ΟΔΗΓΙΕΣ ΣΥΜΜΟΡΦΩΣΗΣ ΣΩΜΑΤΕΙΩΝ ΜΕ GDPR (ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ)

Πίνακας Περιεχομένων

1 Τι είναι προσωπικά δεδομένα;

Σύμφωνα με τη νομοθεσία, προσωπικά δεδομένα είναι κάθε πληροφορία σχετική με ένα φυσικό πρόσωπο, εφόσον αυτό το φυσικό πρόσωπο ταυτοποιείται ή μπορεί να ταυτοποιηθεί (δηλαδή ακόμη και εάν δεν προσδιορίζεται ποιο είναι το πρόσωπο που αφορά η πληροφορία, αλλά αυτό μπορεί να συναχθεί έμμεσα συνδυάζοντας άλλες πληροφορίες).

2 Τι σημαίνει «επεξεργασία προσωπικών δεδομένων»;

Σύμφωνα με την νομοθεσία για την προστασία προσωπικών δεδομένων, επεξεργασία προσωπικών δεδομένων σημαίνει γενικά κάθε πράξη ή σειρά πράξεων που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα με ή χωρίς τη χρήση αυτοματοποιημένων μέσων. Τέτοιες πράξεις μπορεί να περιλαμβάνουν τη συλλογή, την καταχώριση, την οργάνωση, τη διάρθρωση, την αποθήκευση, την προσαρμογή ή τη μεταβολή, την ανάκτηση, την αναζήτηση πληροφοριών, τη χρήση, την κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, τη συσχέτιση ή τον συνδυασμό, τον περιορισμό, τη διαγραφή ή την καταστροφή δεδομένων.

Επομένως, όταν τηρείται ένα αρχείο, ακόμη και εάν δεν γίνεται χρήση των δεδομένων που περιλαμβάνονται σε αυτό, πρόκειται για «επεξεργασία δεδομένων» καθώς η τήρηση του αρχείου προϋποθέτει καταχώριση, οργάνωση και αποθήκευση των δεδομένων.

3 Τι είναι «Υποκείμενο των Δεδομένων»;

Το Υποκείμενο των Δεδομένων είναι το φυσικό πρόσωπο το οποίο ταυτοποιείται ή μπορεί να ταυτοποιηθεί και στο οποίο αναφέρονται τα προσωπικά δεδομένα που υπόκεινται σε επεξεργασία. Υποκείμενα των δεδομένων μπορούν να είναι οι αθλητές, των οποίων τα στοιχεία επεξεργάζεται το σωματείο ή η ένωση, οι εργαζόμενοι των σωαμτείων, οι εθελοντές, οι προπονητές, τα διοικητικά στελέχη των σωματείων και γενικώς κάθε φυσικό πρόσωπο. Τα νομικά πρόσωπα, δηλαδή εταιρείες ή άλλοι φορείς δεν αποτελούν «υποκείμενα δεδομένων» και δεν προστατεύονται από τη νομοθεσία περί προστασίας προσωπικών δεδομένων.

4 Γιατί είναι σημαντική η προστασία των προσωπικών δεδομένων;

Η προστασία των προσωπικών δεδομένων είναι σημαντική διότι εξισορροπεί το δικαίωμα των ατόμων στην ιδιωτικότητα και την ανάγκη των οργανισμών και των επαγγελματιών να επεξεργάζονται δεδομένα για επαγγελματικούς σκοπούς.

Αφενός, τα άτομα πρέπει να απολαύουν το δικαίωμα στην ιδιωτικότητα στον βαθμό που επιθυμούν και σε κάθε περίπτωση να έχουν τον έλεγχο των δεδομένων τους και να γνωρίζουν ποιοι τα επεξεργάζονται και για ποιο σκοπό. Αφετέρου, οι οργανισμοί και οι επαγγελματίες πρέπει να χρησιμοποιούν προσωπικά δεδομένα υπό τις προϋποθέσεις της νομοθεσίας για να ασκούν την επαγγελματική τους δραστηριότητα, να παρέχουν τις υπηρεσίες τους, να συμμορφώνονται με τις υποχρεώσεις τους και να εξυπηρετούν τα συμφέροντά τους.

