλά όλα τα υποκείμενα των δεδομένων πρέπει να έχουν ισότιμη πρόσβαση, χωρίς διακρίσεις ώστε να εφαρμόζονται τα δικαιώματα και οι ελευθερίες τους, όπως προβλέπεται από το άρθρο 12.

3.4 Περιορισμός του σκοπού[34]

[34] Η ομάδα εργασίας του άρθρου 29 παρείχε καθοδήγηση για την κατανόηση της αρχής του περιορισμού του σκοπού βάσει της οδηγίας 95/46/ΕΚ. Παρά το γεγονός ότι η γνωμοδότηση δεν εγκρίνεται από το ΕΣΠΔ, εξακολουθεί να είναι σημαντική, καθώς η διατύπωση της αρχής είναι η ίδια στο πλαίσιο του ΓΚΠΔ. «Γνωμοδότηση 03/2013 σχετικά με τον περιορισμό του σκοπού», της ομάδας εργασίας του άρθρου 29. WP 203, 2 Απριλίου 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

71. Ο υπεύθυνος επεξεργασίας πρέπει να συλλέγει δεδομένα για καθορισμένους, σαφείς και νόμιμους σκοπούς και να μην επεξεργάζεται περαιτέρω τα δεδομένα κατά τρόπο που δεν είναι συμβατός με τους σκοπούς για τους οποίους συλλέχθηκαν.[35] Ο σχεδιασμός της επεξεργασίας θα πρέπει επομένως να διαμορφώνεται σύμφωνα με αυτό που είναι απαραίτητο για την επίτευξη των σκοπών. Εάν πρόκειται να πραγματοποιηθεί περαιτέρω επεξεργασία, ο υπεύθυνος επεξεργασίας πρέπει πρώτα να βεβαιωθεί ότι οι σκοποί της εν λόγω επεξεργασίας είναι συμβατοί με τους αρχικούς και να τη σχεδιάσει αναλόγως. Κατά πόσον ένας σκοπός είναι συμβατός ή όχι αξιολογείται σύμφωνα με τα κριτήρια του άρθρου 6 παράγραφος 4,

72. Τα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού όσον αφορά τον περιορισμό του σκοπού μπορούν να περιλαμβάνουν τα ακόλουθα:
    - Προκαθορισμός – Οι νόμιμοι σκοποί πρέπει να καθορίζονται πριν από τον σχεδιασμό της επεξεργασίας.
    - Ρητός χαρακτήρας – Οι σκοποί πρέπει να είναι συγκεκριμένοι και να προσδιορίζουν ρητά τους λόγους για τους οποίους δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία.
    - Προσανατολισμός σκοπού – Ο σκοπός της επεξεργασίας θα πρέπει να καθοδηγεί τον σχεδιασμό της επεξεργασίας και να θέτει όρια επεξεργασίας.
    - Αναγκαιότητα – Ο σκοπός καθορίζει ποια προσωπικά δεδομένα είναι απαραίτητα για την επεξεργασία.
    - Συμβατότητα – Κάθε νέος σκοπός πρέπει να είναι συμβατός με τον αρχικό σκοπό για τον οποίο συλλέχθηκαν τα δεδομένα και να διέπει τις σχετικές αλλαγές κατά τον σχεδιασμό.
    - Περιορισμός περαιτέρω επεξεργασίας - Ο υπεύθυνος επεξεργασίας δεν θα πρέπει να συνδέει σύνολα δεδομένων ή να πραγματοποιεί περαιτέρω επεξεργασία για νέους μη συμβατούς σκοπούς.
    - Περιορισμοί επαναχρησιμοποίησης - Ο υπεύθυνος επεξεργασίας πρέπει να χρησιμοποιεί τεχνικά μέτρα, συμπεριλαμβανομένου του κατακερματισμού και της κρυπτογράφησης, για τον περιορισμό της πιθανότητας επαναχρησιμοποίησης των δεδομένων προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας πρέπει επίσης να προβλέπει οργανωτικά μέτρα, όπως πολιτικές και συμβατικές υποχρεώσεις, τα οποία περιορίζουν την επαναχρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα.
    - Επανεξέταση – Ο υπεύθυνος επεξεργασίας πρέπει να επανεξετάζει τακτικά εάν η επεξεργασία είναι απαραίτητη για τους σκοπούς για τους οποίους συλλέχθηκαν τα δεδομένα και να δοκιμάζει τον σχεδιασμό σε σχέση με τον περιορισμό του σκοπού.

Παράδειγμα

Ο υπεύθυνος επεξεργασίας επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για τους πελάτες του. Ο σκοπός της επεξεργασίας είναι η εκτέλεση μιας σύμβασης, δηλαδή η παράδοση των προϊόντων στη σωστή διεύθυνση και η λήψη πληρωμής. Τα αποθηκευμένα δεδομένα προσωπικού χαρακτήρα είναι το ιστορικό αγορών, το όνομα, η διεύθυνση, η ηλεκτρονική διεύθυνση και ο αριθμός τηλεφώνου.

Ο υπεύθυνος επεξεργασίας σκέφτεται να αγοράσει ένα προϊόν διαχείρισης των σχέσεων με τους πελάτες (ΔΣΠ) το οποίο συγκεντρώνει όλα τα δεδομένα των πελατών σχετικά με πωλήσεις, μάρκετινγκ και εξυπηρέτηση πελατών σε ένα μέρος. Το προϊόν δίνει τη δυνατότητα αποθήκευσης όλων των τηλεφωνικών κλήσεων, των δραστηριοτήτων, των εγγράφων, των μηνυμάτων

[35] Άρθρο 5 παράγραφος 1 στοιχείο β) του ΓΚΠΔ.

ηλεκτρονικού ταχυδρομείου και των εκστρατειών εμπορίας (μάρκετινγκ) για να αποκτηθεί σφαιρική εικόνα του πελάτη. Επιπλέον, το προϊόν ΔΣΠ μπορεί να αναλύει αυτόματα την αγοραστική δύναμη των πελατών χρησιμοποιώντας δημόσιες πληροφορίες. Ο σκοπός της ανάλυσης είναι η καλύτερη στόχευση των διαφημιστικών δραστηριοτήτων. Οι εν λόγω δραστηριότητες δεν αποτελούν μέρος του αρχικού νόμιμου σκοπού της επεξεργασίας.

Για τη συμμόρφωση προς την αρχή του περιορισμού του σκοπού, ο υπεύθυνος επεξεργασίας απαιτεί από τον πάροχο του προϊόντος να καταγράφει τις διάφορες δραστηριότητες επεξεργασίας που χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα για τους σκοπούς που αφορούν τον υπεύθυνο επεξεργασίας.

Αφότου λάβει τα αποτελέσματα της καταγραφής, ο υπεύθυνος επεξεργασίας αξιολογεί το εάν ο νέος σκοπός εμπορικής προώθησης και ο σκοπός της στοχοθετημένης διαφήμισης είναι συμβατοί με τους αρχικούς σκοπούς που ορίστηκαν κατά τη συλλογή των δεδομένων, καθώς και το εάν υφίσταται επαρκής νομική βάση για την αντίστοιχη επεξεργασία. Εάν η αξιολόγηση δεν δώσει θετική απάντηση, ο υπεύθυνος επεξεργασίας δεν χρησιμοποιεί τις αντίστοιχες λειτουργίες. Εναλλακτικά, ο υπεύθυνος επεξεργασίας μπορεί να επιλέξει να αποφύγει την αξιολόγηση και να μη χρησιμοποιήσει απλώς τις περιγραφόμενες λειτουργίες του προϊόντος.

3.5 Ελαχιστοποίηση των δεδομένων

73. Μόνο δεδομένα προσωπικού χαρακτήρα που είναι επαρκή, συναφή και περιορίζονται στο **αναγκαίο** για τον επιδιωκόμενο σκοπό υποβάλλονται σε επεξεργασία.[36] Επομένως, ο υπεύθυνος επεξεργασίας πρέπει να προκαθορίζει ποια χαρακτηριστικά και παράμετροι των συστημάτων επεξεργασίας και των υποστηρικτικών λειτουργιών τους επιτρέπονται. Η ελαχιστοποίηση των δεδομένων τεκμηριώνει και εφαρμόζει την αρχή της αναγκαιότητας. Κατά την περαιτέρω επεξεργασία, ο υπεύθυνος επεξεργασίας θα πρέπει να ελέγχει τακτικά εάν τα επεξεργασμένα δεδομένα προσωπικού χαρακτήρα εξακολουθούν να είναι επαρκή, συναφή και αναγκαία ή εάν τα δεδομένα πρέπει να διαγραφούν ή να ανωνυμοποιηθούν.

