Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

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

1. Αντίληψη του οργανισμού ότι η προστασία των προσωπικών δεδομένων είναι ευθύνη της Διοίκησης π.χ.
    - Με την ύπαρξη πολιτικών/κανόνων για την επεξεργασία προσωπικών δεδομένων
    - Με την αντίληψη των κινδύνων που ενέχει η επεξεργασία
2. Ορισμός ΥΠΔ
    - Γιατί δεν έχει οριστεί;
    - Αν έχει οριστεί, είναι ξεκάθαρος ο ρόλος του;
    - Έχουν δηλωθεί τα στοιχεία επικοινωνίας του στην ΑΠΔΠΧ;
3. Έλεγχος των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας:
    - είναι σύμφωνα με το σκοπό για τον οποίο έχουν αρχικά συλλεχθεί;
    - είναι μόνο τα απαραίτητα;
    - είναι ορθά και ενημερωμένα;
    - διατηρούνται μόνο για όσο χρονικό διάστημα είναι απολύτως απαραίτητα;
    - λαμβάνονται τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφάλειας και προστασίας τους;
    - αυτά τα μέτρα αναθεωρούνται τακτικά για να λαμβάνουν υπόψη τις νέες τεχνολογικές εξελίξεις;
    - σε κάποια τουλάχιστον μέρη της επεξεργασίας, αντί να χρησιμοποιηθούν πραγματικά δεδομένα, θα μπορούσε να χρησιμοποιηθεί κρυπτογράφηση ή ψευδωνυμοποίηση;
4. Κατάρτιση διαδικασιών για τήρηση Αρχείου Δραστηριοτήτων της επεξεργασίας
5. Κατάρτιση εργαλείων και διαδικασιών που διασφαλίζουν ότι στη φάση σχεδιασμού του έργου/παροχής της υπηρεσίας:
    - συλλέγονται μόνο τα δεδομένα που είναι απαραίτητα για το συγκεκριμένο σκοπό που επιδιώκεται
    - αποφασίζεται το χρονικό διάστημα διατήρησης και τα οργανωτικά και τεχνικά μέτρα ασφάλειας

- η προστασία των προσωπικών δεδομένων αποτελεί αναπόσπαστο μέρος της διαδικασίας ανάπτυξης του έργου/παροχής της υπηρεσίας

6. Εκπαίδευση και ευαισθητοποίηση του προσωπικού:
    - όσοι επεξεργάζονται προσωπικά δεδομένα μέσα στον οργανισμό γνωρίζουν πότε υπάρχει παραβίαση προσωπικών δεδομένων;
7. Υιοθέτηση:
    - εσωτερικής διαδικασίας αναφοράς της παραβίασης
    - εσωτερικού «πλάνου ανταπόκρισης» (response plan) σε περίπτωση παραβίασης
    - διαδικασία γνωστοποίησης ενδεχόμενης παράβασης στην ΑΠΔΠΧ, εντός 72 ωρών
8. Σύναψη συμφωνίας μεταξύ 2 υπεύθυνων επεξεργασίας, σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας
9. Αναθεώρηση των συμβολαίων/συμβάσεων που συνάπτονται με πελάτες, προμηθευτές, υπαλλήλους, εκτελούντες την επεξεργασία (βλ. άρθρο 28 του Κανονισμού για το τι πρέπει να περιλαμβάνει μία σύμβαση ανάθεσης εργασίας σε εκτελούντα)
    - Τι απογίνονται τα δεδομένα μετά τη λήξη της σύμβασης με τον εκτελούντα;
10. Διενέργεια εκτίμησης αντικτύπου εάν η επεξεργασία ενέχει υψηλό κίνδυνο / ρίσκο στα δικαιώματα, ελευθερίες και συμφέροντα των ατόμων:
    - έχει υιοθετηθεί μέθοδος που να αναγνωρίζει εάν υπάρχει υψηλός κίνδυνος;
    - έχει επιλεγεί διαδικασία για διενέργεια ΕΑ;
    - έχει υιοθετηθεί πολιτική με προκαθορισμένη διαδικασία για αντιμετώπιση του υψηλού κινδύνου;
11. Σε περίπτωση διασυνοριακής επεξεργασίας, εντός της ΕΕ, ορισμός του κμ της κύριας εγκατάστασης, του οποίου η εποπτεύουσα αρχή θα είναι αρμόδια ως επικεφαλής αρχή, για την εποπτεία της νομιμότητας της επεξεργασίας εντός της Ε.Ε
12. Αξιολόγηση των συγκαταθέσεων των υποκειμένων, εάν ανταποκρίνονται στις διατάξεις του άρθρου 5 του Κανονισμού
    - Μπορεί πράγματι να αποδειχθεί ότι έχει δοθεί συγκατάθεση;
13. Υιοθέτηση των απαιτήσεων του άρθρου 32 (ασφάλεια):
    - Έχουν αντικατασταθεί οι υφιστάμενες λίστες ελέγχου που αφορούν στους κινδύνους της επεξεργασίας λαμβάνοντας υπόψη τη φύση, πεδίο εφαρμογής, περιεχόμενο και σκοπό της επεξεργασίας;

- Έχει υιοθετηθεί σύστημα διοίκησης για τακτική αναθεώρηση, αξιολόγηση και βελτίωση των μέτρων ασφάλειας;
- Έχουν ληφθεί μέτρα π.χ. ψευδωνυμοποίηση και κρυπτογράφηση για προστασία από παράνομη επεξεργασία από εσωτερικούς και εξωτερικούς εισβολείς;

14. Αναθεώρηση των εντύπων που δίνονται στα υποκείμενα με τα οποία ενημερώνονται για τις πληροφορίες που προβλέπονται στα άρθρα 13 και 14. Για παράδειγμα:
    - στοιχεία επικοινωνίας του ΥΠΔ
    - νομική βάση για την επεξεργασία
    - νομική βάση για διαβίβαση σε τρίτη χώρα (εάν ισχύει)
    - χρονικό διάστημα διατήρησης των δεδομένων
    - τα δικαιώματα που μπορούν να ασκήσουν
    - δικαίωμα υποβολής παραπόνου στην ΑΠΔΠΧ
    - σε περίπτωση που η συγκατάθεση είναι η νομική βάση της επεξεργασίας, να γνωρίζουν ότι μπορούν να την ανακαλέσουν ανά πάσα στιγμή
    - Σε περίπτωση αυτοματοποιημένης λήψης απόφασης (π.χ. κατάρτιση προφίλ), τη λογική, σημασία και επιπτώσεις τέτοιας επεξεργασίας στο υποκείμενο
    - Σε περίπτωση συλλογής των δεδομένων, όχι από το ίδιο το υποκείμενο, την πηγή/προέλευση τους
15. Εφαρμογή διαδικασιών για ικανοποίηση των δικαιωμάτων των υποκειμένων π.χ φορητότητα των δεδομένων
16. Πριν το κλείσιμο λογαριασμού ενός ατόμου, να δίνεται το δικαίωμα στο άτομο να ασκήσει το δικαίωμα στη φορητότητα των δεδομένων του

23/10/2017