Όταν τα σωματεία φροντίζουν για τη συμμόρφωσή τους με το ισχύον πλαίσιο για την ιδιωτικότητα, αποδεικνύουν έμπρακτα ότι σέβονται την ιδιωτικότητα των αθλητών τους προστατεύοντας τα ευαίσθητα δεδομένα τους. Παράλληλα, αποφεύγουν την έκθεση σε σημαντικούς κινδύνους, όπως την εμπλοκή σε έρευνες της αρμόδιας αρχής, σε δικαστικές υποθέσεις διοικητικής, αστικής και

ποινικής φύσεως, την καταβολή υψηλών προστίμων προς τις αρχές και αποζημιώσεων προς ιδιώτες, την απώλεια φήμης και εσόδων. Ως εκ τούτου, η συμμόρφωση έχει εξαιρετική σημασία.

5 Τι είναι ο ΓΚΠΔ (GDPR);

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation / GDPR, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679) («Κανονισμός») περιλαμβάνει το νέο νομικό πλαίσιο για την προστασία δεδομένων. Δημοσιεύθηκε στις 27 Απριλίου 2016 και τίθεται σε εφαρμογή από τις 25 Μαΐου 2018. Ο Κανονισμός έχει άμεση εφαρμογή σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης και δεν χρειάζεται τα τελευταία να ενσωματώσουν τις διατάξεις του στην εθνική νομοθεσία τους. Στην Ελλάδα ψηφίστηκε ο Ν. 4624/2019 ο οποίος εξειδικεύει τις απαιτήσεις του GDPR στο Ελληνικό νομικό πλαίσιο.

6 Αλλαγές Κανονισμού σε σχέση με προηγούμενο Νομικό Πλαίσιο

Ο Κανονισμός εισάγει αρκετές αλλαγές στο προηγούμενο νομικό καθεστώς για την προστασία των φυσικών προσώπων αναφορικά με την επεξεργασία των προσωπικών δεδομένων τους και θεσπίζει αυξημένες υποχρεώσεις για οποιονδήποτε οργανισμό επεξεργάζεται προσωπικά δεδομένα. Κατάργηση γνωστοποιήσεων/ αδειών: Πλέον δεν απαιτείται προηγούμενη γνωστοποίηση της επεξεργασίας δεδομένων στην αρχή προστασίας δεδομένων ούτε είναι απαραίτητο να ληφθεί προηγούμενη άδεια της αρχής σε περιπτώσεις επεξεργασίας ευαίσθητων δεδομένων (ή «ειδικών κατηγοριών δεδομένων» σύμφωνα με τους όρο που χρησιμοποιείται στον Κανονισμό), όπως τα δεδομένα που αφορούν την υγεία. Είναι όμως αναγκαίο να λαμβάνονται τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των ατόμων. Όσοι επεξεργάζονται προσωπικά δεδομένων θα πρέπει να είναι σε θέση να αποδεικνύουν τη συμμόρφωσή τους με το νέο νομικό πλαίσιο και να ενημερώνουν αντίστοιχα την αρμόδια αρχή και τα ενδιαφερόμενα πρόσωπα.

6.1 Αρχή της Λογοδοσίας

Ο Κανονισμός εισάγει την αρχή της «λογοδοσίας», που σημαίνει ότι όσοι επεξεργάζονται προσωπικά δεδομένα δεν αρχεί να συμμορφώνονται με τις υποχρεώσεις τους, αλλά πρέπε και να είναι σε θέση να αποδείξουν τη συμμόρφωσή τους. Συγκεκριμένα, πρέπει να τηρούν επικαιροποιημένα αρχεία των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων καθώς και να εφαρμόζουν διαδικασίες που αντανακλούν όλες τις αρχές τις επεξεργασίας και αντιμετωπίζουν ορθά οποιαδήποτε αιτήματα προβάλλουν τα υποκείμενα των δεδομένων. Όποιος επεξεργάζεται προσωπικά δεδομένα πρέπει να ορίζει και να καταγράφει τη νομική βάση και τον σκοπό της επεξεργασίας και να προάγει την διαφάνεια κάθε επεξεργασίας. Σε ορισμένες περιπτώσεις, όπως αναφέρεται κατωτέρω, εκείνοι που επεξεργάζονται προσωπικά δεδομένα χρειάζεται να διενεργούν Εκτιμήσεις Αντικτύπου σχετικά με την Προστασία Δεδομένων, όταν η επεξεργασία δεδομένων είναι υψηλού ρίσκου, και να διορίζουν, εφόσον απαιτείται, Υπεύθυνο Προστασίας Δεδομένων.