74. Οι υπεύθυνοι επεξεργασίας πρέπει καταρχάς να προσδιορίζουν εάν πρέπει να επεξεργαστούν τα δεδομένα προσωπικού χαρακτήρα για τους συναφείς σκοπούς επεξεργασίας. Ο υπεύθυνος επεξεργασίας πρέπει να ελέγχει εάν οι συναφείς σκοποί μπορούν να επιτυγχάνονται μέσω της επεξεργασίας λιγότερων δεδομένων προσωπικού χαρακτήρα ή με τη λήψη λιγότερο λεπτομερών και συγκεντρωμένων δεδομένων προσωπικού χαρακτήρα ή χωρίς καθόλου επεξεργασία δεδομένων προσωπικού χαρακτήρα[37]. Ένας τέτοιος έλεγχος πρέπει να γίνεται πριν από τη διενέργεια οποιασδήποτε επεξεργασίας, αλλά μπορεί επίσης να διενεργείται ανά πάσα στιγμή κατά τη διάρκεια του κύκλου ζωής της επεξεργασίας. Αυτό συνάδει επίσης με το άρθρο 11.

75. Η ελαχιστοποίηση μπορεί επίσης να αναφέρεται στον βαθμό ταυτοποίησης. Εάν ο σκοπός της επεξεργασίας δεν απαιτεί το τελικό σύνολο δεδομένων να αναφέρεται σε ένα ταυτοποιούμενο ή ταυτοποιήσιμο φυσικό πρόσωπο (όπως στα στατιστικά στοιχεία), αλλά η αρχική επεξεργασία το απαιτεί (για παράδειγμα πριν από τη συγκέντρωση των δεδομένων), τότε ο υπεύθυνος επεξεργασίας διαγράφει ή ανωνυμοποιεί τα δεδομένα προσωπικού χαρακτήρα τη στιγμή που δεν θα είναι πλέον απαραίτητη η ταυτοποίηση. Ή, εάν απαιτείται συνεχής ταυτοποίηση για άλλες

[36] Άρθρο 5 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ.

[37] Η αιτιολογική σκέψη 39 του ΓΚΠΔ αναφέρει: «...Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία μόνο εάν ο σκοπός της επεξεργασίας δεν μπορεί να επιτευχθεί με άλλα μέσα.»

δραστηριότητες επεξεργασίας, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να ψευδωνυμοποιούνται για τον μετριασμό των κινδύνων για τα δικαιώματα των υποκειμένων των δεδομένων.

76. Τα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού όσον αφορά την ελαχιστοποίηση των δεδομένων μπορούν να περιλαμβάνουν τα ακόλουθα:
    - Κατάργηση δεδομένων – Η μη επεξεργασία δεδομένων προσωπικού χαρακτήρα συνολικά όταν αυτό είναι δυνατό για τον σχετικό σκοπό.
    - Περιορισμός – Περιορισμός του όγκου των δεδομένων προσωπικού χαρακτήρα που συλλέγονται σε ό, τι είναι αναγκαίο για τον σκοπό της επεξεργασίας
    - Περιορισμός της πρόσβασης – Διαμόρφωση της επεξεργασίας των δεδομένων έτσι ώστε να απαιτείται η πρόσβαση του ελάχιστου δυνατού αριθμού ατόμων σε δεδομένα προσωπικού χαρακτήρα προκειμένου να εκτελέσουν τα καθήκοντά τους, και ανάλογος περιορισμός της πρόσβασης.
    - Συνάφεια – Τα δεδομένα προσωπικού χαρακτήρα πρέπει να αφορούν την εκάστοτε επεξεργασία και ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδεικνύει αυτή τη συνάφεια.
    - Αναγκαιότητα – Κάθε κατηγορία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι αναγκαία για τους καθορισμένους σκοπούς και θα πρέπει να υποβάλλεται σε επεξεργασία μόνο εάν δεν είναι δυνατή η επίτευξη του σκοπού με άλλα μέσα.
    - Συγκέντρωση δεδομένων – Χρήση συγκεντρωτικών δεδομένων στο μέτρο του δυνατού.
    - Ψευδωνυμοποίηση – Ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα τη στιγμή που δεν θα είναι πλέον απαραίτητη η ύπαρξη άμεσα ταυτοποιήσιμων δεδομένων προσωπικού χαρακτήρα και ξεχωριστή αποθήκευση αναγνωριστικών κλειδιών.
    - Ανωνυμοποίηση και διαγραφή – Όταν τα δεδομένα προσωπικού χαρακτήρα δεν είναι ή δεν είναι πλέον απαραίτητα για τον επιδιωκόμενο σκοπό, τα δεδομένα προσωπικού χαρακτήρα ανωνυμοποιούνται ή διαγράφονται.
    - Ροή δεδομένων – Η ροή δεδομένων πρέπει να είναι αρκετά αποτελεσματική ώστε να μην δημιουργεί περισσότερα αντίγραφα από ό, τι είναι απαραίτητο.
    - «Τελευταίες εξελίξεις» – Ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει διαθέσιμες και κατάλληλες τεχνολογίες για την κατάργηση και την ελαχιστοποίηση των δεδομένων.

Παράδειγμα 1

Ένα βιβλιοπωλείο θέλει να αυξήσει τα έσοδά του, πουλώντας τα βιβλία του ηλεκτρονικά. Ο ιδιοκτήτης του βιβλιοπωλείου θέλει να δημιουργήσει ένα τυποποιημένο έντυπο για τη διαδικασία της παραγγελίας. Για να διασφαλίζεται η συμπλήρωση όλων των ζητούμενων πληροφοριών από τους πελάτες, ο ιδιοκτήτης του βιβλιοπωλείου καθιστά όλα τα πεδία του εντύπου υποχρεωτικά (εάν ο πελάτης δεν συμπληρώσει όλα τα πεδία, δεν μπορεί να προβεί στην παραγγελία). Ο ιδιοκτήτης του ηλεκτρονικού καταστήματος χρησιμοποιεί αρχικά ένα τυποποιημένο έντυπο επικοινωνίας, το οποίο ζητά πληροφορίες που περιλαμβάνουν την ημερομηνία γέννησης, τον αριθμό τηλεφώνου και τη διεύθυνση κατοικίας του πελάτη. Ωστόσο, δεν είναι όλα τα πεδία του εντύπου απαραίτητα για την αγορά και την παράδοση των βιβλίων. Σε μια τέτοια περίπτωση, εάν το υποκείμενο των δεδομένων πληρώνει για το προϊόν προκαταβολικά, τότε η ημερομηνία γέννησης και ο αριθμός τηλεφώνου του δεν είναι απαραίτητα για την αγορά του προϊόντος. Αυτό σημαίνει ότι τα εν λόγω στοιχεία δεν μπορούν αντιστοιχούν σε απαιτούμενα πεδία στο ηλεκτρονικό έντυπο για την παραγγελία του προϊόντος, εκτός εάν ο υπεύθυνος επεξεργασίας μπορεί σαφώς να αποδείξει ότι

είναι εν τέλει απαραίτητα και τον λόγο για τον οποίο είναι απαραίτητα. Επιπλέον, υπάρχουν περιπτώσεις όπου η διεύθυνση δεν θα είναι απαραίτητη. Για παράδειγμα, κατά την παραγγελία ενός ηλεκτρονικού βιβλίου ο πελάτης μπορεί να μεταφορτώσει το προϊόν απευθείας στη συσκευή του.

Ο ιδιοκτήτης του ηλεκτρονικού καταστήματος αποφασίζει να δημιουργήσει δύο ηλεκτρονικά έντυπα: ένα για την παραγγελία βιβλίων, με ένα πεδίο για τη συμπλήρωση της διεύθυνσης του πελάτη και ένα για την παραγγελία ηλεκτρονικών βιβλίων χωρίς πεδίο για τη συμπλήρωση της διεύθυνσης του πελάτη.