6.2 Αρχές Επεξεργασίας & Ενισχυμένα δικαιώματα των υποκειμένων

Ο Κανοινσμός ορίζει πλέον με σαφή τρόπο τις βασικές αρχές που πρέπει να τηρούνται σε κάθε επεξεργασία προσωπικών δεδομένων και ενιχύει τα δικαιώματα των επηρεαζόμενων προσώπων. Επεξεργασία προσωπικών δεδομένων χωρεί μόνο όταν πληρούνται τα κριτήρια που θέτει η νομοθεσία για την προστασία των δεδομένων. Όποιος επεξεργάζεται προσωπικά δεδομένα οφείλει να τηρεί τις αρχές του Κανονισμού, όπως η ελαχιστοποίηση των δεδομένων, η ακρίβεια, η ακεραιότητα και η εμπιστευτικότητα των δεδομένων, κτλ.

6.3 Αυστηρότερες προϋποθέσεις για να είναι έγκυρη η συναίνεση
Όταν η επεξεργασία των δεδομένων βασίζεται στην συγκατάθεση του ατόμου, θα πρέπει να διασφαλίζεται, επιπλέον των κριτηρίων που είχαν τεθεί από το προηγούμενο νομικό πλαίσιο, ότι η συγκατάθεση είναι σαφής και λεπτομερής. Πριν συναινέσει πρέπει να έχει ενημερωθεί επαρκώς σχετικά με το ποιος θα επεξεργαστεί τα δεδομένα του και για ποιο σκοπό. Ειδικά για τα δεδομένα υγείας, όταν η επεξεργασία τους βασίζεται σε συγκατάθεση, πρέπει αυτή να είναι ρητή.
6.4 Νέα δικαιώματα
Στα υποκείμενα των δεδομένων παρέχονται περισσότερα δικαιώματα σε σχέση με το προηγούμενο καθεστώς (δικαίωμα διαγραφής – «δικαίωμα στη λήθη», δικαίωμα στη φορητότητα δεδομένων, κτλ.).
6.5 Προστασία Δεδομένων εκ του σχεδιασμού
Τα μέτρα για την προστασία των προσωπικών δεδομένων πρέπει να λαμβάνονται ήδη από τον σχεδιασμό των διαδικασιών και εξ ορισμού.
6.6 Συνεργασία με τρίτους για επεξεργασία δεδομένων
Όποιος επεξεργάζεται προσωπικά δεδομένα θα πρέπει να εφαρμόζει νέες προδιαγραφές στις συνεργασίες του με τρίτα μέρη, οι οποίοι ενδέχεται να ενεργούν ως υπεύθυνοι ή συνυπεύθυνοι της επεξεργασίας ή εκτελούντες την επεξεργασία.
6.7 Γνωστοποίηση παραβιάσεων
Σε περίπτωση διαπιστωμένης παραβίασης προσωπικών δεδομένων θα πρέπει να γίνεται γνωστοποίηση στην αρμόδια εποπτική αρχή με τον τρόπο και εντός της προθεσμίας που προβλέπεται από το νομικό πλαίσιο. Περισσότερες λεπτομέρειες για τις παραπάνω έννοιες (αρχές, δικαιώματα, τεχνικά και οργανωτικά μέτρα, υποχρεώσεις γνωστοποίησης παραβίασης προσωπικών δεδομένων) θα βρείτε στις επόμενες ενότητες.
6.8 Κίνδυνος μη συμμόρφωσης
Ο Κανονισμός αυξάνει σημαντικά τους κινδύνους εκ της μη συμμόρφωσης για τα φυσικά ή νομικά πρόσωπα που επεξεργάζονται δεδομένα. Τα πρόστιμα που προβλέπονται σε περίπτωση παραβίασης της νομοθεσίας για την προστασία των προσωπικών δεδομένων μπορούν να αγγίξουν τα 20 εκατομμύρια Ευρώ ή το 4% του ετήσιου παγκόσμιου κύκλου εργασιών, ανάλογα με το ποιο είναι υψηλότερο. Επιπρόσθετα, αυξάνονται οι ελεγκτικές αρμοδιότητες των αρχών για την προστασία των προσωπικών δεδομένων, οι οποίες μπορούν να διενεργούν ελέγχους και επιτόπιες εφόδους, πρόσβαση στα προσωπικά δεδομένα που αποτελούν αντικείμενο επεξεργασίας, κτλ.