Παράδειγμα 2

Μια εταιρεία δημόσιων μεταφορών επιθυμεί να συγκεντρώσει στατιστικά στοιχεία με βάση τις διαδρομές των επιβατών. Αυτό είναι χρήσιμο για να γίνονται καλύτερες επιλογές σε περίπτωση αλλαγών στα ωράρια των δημόσιων συγκοινωνιών και για την ομαλή εκτέλεση των δρομολογίων των τρένων. Οι επιβάτες πρέπει να περάσουν το εισιτήριό τους μέσω ενός αναγνώστη κάθε φορά που εισέρχονται ή εξέρχονται από ένα μέσο μεταφοράς. Έχοντας διενεργήσει αξιολόγηση κινδύνου σχετικά με τα δικαιώματα και τις ελευθερίες των επιβατών όσον αφορά τη συλλογή δεδομένων που αφορούν τις ταξιδιωτικές διαδρομές των επιβατών, ο υπεύθυνος επεξεργασίας διαπιστώνει ότι είναι δυνατός ο εντοπισμός των επιβατών σε περιπτώσεις όπου αυτοί ζουν ή εργάζονται σε αραιοκατοικημένες περιοχές, με βάση την αναγνώριση μοναδικής διαδρομής χάρη στο αναγνωριστικό του εισιτηρίου. Επομένως, δεδομένου ότι δεν είναι απαραίτητο για τον σκοπό της βελτιστοποίησης των ωραρίων των δημόσιων συγκοινωνιών και των δρομολογίων των τρένων, ο υπεύθυνος επεξεργασίας δεν αποθηκεύει το αναγνωριστικό του εισιτηρίου. Μετά το τέλος του ταξιδιού, ο υπεύθυνος επεξεργασίας αποθηκεύει μόνο τις μεμονωμένες ταξιδιωτικές διαδρομές ώστε να μην είναι σε θέση να εντοπίσει ταξίδια που συνδέονται με ένα ενιαίο εισιτήριο, αλλά διατηρεί μόνο πληροφορίες για ξεχωριστές ταξιδιωτικές διαδρομές.

Σε περιπτώσεις όπου εξακολουθεί να υπάρχει κίνδυνος να εντοπιστεί ένα άτομο αποκλειστικά από την ταξιδιωτική διαδρομή του με δημόσιο μέσο μεταφοράς, ο υπεύθυνος επεξεργασίας εφαρμόζει στατιστικά μέτρα για τον περιορισμό του κινδύνου, όπως η διαγραφή της έναρξης και του τέλους της διαδρομής.

Παράδειγμα 3

Μια υπηρεσία ταχυμεταφορών επιδιώκει την αξιολόγηση της αποτελεσματικότητας των παραδόσεών της όσον αφορά τους χρόνους παράδοσης, τον προγραμματισμό του φόρτου εργασίας και την κατανάλωση καυσίμου. Για να επιτευχθεί ο στόχος αυτός, η υπηρεσία ταχυμεταφορών πρέπει να επεξεργαστεί ορισμένα δεδομένα προσωπικού χαρακτήρα που αφορούν τόσο τους υπαλλήλους (οδηγούς), όσο και τους καταναλωτές (διευθύνσεις, αντικείμενα που πρέπει να παραδοθούν, κ.λπ.). Αυτή η διαδικασία επεξεργασίας συνεπάγεται τον κίνδυνο ελέγχου των υπαλλήλων, για τον οποίο απαιτούνται ειδικές νομικές εγγυήσεις, καθώς και της παρακολούθησης των συνηθειών των πελατών μέσω των πληροφοριών σχετικά με τα παραδοθέντα αντικείμενα με την πάροδο του χρόνου. Αυτοί οι κίνδυνοι μπορούν να μειωθούν σημαντικά με την κατάλληλη ψευδωνυμοποίηση των υπαλλήλων και των πελατών. Ειδικότερα, εάν οι κλείδες ψευδωνυμοποίησης εναλλάσσονται συχνά και λαμβάνονται υπόψη ευρύτερες περιοχές και όχι λεπτομερείς διευθύνσεις, επιδιώκεται η αποτελεσματική ελαχιστοποίηση των δεδομένων και ο

υπεύθυνος επεξεργασίας μπορεί να επικεντρωθεί αποκλειστικά στη διαδικασία παράδοσης και στον σκοπό της βελτιστοποίησης πόρων, χωρίς να υπερβαίνει το όριο του ελέγχου ατομικών συμπεριφορών (πελατών και υπαλλήλων).

Παράδειγμα 4

Ένα νοσοκομείο συλλέγει δεδομένα σχετικά με τους ασθενείς του μέσω νοσοκομειακού πληροφορικού συστήματος (ηλεκτρονικό μητρώο υγείας). Το προσωπικό του νοσοκομείου χρειάζεται πρόσβαση σε φακέλους ασθενών ώστε να τεκμηριώνει τις αποφάσεις του σχετικά με την περίθαλψη και τη θεραπεία των ασθενών, καθώς και για την τεκμηρίωση όλων των μέτρων διάγνωσης, περίθαλψης και θεραπείας που λαμβάνονται. Εξ ορισμού, η πρόσβαση παρέχεται μόνο σε εκείνα τα μέλη του ιατρικού προσωπικού που αναλαμβάνουν τη θεραπεία του αντίστοιχου ασθενούς στο τμήμα της ειδικότητας όπου αυτός υπάγεται. Η ομάδα ατόμων που έχουν πρόσβαση στον φάκελο ενός ασθενούς διευρύνεται εφόσον στη θεραπεία του συμμετέχουν και άλλα τμήματα ή διαγνωστικές μονάδες. Μετά το εξιτήριο του ασθενούς και την ολοκλήρωση της τιμολόγησης των υπηρεσιών, η πρόσβαση περιορίζεται σε μια μικρή ομάδα εργαζομένων ανά τμήμα ειδικότητας, οι οποίοι απαντούν σε αιτήματα παροχής ιατρικών πληροφοριών ή ιατρικής επίσκεψης που πραγματοποιείται ή ζητείται από άλλους παρόχους ιατρικών υπηρεσιών κατόπιν εξουσιοδότησης από τον αντίστοιχο ασθενή.

3.6 Ακρίβεια

77. Τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και επικαιροποιούνται, και λαμβάνονται όλα τα εύλογα μέτρα που διασφαλίζουν τη χωρίς καθυστέρηση διαγραφή ή διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα, λαμβανομένων υπόψη των σκοπών της επεξεργασίας.[38]

78. Οι απαιτήσεις πρέπει να αξιολογούνται σε σχέση με τους κινδύνους και τις συνέπειες της χρήσης των δεδομένων στην πράξη. Τα ανακριβή δεδομένα προσωπικού χαρακτήρα θα μπορούσαν να θέσουν σε κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, π.χ. όταν οδηγούν σε εσφαλμένη διάγνωση ή λανθασμένη επεξεργασία ενός υγειονομικού πρωτοκόλλου ή η λανθασμένη εικόνα ενός προσώπου μπορεί να οδηγήσει σε λανθασμένες αποφάσεις είτε με μη αυτόματο τρόπο, είτε με τη χρήση αυτοματοποιημένης λήψης αποφάσεων ή μέσω της τεχνητής νοημοσύνης.

79. Τα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού όσον αφορά την ακρίβεια μπορούν να περιλαμβάνουν τα ακόλουθα:
    - Πηγή δεδομένων – Οι πηγές δεδομένων προσωπικού χαρακτήρα πρέπει να είναι αξιόπιστες όσον αφορά την ακρίβεια των δεδομένων.
    - Βαθμός ακρίβειας – Κάθε στοιχείο δεδομένων προσωπικού χαρακτήρα πρέπει να είναι ακριβές στο μέτρο του αναγκαίου για τους καθορισμένους σκοπούς.
    - Μετρήσιμη ακρίβεια - Περιορισμός του αριθμού των ψευδώς θετικών/αρνητικών αποτελεσμάτων, όπως π.χ. διακρίσεις σε αυτοματοποιημένες αποφάσεις και τεχνητή νοημοσύνη.
    - Επαλήθευση – Ανάλογα με τη φύση των δεδομένων, σε συνάρτηση με το πόσο συχνά μπορεί αυτή να αλλάξει, ο υπεύθυνος επεξεργασίας πρέπει να επαληθεύει την ορθότητα

[38] Άρθρο 5 παράγραφος 1 στοιχείο δ) του ΓΚΠΔ.

των δεδομένων προσωπικού χαρακτήρα με το υποκείμενο των δεδομένων πριν από και κατά τα διάφορα στάδια της επεξεργασίας (π.χ. όσον αφορά τις απαιτήσεις ηλικίας).

- Διαγραφή/διόρθωση – Ο υπεύθυνος επεξεργασίας πρέπει να διαγράφει ή να διορθώνει ανακριβή δεδομένα χωρίς καθυστέρηση. Ο υπεύθυνος επεξεργασίας πρέπει ειδικότερα να διευκολύνει αυτές τις διαδικασίες, εφόσον τα υποκείμενα των δεδομένων είναι ή ήταν παιδιά και επιθυμούν αργότερα την αφαίρεση τέτοιων δεδομένων προσωπικού χαρακτήρα.[39]
- Αποφυγή διάδοσης σφαλμάτων – Οι υπεύθυνοι επεξεργασίας πρέπει να μετριάζουν τις επιπτώσεις ενός συσσωρευμένου σφάλματος στην αλυσίδα επεξεργασίας.
- Πρόσβαση – Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται σχετικά με τα δεδομένα προσωπικού χαρακτήρα και να έχουν αποτελεσματική πρόσβαση σε αυτά σύμφωνα με τα άρθρα 12 έως 15 του ΓΚΠΔ προκειμένου να ελέγχουν την ακρίβειά τους και να προβαίνουν σε διορθώσεις κατά περίπτωση.
- Συνεχής ακρίβεια – Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι ακριβή σε όλα τα στάδια της επεξεργασίας και οι δοκιμές ακρίβειας θα πρέπει να διεξάγονται σε κρίσιμα στάδια.
- Επικαιροποίηση – Τα δεδομένα προσωπικού χαρακτήρα επικαιροποιούνται, αν είναι απαραίτητο, σύμφωνα με τον επιδιωκόμενο σκοπό.
- Σχεδιασμός των δεδομένων - Χρήση τεχνολογικών και οργανωτικών χαρακτηριστικών σχεδιασμού για τον περιορισμό της ανακρίβειας, π.χ. μέσω της πρόβλεψης σύντομων προκαθορισμένων επιλογών αντί πεδίων ελεύθερου κειμένου.

Παράδειγμα 1

Μια ασφαλιστική εταιρεία επιθυμεί να χρησιμοποιήσει την τεχνητή νοημοσύνη (ΤΝ) για τη δημιουργία προφίλ των πελατών της ως βάση για τη λήψη αποφάσεων κατά τον υπολογισμό του ασφαλιστικού κινδύνου. Κατά τον καθορισμό του τρόπου με τον οποίο θα πρέπει να αναπτυχθούν οι λύσεις ΤΝ, ο υπεύθυνος επεξεργασίας καθορίζει τα μέσα επεξεργασίας και πρέπει να λαμβάνει υπόψη του την προστασία των δεδομένων ήδη από τον σχεδιασμό όταν επιλέγει μια εφαρμογή ΤΝ από έναν πωλητή και όταν αποφασίζει πώς να εκπαιδεύσει το σύστημα ΤΝ.

Κατά τον καθορισμό του τρόπου εκπαίδευσης του συστήματος ΤΝ, ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει ακριβή δεδομένα για την επίτευξη ακριβών αποτελεσμάτων. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίσει ότι τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του συστήματος ΤΝ είναι ακριβή.

Δεδομένου ότι διαθέτει τη νομική βάση για την εκπαίδευση του συστήματος ΤΝ με τη χρήση δεδομένων προσωπικού χαρακτήρα από μεγάλο υποσύνολο υφιστάμενων πελατών, ο υπεύθυνος επεξεργασίας επιλέγει μια ομάδα πελατών που είναι αντιπροσωπευτική του πληθυσμού για να αποφευχθούν επίσης οι διακρίσεις.

Τα δεδομένα πελατών συλλέγονται στη συνέχεια από το αντίστοιχο σύστημα χειρισμού δεδομένων, συμπεριλαμβανομένων δεδομένων σχετικά με τον τύπο ασφάλισης, π.χ. ασφάλιση υγείας, ασφάλιση κατοικίας, ταξιδιωτική ασφάλιση κλπ., καθώς και δεδομένων από δημόσια μητρώα στα οποία παρέχεται νόμιμη πρόσβαση. Όλα τα δεδομένα υποβάλλονται σε ψευδωνυμοποίηση πριν από τη μεταφορά τους στο σύστημα που προβλέπεται για την εκπαίδευση στο μοντέλο ΤΝ.

[39] Πρβλ. αιτιολογική σκέψη 65.

Για να διασφαλιστεί ότι τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του συστήματος ΤΝ είναι όσο το δυνατόν ακριβέστερα, ο υπεύθυνος επεξεργασίας συλλέγει μόνο δεδομένα από πηγές δεδομένων με σωστές και επικαιροποιημένες πληροφορίες.

Η ασφαλιστική εταιρεία ελέγχει εάν το σύστημα ΤΝ είναι αξιόπιστο και παρέχει αποτελέσματα που δεν εισάγουν διακρίσεις, τόσο κατά τη φάση της ανάπτυξης όσο και πριν από την κυκλοφορία του προϊόντος. Όταν έχει ολοκληρωθεί η εκπαίδευση του συστήματος ΤΝ και αυτό είναι πλέον λειτουργικό, η ασφαλιστική εταιρεία χρησιμοποιεί τα αποτελέσματα προς υποστήριξη των αξιολογήσεων των ασφαλιστικών κινδύνων, χωρίς ωστόσο να βασίζεται αποκλειστικά και μόνο στο σύστημα ΤΝ προκειμένου να αποφασίσει πότε θα χορηγήσει ασφάλιση, εκτός εάν η απόφαση λαμβάνεται σύμφωνα με τις εξαιρέσεις του άρθρου 22 παράγραφος 2 του ΓΚΠΔ.

Η ασφαλιστική εταιρεία θα ελέγχει επίσης τακτικά τα αποτελέσματα του συστήματος ΤΝ, ώστε να διατηρεί την αξιοπιστία του και, όταν είναι αναγκαίο, να προσαρμόζει τον αλγόριθμο.

Παράδειγμα 2

Ο υπεύθυνος επεξεργασίας είναι ένα νοσηλευτικό ίδρυμα που αναζητά μεθόδους για τη διασφάλιση της ακεραιότητας και της ακρίβειας των δεδομένων προσωπικού χαρακτήρα στα μητρώα των πελατών του.

Στις περιπτώσεις όπου δύο άτομα φθάνουν ταυτόχρονα στο ίδρυμα και λαμβάνουν την ίδια θεραπεία, υπάρχει κίνδυνος να τα μπερδέψουν εάν η μόνη παράμετρος που τα διαφοροποιεί είναι το όνομά τους. Για την εξασφάλιση της ακρίβειας, ο υπεύθυνος επεξεργασίας χρειάζεται ένα μοναδικό αναγνωριστικό για κάθε άτομο, και επομένως περισσότερες πληροφορίες από το όνομα του πελάτη μόνο.

Το ίδρυμα χρησιμοποιεί διάφορα συστήματα που περιλαμβάνουν προσωπικές πληροφορίες πελατών, και πρέπει να διασφαλίζει ότι οι πληροφορίες που αφορούν τον πελάτη είναι σωστές, ακριβείς και συνεκτικές σε όλα τα συστήματα ανά πάσα στιγμή. Το ίδρυμα έχει εντοπίσει πολλούς κινδύνους που ενδέχεται να προκύψουν εάν αλλάξουν οι πληροφορίες σε ένα σύστημα αλλά όχι στα υπόλοιπα.

Ο υπεύθυνος επεξεργασίας αποφασίζει να μετριάσει τον κίνδυνο χρησιμοποιώντας μια τεχνική κατακερματισμού που μπορεί να χρησιμοποιηθεί για την εξασφάλιση της ακεραιότητας των δεδομένων στο αρχείο καταγραφής θεραπειών. Έχουν δημιουργηθεί αμετάβλητες κρυπτογραφικές χρονοσφραγίδες για τα αρχεία καταγραφής θεραπειών και τον πελάτη που συνδέεται με αυτά, ώστε να υπάρχει η δυνατότητα αναγνώρισης, συσχετισμού και ανίχνευσης τυχόν αλλαγών εάν απαιτείται.

3.7 Περιορισμός της περιόδου αποθήκευσης

80. Ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.[40]
Είναι εξαιρετικά σημαντικό για τον υπεύθυνο επεξεργασίας να γνωρίζει επακριβώς ποια προσωπικά δεδομένα υποβάλλονται σε επεξεργασία από την εταιρεία και για ποιους λόγους. Ο σκοπός της

[40] Άρθρο 5 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ.

επεξεργασίας πρέπει να είναι το βασικό κριτήριο όσον αφορά το χρονικό διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα.

81. Τα μέτρα και οι εγγυήσεις που εφαρμόζουν την αρχή του περιορισμού της αποθήκευσης συμπληρώνουν τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, συγκεκριμένα το δικαίωμα διαγραφής και το δικαίωμα προβολής αντιρρήσεων.

82. Τα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού όσον αφορά τον περιορισμό της αποθήκευσης μπορούν να περιλαμβάνουν τα ακόλουθα:

- Διαγραφή και ανωνυμοποίηση – Ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει σαφείς εσωτερικές διαδικασίες και λειτουργίες για τη διαγραφή ή/και την ανωνυμοποίηση.
- Αποτελεσματικότητα της ανωνυμοποίησης/διαγραφής - Ο υπεύθυνος επεξεργασίας διασφαλίζει ότι δεν θα υπάρξει η δυνατότητα να ταυτοποιηθούν εκ νέου ανωνυμοποιημένα δεδομένα ή να ανακτηθούν διαγραμμένα δεδομένα και θα πρέπει να δοκιμάζει εάν αυτό είναι δυνατό.
- Αυτοματοποίηση – Η διαγραφή ορισμένων δεδομένων προσωπικού χαρακτήρα πρέπει να είναι αυτοματοποιημένη
- Κριτήρια αποθήκευσης - Ο υπεύθυνος επεξεργασίας καθορίζει τα δεδομένα και τη διάρκεια αποθήκευσης που είναι αναγκαία για τον σκοπό της επεξεργασίας.
- Αιτιολόγηση – Ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να αιτιολογεί γιατί η περίοδος αποθήκευσης είναι απαραίτητη για τον εκάστοτε σκοπό και για τα αντίστοιχα δεδομένα προσωπικού χαρακτήρα και να μπορεί επίσης να γνωστοποιεί το σκεπτικό και τους νομικούς λόγους που δικαιολογούν την περίοδο διατήρησης.
- Επιβολή πολιτικών διατήρησης - Ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει εσωτερικές πολιτικές διατήρησης και να διενεργεί δοκιμές σχετικά με το εάν ο οργανισμός υλοποιεί τις πολιτικές του.
- Εφεδρικά αντίγραφα/αρχεία καταγραφής – Οι υπεύθυνοι επεξεργασίας καθορίζουν τα δεδομένα προσωπικού χαρακτήρα και τη διάρκεια αποθήκευσης που είναι αναγκαία για τα εφεδρικά αντίγραφα και τα αρχεία καταγραφής
- Ροή δεδομένων – Οι υπεύθυνοι επεξεργασίας πρέπει να έχουν γνώση της ροής των δεδομένων προσωπικού χαρακτήρα και της αποθήκευσης τυχόν αντιγράφων τους, και να επιδιώκουν τον περιορισμό της «προσωρινής» τους αποθήκευσης.

Παράδειγμα

Ο υπεύθυνος επεξεργασίας συλλέγει δεδομένα προσωπικού χαρακτήρα όταν ο σκοπός της επεξεργασίας είναι η χορήγηση ιδιότητας μέλους του υποκείμενου των δεδομένων. Τα δεδομένα προσωπικού χαρακτήρα διαγράφονται όταν λήγει η ισχύς της ιδιότητας μέλους και δεν υφίσταται νομική βάση για την περαιτέρω αποθήκευση των δεδομένων.

Ο υπεύθυνος επεξεργασίας εφαρμόζει καταρχάς εσωτερική διαδικασία για τη διατήρηση και τη διαγραφή δεδομένων. Σύμφωνα με αυτήν, οι υπάλληλοι διαγράφουν χειροκίνητα τα δεδομένα προσωπικού χαρακτήρα μετά τη λήξη της περιόδου διατήρησης. Ο υπάλληλος ακολουθεί τη διαδικασία διαγραφής και διόρθωσης δεδομένων σε τακτά χρονικά διαστήματα από οποιαδήποτε συσκευή, από εφεδρικά αντίγραφα, αρχεία καταγραφής, μηνύματα ηλεκτρονικού ταχυδρομείου και άλλα συναφή μέσα αποθήκευσης.

Για να καταστεί η διαγραφή αποτελεσματικότερη και λιγότερο επιρρεπής στα σφάλματα, ο υπεύθυνος επεξεργασίας εφαρμόζει στη συνέχεια ένα αυτόματο σύστημα προκειμένου να διαγράφει δεδομένα αυτομάτως, αξιόπιστα και πιο τακτικά. Το σύστημα είναι ρυθμισμένο να

ακολουθεί τη δεδομένη διαδικασία για τη διαγραφή δεδομένων, η οποία στη συνέχεια πραγματοποιείται σε προκαθορισμένα τακτά χρονικά διαστήματα για την διαγραφή δεδομένων προσωπικού χαρακτήρα από όλα τα μέσα αποθήκευσης της εταιρείας. Ο υπεύθυνος επεξεργασίας ελέγχει και δοκιμάζει τακτικά τη διαδικασία διατήρησης και διασφαλίζει ότι αυτή ευθυγραμμίζεται με την επικαιροποιημένη πολιτική διατήρησης.

3.8 Ακεραιότητα και εμπιστευτικότητα

83. Η αρχή της ακεραιότητας και της εμπιστευτικότητας περιλαμβάνει την προστασία έναντι της άνευ εξουσιοδότησης και αθέμιτης επεξεργασίας, καθώς και έναντι της τυχαίας απώλειας, καταστροφής ή ζημίας, με τη χρήση των κατάλληλων τεχνικών και οργανωτικών μέτρων. Η ασφάλεια των δεδομένων προσωπικού χαρακτήρα απαιτεί κατάλληλα μέτρα που σχεδιάζονται με σκοπό την πρόληψη και διαχείριση συμβάντων παραβίασης δεδομένων, την εγγύηση της ορθής εκτέλεσης των καθηκόντων επεξεργασίας των δεδομένων και τη συμμόρφωση προς τις υπόλοιπες αρχές, καθώς και τη διευκόλυνση της αποτελεσματικής άσκησης των δικαιωμάτων των ατόμων.

84. Η αιτιολογική σκέψη 78 αναφέρει ότι ένα από τα μέτρα της ΠΔΣΕΟ θα μπορούσε να συνίσταται στο να είναι σε θέση ο υπεύθυνος επεξεργασίας να «δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφάλειας». Παράλληλα με τα άλλα μέτρα της ΠΔΣΕΟ, η αιτιολογική σκέψη 78 αναφέρεται στην ευθύνη των υπεύθυνων επεξεργασίας να αξιολογούν διαρκώς εάν χρησιμοποιούν τα κατάλληλα μέτρα επεξεργασίας ανά πάσα στιγμή και να αξιολογούν εάν τα μέτρα που επιλέγονται αντισταθμίζουν τα υπάρχοντα τρωτά σημεία. Επιπλέον, οι υπεύθυνοι επεξεργασίας πρέπει να επανεξετάζουν τακτικά τα μέτρα ασφάλειας των πληροφοριών που περιβάλλουν και προστατεύουν τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη διαδικασία χειρισμού των παραβιάσεων δεδομένων.

85. Τα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού όσον αφορά την ακεραιότητα και την εμπιστευτικότητα μπορούν να περιλαμβάνουν τα ακόλουθα:
    - Σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) – Ύπαρξη ενός λειτουργικού μέσου για τη διαχείριση πολιτικών και διαδικασιών για την ασφάλεια των πληροφοριών.
    - Ανάλυση κινδύνων – Αξιολόγηση των κινδύνων για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα μέσω της εξέτασης του αντίκτυπου στα δικαιώματα των ατόμων και αντιστάθμιση των εντοπιζόμενων κινδύνων. Για χρήση στην αξιολόγηση κινδύνων, ανάπτυξη και διατήρηση μιας συνολικής, συστηματικής και ρεαλιστικής «μοντελοποίησης απειλών», καθώς και μια ανάλυση επιθέσεων επιφάνειας του σχεδιαζόμενου συστήματος για τον περιορισμό των φορέων επίθεσης και των ευκαιριών εκμετάλλευσης αδύναμων και ευάλωτων σημείων.
    - Ασφάλεια ήδη από τον σχεδιασμό – Εξέταση των απαιτήσεων ασφάλειας όσο το δυνατόν νωρίτερα κατά τον σχεδιασμό του συστήματος και ανάπτυξη με συνεχή ενσωμάτωση και εκτέλεση των σχετικών δοκιμών.
    - Συντήρηση – Τακτικός έλεγχος και δοκιμή λογισμικού, υλισμικού, συστημάτων και υπηρεσιών κλπ., με σκοπό τον εντοπισμό αδυναμιών των συστημάτων που υποστηρίζουν την επεξεργασία.
    - Διαχείριση του ελέγχου πρόσβασης – Μόνο το εξουσιοδοτημένο προσωπικό που τη χρειάζεται πρέπει να έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τα καθήκοντα επεξεργασίας τους, ο δε υπεύθυνος επεξεργασίας πρέπει να διαφοροποιεί τα προνόμια πρόσβασης του εξουσιοδοτημένου προσωπικού.

- Περιορισμός της πρόσβασης (υπάλληλοι) – Διαμόρφωση της επεξεργασίας των δεδομένων με τρόπο ώστε να απαιτείται η πρόσβαση του ελάχιστου δυνατού αριθμού ατόμων σε δεδομένα προσωπικού χαρακτήρα προκειμένου να εκτελέσουν τα καθήκοντά τους, και ανάλογος περιορισμός της πρόσβασης.
- Περιορισμός της πρόσβασης (περιεχόμενο) – Στο πλαίσιο κάθε πράξης επεξεργασίας, περιορισμός της πρόσβασης μόνο σε εκείνα τα χαρακτηριστικά ανά σύνολο δεδομένων που είναι απαραίτητα για την εκτέλεση της εκάστοτε πράξης. Επιπλέον, παροχή πρόσβασης σε δεδομένα υποκειμένων μόνο στον εκάστοτε υπάλληλο στο πεδίο αρμοδιότητας του οποίου εμπίπτουν τα υποκείμενα.
- Διαχωρισμός της πρόσβασης – Διαμόρφωση της επεξεργασίας δεδομένων με τρόπο ώστε κανένα άτομο να μην χρειάζεται συνολική πρόσβαση σε όλα τα δεδομένα που συλλέγονται για ένα υποκείμενο δεδομένων και ακόμη λιγότερη στο σύνολο των δεδομένων προσωπικού χαρακτήρα μιας συγκεκριμένης κατηγορίας υποκειμένων δεδομένων.

- Ασφαλείς διαβιβάσεις – Οι διαβιβάσεις πρέπει να ασφαλίζονται έναντι της μη εξουσιοδοτημένης πρόσβασης και των αλλαγών.
- Ασφαλής αποθήκευση – Η αποθήκευση των δεδομένων πρέπει να ασφαλίζεται έναντι της μη εξουσιοδοτημένης πρόσβασης και των αλλαγών. Πρέπει να προβλέπονται διαδικασίες για την αξιολόγηση του κινδύνου της κεντρικής ή αποκεντρωμένης αποθήκευσης και να ορίζονται οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα για τις οποίες αυτές ισχύουν. Ορισμένα δεδομένα ενδέχεται να χρειάζονται συμπληρωματικά μέτρα ασφάλειας σε σχέση με άλλα ή απομόνωση από άλλα.
- Ψευδωνυμοποίηση – Τα δεδομένα προσωπικού χαρακτήρα και τα εφεδρικά αντίγραφα/αρχεία καταγραφής πρέπει να ψευδωνυμοποιούνται, ως μέτρο ασφαλείας για την ελαχιστοποίηση των κινδύνων πιθανών παραβιάσεων δεδομένων, για παράδειγμα με τη χρήση κατακερματισμού ή κρυπτογράφησης.
- Εφεδρικά αντίγραφα/αρχεία καταγραφής – Διατήρηση εφεδρικών αντιγράφων και αρχείων καταγραφής στον βαθμό που είναι αναγκαίο για την ασφάλεια των πληροφοριών, χρήση διαδρομών ελέγχου και παρακολούθηση συμβάντων ως συνήθης έλεγχος ασφαλείας. Αυτά προστατεύονται από μη εξουσιοδοτημένη ή τυχαία πρόσβαση και αλλαγή και ελέγχονται τακτικά με άμεση αντιμετώπιση τυχόν συμβάντων.
- Ανάκτηση κατεστραμμένων δεδομένων/ συνέχεια των δραστηριοτήτων – Τήρηση των απαιτήσεων για την ανάκτηση κατεστραμμένων δεδομένων πληροφοριακού συστήματος και τη συνέχεια των δραστηριοτήτων με σκοπό την αποκατάσταση της διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα μετά από σοβαρά συμβάντα.
- Προστασία έναντι κινδύνου – Όλες οι κατηγορίες δεδομένων προσωπικού χαρακτήρα πρέπει να προστατεύονται μέσω κατάλληλων μέτρων όσον αφορά τον κίνδυνο παραβίασης της ασφάλειας. Τα δεδομένα που παρουσιάζουν ιδιαίτερους κινδύνους πρέπει, στον βαθμό του εφικτού, να τηρούνται χωριστά από τα υπόλοιπα δεδομένα προσωπικού χαρακτήρα.
- Διαχείριση αντιμετώπισης συμβάντων ασφαλείας – Εφαρμογή συνήθων πρακτικών, διαδικασιών και πόρων για τον εντοπισμό, τον περιορισμό, τον χειρισμό, την αναφορά και τα διδάγματα από τις παραβιάσεις δεδομένων.
- Διαχείριση συμβάντων – Ο υπεύθυνος επεξεργασίας πρέπει να έχει προβλέψει διεργασίες για τον χειρισμό παραβιάσεων και συμβάντων, ώστε να καθιστά το σύστημα επεξεργασίας περισσότερο άρτιο. Αυτές περιλαμβάνουν διαδικασίες γνωστοποίησης, όπως η διαχείριση γνωστοποιήσεων (στην εποπτική αρχή) και πληροφοριών (στα υποκείμενα των δεδομένων).

Παράδειγμα

Ένας υπεύθυνος επεξεργασίας θέλει να εξαγάγει μεγάλες ποσότητες δεδομένων προσωπικού χαρακτήρα από ιατρική βάση δεδομένων που περιέχει ηλεκτρονικά αρχεία περίθαλψης (ασθενών) σε συγκεκριμένο διακομιστή βάσης δεδομένων στην εταιρεία ώστε να επεξεργαστεί τα εξαχθέντα δεδομένα για σκοπούς διασφάλισης ποιότητας. Η εταιρεία έχει αξιολογήσει ότι ο κίνδυνος δρομολόγησης των αποσπασμάτων σε ένα διακομιστή στον οποίο έχουν πρόσβαση όλοι οι υπάλληλοι της εταιρείας είναι πιθανότητα υψηλός για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Καθώς υπάρχει ένα μόνο τμήμα της εταιρείας που χρειάζεται να επεξεργαστεί τα αποσπάσματα δεδομένων των ασθενών, ο υπεύθυνος επεξεργασίας αποφασίζει να επιτρέψει την πρόσβαση στον συγκεκριμένο διακομιστή μόνο στους υπαλλήλους του εν λόγω τμήματος. Επιπλέον, για περαιτέρω περιορισμό του κινδύνου, τα δεδομένα υποβάλλονται σε ψευδωνυμοποίηση πριν από τη μεταφορά τους.

Για τη ρύθμιση της πρόσβασης και για τον περιορισμό ενδεχόμενης ζημίας που μπορεί να προκληθεί από κακόβουλο λογισμικό, η εταιρεία αποφασίζει να διαχωρίσει το δίκτυο και να ορίσει στοιχεία ελέγχου πρόσβασης στον διακομιστή. Επιπλέον, εγκαθίσταται σύστημα παρακολούθησης ασφαλείας και ένα σύστημα ανίχνευσης και πρόληψης εισβολών, το οποίο απομονώνεται από τη συνήθη χρήση. Εγκαθίσταται αυτοματοποιημένο σύστημα ελέγχου για την παρακολούθηση της πρόσβασης και των αλλαγών. Από αυτό δημιουργούνται αναφορές και αυτοματοποιημένες ειδοποιήσεις όταν ρυθμίζονται ορισμένα συμβάντα που σχετίζονται με τη χρήση. Ο υπεύθυνος επεξεργασίας διασφαλίζει ότι έχουν πρόσβαση μόνο οι χρήστες με το κατάλληλο επίπεδο πρόσβασης και βάσει της αρχής περί «ανάγκης γνώσης». Η ακατάλληλη χρήση μπορεί να εντοπιστεί με γρήγορο και απλό τρόπο.

Ορισμένα από τα αποσπάσματα πρέπει να συγκριθούν με νέα αποσπάσματα και, κατά συνέπεια, πρέπει να φυλαχθούν για τρεις μήνες. Ο υπεύθυνος επεξεργασίας αποφασίζει να τα τοποθετήσει σε χωριστές βάσεις δεδομένων του ίδιου διακομιστή και να χρησιμοποιήσει τόσο διαφανή κρυπτογράφηση όσο και κρυπτογράφηση σε επίπεδο στήλης για την αποθήκευσή τους. Τα κλειδιά για την αποκρυπτογράφηση των δεδομένων στηλών αποθηκεύονται σε ειδικά δομοστοιχεία ασφάλειας, τα οποία μπορούν να χρησιμοποιούνται μόνο από εξουσιοδοτημένο προσωπικό αλλά όχι να εξάγονται.

Ο χειρισμός των επερχόμενων συμβάντων καθιστά το σύστημα περισσότερο άρτιο και αξιόπιστο. Ο υπεύθυνος επεξεργασίας κατανοεί ότι πρέπει να ενσωματωθούν προληπτικά και αποτελεσματικά μέτρα και εγγυήσεις στο σύνολο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα τώρα και στο μέλλον, και ότι με αυτόν τον τρόπο μπορεί να συμβάλλει στην πρόληψη μελλοντικών συμβάντων παραβίασης δεδομένων.

Ο υπεύθυνος επεξεργασίας εφαρμόζει τα εν λόγω μέτρα ασφαλείας για την εξασφάλιση της ακρίβειας, της ακεραιότητας και της εμπιστευτικότητας, αλλά και για την πρόληψη της εξάπλωσης κακόβουλου λογισμικού από κυβερνοεπιθέσεις, καθώς και για να καταστήσει τη λύση αξιόπιστη. Η ύπαρξη άρτιων μέτρων ασφάλειας συμβάλλει στην εδραίωση σχέσης εμπιστοσύνης με τα υποκείμενα των δεδομένων.

3.9 Λογοδοσία[41]

86. Η αρχή της λογοδοσίας ορίζει ότι ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για όλες τις προαναφερθείσες αρχές και πρέπει να μπορεί να αποδεικνύει τη συμμόρφωση προς αυτές.

[41] Βλ. αιτιολογική σκέψη 74, σύμφωνα με την οποία οι υπεύθυνοι επεξεργασίας οφείλουν να αποδεικνύουν την αποτελεσματικότητα των μέτρων τους.

87. Ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση προς τις αρχές. Με τον τρόπο αυτό, ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει τις συνέπειες των μέτρων που λαμβάνονται για την προστασία των υποκειμένων των δεδομένων και τους λόγους για τους οποίους τα μέτρα θεωρούνται κατάλληλα και αποτελεσματικά. Για παράδειγμα, αποδεικνύοντας γιατί ένα μέτρο είναι κατάλληλο ώστε να διασφαλίζεται η αποτελεσματική εφαρμογή της αρχής του περιορισμού της αποθήκευσης.

88. Για να μπορεί να επεξεργάζεται υπεύθυνα τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει τόσο τη γνώση όσο και την ικανότητα να εφαρμόζει την προστασία των δεδομένων. Αυτό συνεπάγεται ότι ο υπεύθυνος επεξεργασίας πρέπει να κατανοεί τις υποχρεώσεις του όσον αφορά την προστασία δεδομένων που προβλέπονται από τον ΓΚΠΔ και να είναι σε θέση να συμμορφώνεται προς αυτές.

4 ΆΡΘΡΟ 25 ΠΑΡΑΓΡΑΦΟΣ 3 ΠΙΣΤΟΠΟΙΗΣΗ

89. Σύμφωνα με το άρθρο 25 παράγραφος 3, η πιστοποίηση βάσει του άρθρου 42 μπορεί να χρησιμοποιηθεί ως στοιχείο που αποδεικνύει τη συμμόρφωση προς την ΠΔΣΕΟ. Αντίστροφα, έγγραφα που αποδεικνύουν τη συμμόρφωση προς την ΠΔΣΕΟ μπορούν επίσης να είναι χρήσιμα σε μια διαδικασία πιστοποίησης. Αυτό σημαίνει ότι όταν μια πράξη επεξεργασίας εκ μέρους υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασία έχει πιστοποιηθεί σύμφωνα με το άρθρο 42, οι εποπτικές αρχές το λαμβάνουν υπόψη τους στη συνολική αξιολόγησή τους για τη συμμόρφωση προς τον ΓΚΠΔ, ιδίως όσον αφορά την ΠΔΣΕΟ.

90. Όταν μια πράξη επεξεργασίας εκ μέρους υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασία πιστοποιείται σύμφωνα με το άρθρο 42, τα στοιχεία που συμβάλλουν στην απόδειξη της συμμόρφωσης προς το άρθρο 25 παράγραφος 1 και παράγραφος 2 είναι οι διαδικασίες σχεδιασμού, δηλαδή οι διαδικασίες καθορισμού του μέσου επεξεργασίας, η διακυβέρνηση και τα τεχνικά και οργανωτικά μέτρα για την εφαρμογή των αρχών της προστασίας δεδομένων. Τα κριτήρια πιστοποίησης της προστασίας των δεδομένων καθορίζονται από τους φορείς πιστοποίησης ή τους ιδιοκτήτες συστημάτων πιστοποίησης και στη συνέχεια εγκρίνονται από την αρμόδια εποπτική αρχή ή από το ΕΣΠΔ. Για περαιτέρω πληροφορίες σχετικά με τους μηχανισμούς πιστοποίησης, συμβουλευθείτε τις Κατευθυντήριες γραμμές του ΕΣΠΔ σχετικά με την πιστοποίηση[42] και άλλες σχετικές οδηγίες, που δημοσιεύονται στον διαδικτυακό τόπο του ΕΣΠΔ.

91. Ακόμη και όταν μια πράξη επεξεργασίας λαμβάνει πιστοποίηση σύμφωνα με το άρθρο 42, ο υπεύθυνος επεξεργασίας εξακολουθεί να είναι υπεύθυνος για τη συνεχή παρακολούθηση και βελτίωση της συμμόρφωσης προς τα κριτήρια ΠΔΣΕΟ του άρθρου 25.

5 ΕΦΑΡΜΟΓΗ ΤΟΥ ΑΡΘΡΟΥ 25 ΚΑΙ ΣΥΝΕΠΕΙΕΣ

92. Οι εποπτικές αρχές μπορούν να αξιολογούν την συμμόρφωση προς το άρθρο 25 σύμφωνα με τις διαδικασίες που αναφέρονται στο άρθρο 58. Οι διορθωτικές εξουσίες αναφέρονται στο άρθρο 58 παράγραφος 2 και, σύμφωνα με αυτές, κάθε εποπτική αρχή μπορεί να απευθύνει προειδοποιήσεις, επιπλήξεις, εντολές συμμόρφωσης με τα δικαιώματα των υποκειμένων των δεδομένων, περιορισμούς ή απαγόρευση της επεξεργασίας, διοικητικά πρόστιμα, κ.λπ.

[42] ΕΣΠΔ. «Κατευθυντήριες γραμμές 1/2018 σχετικά με την πιστοποίηση και τον προσδιορισμό κριτηρίων πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 του κανονισμού». Έκδοση 3.0, 4 Ιουνίου 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_el.pdf

93. Η ΠΔΣΕΟ αποτελεί περαιτέρω παράγοντα για τον καθορισμό του επιπέδου των χρηματικών κυρώσεων για παραβάσεις του ΓΚΠΔ, βλ. άρθρο 83 παράγραφος 4.[43] [44]

6 ΣΥΣΤΑΣΕΙΣ

94. Παρότι δεν μνημονεύονται άμεσα στο άρθρο 25, οι εκτελούντες την επεξεργασία και οι παραγωγοί αναγνωρίζονται επίσης ως βασικοί παράγοντες για την εφαρμογή της ΠΔΣΕΟ και πρέπει να γνωρίζουν ότι οι υπεύθυνοι επεξεργασίας υποχρεούνται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μόνο με συστήματα και τεχνολογίες που διαθέτουν ενσωματωμένη προστασία δεδομένων.

95. Κατά την επεξεργασία για λογαριασμό των υπευθύνων επεξεργασίας ή κατά την παροχή λύσεων σε υπευθύνους επεξεργασίας, οι εκτελούντες την επεξεργασία και οι παραγωγοί πρέπει να χρησιμοποιούν την τεχνογνωσία τους, να εδραιώνουν σχέση εμπιστοσύνης με τους πελάτες τους, περιλαμβανομένων των ΜΜΕ, και να τους καθοδηγούν στον σχεδιασμό λύσεων που ενσωματώνουν την προστασία δεδομένων στη διαδικασία επεξεργασίας. Αυτό σημαίνει ότι ο σχεδιασμός των προϊόντων και υπηρεσιών πρέπει να διευκολύνει τις ανάγκες των υπευθύνων επεξεργασίας.

96. Επισημαίνεται ότι, κατά την εφαρμογή του άρθρου 25, ο κύριος στόχος του σχεδιασμού είναι η *αποτελεσματική εφαρμογή* των αρχών και η *προστασία* των δικαιωμάτων των υποκείμενων των δεδομένων μέσω των κατάλληλων μέτρων της επεξεργασίας. Για τη διευκόλυνση και την καλύτερη υιοθέτηση της ΠΔΣΕΟ, οι συστάσεις μας προς τους υπεύθυνους επεξεργασίας, καθώς και προς τους παραγωγούς και εκτελούντες την επεξεργασία είναι οι ακόλουθες:
    - Οι υπεύθυνοι επεξεργασίας πρέπει να σκέφτονται την προστασία δεδομένων από τα *αρχικά στάδια* του προγραμματισμού μιας πράξης επεξεργασίας, ακόμη και πριν από τον καθορισμό του μέσου επεξεργασίας.
    - Όταν ο υπεύθυνος επεξεργασίας διαθέτει υπεύθυνο προστασίας δεδομένων (ΥΠΔ), το ΕΣΠΔ ενθαρρύνει την ενεργό συμμετοχή του ΥΠΔ για την ενσωμάτωση της ΠΔΣΕΟ στις διαδικασίες προμηθειών και ανάπτυξης, καθώς και στον συνολικό κύκλο ζωής της επεξεργασίας.
    - Μια πράξη επεξεργασίας δύναται να *πιστοποιηθεί*. Η ικανότητα πιστοποίησης μιας πράξης επεξεργασίας συνεπάγεται προστιθέμενη αξία για έναν υπεύθυνο επεξεργασίας κατά την επιλογή μεταξύ διαφορετικών λογισμικών, υλισμικών, υπηρεσιών ή/και συστημάτων από παραγωγούς ή εκτελούντες την επεξεργασία. Ως εκ τούτου, οι παραγωγοί πρέπει να προσπαθούν να καταδείξουν την ΠΔΣΕΟ στον κύκλο ζωής της ανάπτυξης μιας λύσης επεξεργασίας. Μια σφραγίδα πιστοποίησης μπορεί επίσης να καθοδηγεί τα υποκείμενα των δεδομένων στην επιλογή τους μεταξύ διαφορετικών αγαθών και υπηρεσιών. Η ικανότητα πιστοποίησης μιας επεξεργασίας μπορεί να αποτελέσει ανταγωνιστικό πλεονέκτημα για παραγωγούς, εκτελούντες την επεξεργασία και υπεύθυνους επεξεργασίας, ενώ ενισχύει ακόμη την εμπιστοσύνη των υποκειμένων των δεδομένων έναντι της επεξεργασίας των

[43] Το άρθρο 83 παράγραφος 2 στοιχείο δ) ορίζει ότι για τον καθορισμό των προστίμων για παραβάσεις του ΓΚΠΔ *«λαμβάνεται δεόντως υπόψη ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν δυνάμει των άρθρων 25 και 32».*

[44] Περισσότερες πληροφορίες σχετικά με τα πρόστιμα περιλαμβάνονται στο έγγραφο της ομάδας εργασίας του άρθρου 29 «Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679». WP 253, 3 Οκτωβρίου 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - οι οποίες εγκρίθηκαν από το ΕΣΠΔ

προσωπικών τους δεδομένων. Εάν δεν παρέχεται πιστοποίηση, οι υπεύθυνοι επεξεργασίας πρέπει να επιδιώκουν άλλες *εγγυήσεις* σύμφωνα με τις οποίες οι παραγωγοί ή οι εκτελούντες την επεξεργασία συμμορφώνονται προς τις απαιτήσεις της ΠΔΣΕΟ.

- Οι υπεύθυνοι επεξεργασίας, οι εκτελούντες την επεξεργασία και οι παραγωγοί πρέπει να λαμβάνουν υπόψη τις υποχρεώσεις τους να παρέχουν στα παιδιά ηλικίας κάτω των 18 ετών και σε άλλες ευάλωτες ομάδες ειδική προστασία σύμφωνα με την ΠΔΣΕΟ.
- Οι παραγωγοί και οι εκτελούντες την επεξεργασία πρέπει να επιδιώκουν τη διευκόλυνση της ΠΔΣΕΟ προκειμένου να υποστηρίζουν την ικανότητα του υπεύθυνου επεξεργασίας να συμμορφώνεται προς τις απαιτήσεις του άρθρου 25. Από την άλλη πλευρά, οι υπεύθυνοι επεξεργασίας δεν πρέπει να επιλέγουν παραγωγούς ή εκτελούντες την επεξεργασία που δεν προτείνουν συστήματα τα οποία επιτρέπουν στον υπεύθυνο επεξεργασίας ή τον υποστηρίζουν στο να συμμορφώνεται προς το άρθρο 25, διότι οι υπεύθυνοι επεξεργασίας θα λογοδοτούν σε περίπτωση μη εφαρμογής των διατάξεων του άρθρου.
- Οι παραγωγοί και εκτελούντες την επεξεργασία πρέπει να διαδραματίζουν ενεργό ρόλο στην εξασφάλιση της τήρησης των κριτηρίων των «τελευταίων εξελίξεων» και να ενημερώνουν τους υπευθύνους επεξεργασίας για τυχόν αλλαγές στις «τελευταίες εξελίξεις» που θα μπορούσαν να επηρεάσουν την αποτελεσματικότητα των μέτρων που εφαρμόζονται. Οι υπεύθυνοι επεξεργασίας θα πρέπει να συμπεριλάβουν την εν λόγω απαίτηση ως συμβατική ρήτρα ώστε να διασφαλίζεται ότι θα ενημερώνονται.
- Το ΕΣΠΔ συνιστά στους υπεύθυνους επεξεργασίας να απαιτούν από τους παραγωγούς και τους εκτελούντες την επεξεργασία να καταδεικνύουν τον τρόπο με τον οποίο το υλισμικό, το λογισμικό, οι υπηρεσίες ή τα συστήματά τους δίνουν τη δυνατότητα στον υπεύθυνο επεξεργασίας να συμμορφώνεται προς τις απαιτήσεις λογοδοσίας σύμφωνα με την ΠΔΣΕΟ, για παράδειγμα χρησιμοποιώντας δείκτες επιδόσεων ώστε να καταδεικνύεται η αποτελεσματικότητα των μέτρων και εγγυήσεων κατά την εφαρμογή των αρχών και των δικαιωμάτων.
- Το ΕΣΠΔ υπογραμμίζει την ανάγκη μιας εναρμονισμένης προσέγγισης για την αποτελεσματική εφαρμογή των αρχών και δικαιωμάτων και ενθαρρύνει ενώσεις και φορείς που καταρτίζουν κώδικες δεοντολογίας σύμφωνα με το άρθρο 40 να ενσωματώσουν επίσης ειδικές για τον τομέα τους οδηγίες σχετικά με την ΠΔΣΕΟ.
- Οι υπεύθυνοι επεξεργασίας θα πρέπει να είναι δίκαιοι έναντι των υποκειμένων των δεδομένων και να επιδεικνύουν διαφάνεια όσον αφορά τον τρόπο με τον οποίο αξιολογούν και αποδεικνύουν την αποτελεσματική εφαρμογή της ΠΔΣΕΟ, με τον ίδιο τρόπο που οι υπεύθυνοι επεξεργασίας αποδεικνύουν τη συμμόρφωσή τους με τον ΓΚΠΔ βάσει της αρχής της λογοδοσίας.
- Τεχνολογίες για τη βελτίωση της προστασίας της ιδιωτικής ζωής, οι οποίες έχουν φτάσει σε επίπεδο ωρίμανσης από πλευράς ανάπτυξης, μπορούν να χρησιμοποιούνται ως μέτρο σύμφωνα με τις απαιτήσεις ΠΔΣΕΟ, εφόσον κρίνεται σκόπιμο στο πλαίσιο προσέγγισης βάσει κινδύνων. Από μόνες τους αυτές οι τεχνολογίες δεν καλύπτουν κατ' ανάγκη τις υποχρεώσεις του άρθρου 25. Οι υπεύθυνοι επεξεργασίας αξιολογούν εάν το μέτρο είναι κατάλληλο και αποτελεσματικό κατά την εφαρμογή των αρχών της προστασίας των δεδομένων προσωπικού χαρακτήρα και των δικαιωμάτων των υποκειμένων των δεδομένων.
- Τα υφιστάμενα συστήματα διέπονται από τις ίδιες υποχρεώσεις ΠΔΣΕΟ όπως και τα νέα συστήματα. Εάν τα παλαιότερα συστήματα δεν συμμορφώνονται ήδη προς την ΠΔΣΕΟ και

δεν μπορούν να γίνουν αλλαγές ώστε να διασφαλιστεί η συμμόρφωση προς τις υποχρεώσεις, τότε αυτά δεν πληρούν απλώς τις υποχρεώσεις ΓΚΠΔ και δεν μπορούν να χρησιμοποιηθούν για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

- Το άρθρο 25 δεν προβλέπει χαμηλότερο κατώφλιο απαιτήσεων για τις ΜΜΕ. Τα ακόλουθα σημεία ενδέχεται να διευκολύνουν τη συμμόρφωση των ΜΜΕ προς το άρθρο 25:
    - Διενέργεια πρώιμων αξιολογήσεων κινδύνου
    - Εκκίνηση με μικρής έκτασης επεξεργασία – και στη συνέχεια διεύρυνση του πεδίου εφαρμογής και της εξειδίκευσής του αργότερα
    - Αναζήτηση εγγυήσεων για την ΠΔΣΕΟ από πλευράς παραγωγών και εκτελούντων την επεξεργασία, όπως πιστοποίηση και τήρηση του κώδικα δεοντολογίας
    - Συνεργασία με εταίρους με καλό ιστορικό
    - Επικοινωνία με τις αρχές προστασίας δεδομένων
    - Ανάγνωση οδηγιών των αρχών προστασίας δεδομένων και του ΕΣΠΔ
    - Τήρηση κωδίκων δεοντολογίας, όπου υπάρχουν
    - Λήψη επαγγελματικής βοήθειας και συμβουλών

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η Πρόεδρος

(Andrea Jelinek)