7 Ποιά δεδομένα αποτελούν «ειδικές κατηγορίες δεδομένων»;
Η επεξεργασία ορισμένων κατηγοριών προσωπικών δεδομένων μπορεί να έχει σημαντικό αντίκτυπο στα δικαιώματα των ατόμων στην ιδιωτικότητα και, άρα, πρέπει να προστατεύονται με αυξημένα μέτρα ασφάλειας σε σχέση με άλλες κατηγορίες προσωπικών δεδομένων. Ο Κανονισμός περιγράφει τα δεδομένα αυτά ως οποιαδήποτε δεδομένα που είναι σε θέση να αποκαλύψουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, τα γενετικά ή βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό. Η επεξεργασία των εν λόγω δεδομένων κατά κανόνα

απαγορεύεται, εκτός εάν συντρέχουν οι προϋποθέσεις που ορίζει ο κανονισμός (δείτε κατωτέρω, «Πότε επιτρέπεται η επεξεργασία ειδικών κατηγοριών δεδομένων;»).
Δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα διενεργείται μόνο υπό τον έλεγχο επίσημης αρχής ή υπό την προϋπόθεση ότι η νομοθεσία προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Επομένως, δεν μπορούν να ζητούνται αδιακρίτως ποινικά μητρώα συνεργατών ή εργαζομένων, παρά μόνο ότι υπό προϋποθέσεις και συγκεκριμένους σκοπούς.
Θα πρέπει να δοθεί ιδιαίτερη προσοχή στο γεγονός ότι η νομική βάση της επεξεργασίας των ειδικών κατηγοριών δεδομένων διαφέρει από τη νομική βάση των μη ειδικών κατηγοριών.

8. Πότε επιτρέπεται η επεξεργασία ειδικών κατηγοριών δεδομένων;

Η επεξεργασία ειδικών κατηγοριών δεδομένων επιτρέπεται υπό προϋποθέσεις. Περιπτώσεις στις οποίες επιτρέπεται η επεξεργασία των ειδικών κατηγοριών δεδομένων, οι οποίες τυγχάνουν εφαρμογής όταν διενεργείται επεξεργασία από επαγγελματίες υγείας, αποτελούν ενδεικτικά
Α) η επεξεργασία που γίνεται με ρητή συγκατάθεση του υποκειμένου,
b) η επεξεργασία που γίνεται για την προστασία των ζωτικών συμφερόντων του υποκειμένου ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,
c) η επεξεργασία που είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία ή άθληση του εργαζομένου ή του αθλητού, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει της εφαρμοστέας νομοθεσίας ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας,
d) η επεξεργασία που είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων.
Ο Κανονισμός προβλέπει και άλλες περιπτώσεις στις οποίες επιτρέπεται η επεξεργασία ειδικών κατηγοριών δεδομένων, ωστόσο οι ανωτέρω είναι οι πιο συνήθεις νόμιμες βάσεις για την επεξεργασία δεδομένων. Διευκρινίζεται ότι δε χρειάζεται να συντρέχουν όλες οι ανωτέρω προϋποθέσεις, αρκεί μία από αυτές για να θεμελιωθεί η νόμιμη βάση της επεξεργασίας.

9 Εξασφάλιση έγκυρης συγκατάθεσης για την επεξεργασία ειδικών κατηγοριών δεδομένων;

Ως συγκατάθεση του υποκειμένου των δεδομένων ορίζεται κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

10 Πρέπει να τηρώ Αρχείο Δραστηριοτήτων Επεξεργασίας;

Το άρθρο 30 προβλέπει την υποχρέωση του Υπεύθυνου Επεξεργασίας να τηρεί ένα αρχείο όπου καταγράφονται οι δραστηριότητες επεξεργασίας για τις οποίες είναι υπεύθυνος. Το αρχείο πρέπει να περιλαμβάνει:

Όνομα και στοιχεία επικοινωνίας υπεύθυνου επεξεργασίας, εκπροσώπου και DPO (εάν έχει οριστεί)
Σκοπούς επεξεργασίας
Κατηγορίες υποκειμένων δεδομένων (π.χ. αθλητές, εργαζόμενοι)
Κατηγορίες αποδεκτών στους οποίους γνωστοποιούνται τα δεδομένα
Διαβιβάσεις σε τρίτες χώρες ή διεθνείς οργανισμούς
Προβλεπόμενες προθεσμίες διαγραφής
Τεχνικά και οργανωτικά μέτρα ασφάλειας
Στην παράγραφο 5 προβλέπεται παρέκλιση από αυτήν την υποχρεώση για επιχειρήσεις ή οργανισμούς που απασχολούν λιγότερο από 250 άτομα. Ωστόσο, η παρέκκλιση που προβλέπεται στο άρθρο 30 παράγραφος 5 δεν είναι απόλυτη.
Υπάρχουν τρεις τύποι επεξεργασίας στην οποία δεν εφαρμόζεται:

Επεξεργασία που ενδέχεται να έχει ως αποτέλεσμα κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

Επεξεργασία που δεν είναι περιστασιακή.
Επεξεργασία που περιλαμβάνει ειδικές κατηγορίες δεδομένων ή προσωπικά δεδομένα που αφορούν σε ποινικές καταδίκες και αδικήματα.
Συνεπώς, όταν γίνεται επεξεργασία δεδομένων υγείας, που εμπίπτουν στην κατηγορία των ειδικών κατηγοριών δεδομένων (δελτίο υγείας), δεν ισχύει η παρέκλιση. Επιβάλλεται η τήρηση αρχείου επεξεργασίας, ακόμη και εάν ο υπεύθυνος επεξεργασίας απασχολεί λιγότερα από 250 άτομα. Ωστόσο, οι οργανισμοί αυτοί πρέπει να τηρούν αρχεία επεξεργασίας μόνογια τις μορφές επεξεργασίας που αναφέρονται στο άρθρο 30 παράγραφος 5, όχι για κάθε επεξεργασία.
11 Τι σημαίνει παραβίαση δεδομένων προσωπικού χαρακτήρα;
Παραβίαση δεδομένων προσωπικού χαρακτήρα συντελείται όταν υπάρχει παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, χωρίς άδεια γνωστοποίηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που αποτέλεσαν αντικείμενο επεξεργασίας. Η ασφάλεια των ειδικών κατηγοριών δεδομένων, στα οποία περιλαμβάνονται τα δεδομένα υγείας, είναι μέγιστης σημασίας για τα συμφέροντα των υποκειμένων.
Επομένως, είναι σημαντικό να λαμβάνεται υπ’ όψιν ότι η προστασία των δεδομένων δεν αφορά μόνο την προστασία της εμπιστευτικότητάς τους (αποτροπή διαρροής), αλλά και της ακεραιότητάς τους (αποτροπή της αλλοίωσής τους) και της διαθεσιμότητάς τους (αποτροπή απώλειας). Ο τύπος παραβίασης που έχει συμβεί πρέπει να λαμβάνεται υπ’ όψιν για να προσδιοριστεί ο κίνδυνος που προκαλείτα από αυτήν.
12 Τι είναι Υπεύθυνος της επεξεργασίας;
Ο Υπεύθυνος της επεξεργασίας είναι το φυσικό ή νομικό πρόσωπο, το οποίο καθορίζει, μεμονωμένα ή μαζί με άλλους, τους σκοπούς και τα μέσα της επεξεργασίας προσωπικών δεδομένων.
Όταν αναφερομαστε σε ένα σωματείο, ο Υπεύθυνος Επεξεργασίας είναι η διοίκηση του σωματείου, που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών δεδομένων στο πλαίσιο λειτουργίας του.

13 Τι είναι Εκτελών την Επεξεργασία;

Ο Εκτελών την Επεξεργασία είναι ένα φυσικό ή νομικό πρόσωπο που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπεύθυνου Επεξεργασίας. Ενδεικτικά, εκτελούντες την επεξεργασία μπορεί να είναι εξωτερικοί συνεργάτες που παρέχουν υπηρεσίες ή συστήματα πληροφορικής που χρησιμοποιούνται για τη διαβίαση ή αποθήκευση προσωπικών δεδομένων.

14 Τι πρέπει να γνωρίζω όταν συνεργάζομαι με έναν Εκτελούντα την Επεξεργασία;

Ο Υπεύθυνος Επεξεργασίας υποχρεούται να χρησιμοποιεί μόνο Εκτελούντες την Επεξεργασία που παρέχουν επαρκείς εγγυήσεις για την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων κατά τρόπον ώστε η επεξεργασία να πληροί τις απαιτήσεις της νομοθεσίας για την προστασίας των προσωπικών δεδομένων.

Η επεξεργασία από έναν Εκτελούντα την Επεξεργασία πρέπει να διέπεται από σύμβαση ή νόμο που δεσμεύει τον τελευταίο και οριοθετεί το αντικείμενο, τη διάρκεια, τη φύση και τον σκοπό της επεξεργασίας, τον τύπο των δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες των προσώπων στα οποία αναφέρονται τα δεδομένα και τις υποχρεώσεις και τα δικαιώματα του Υπεύθυνου Επεξεργασίας.

15 Τι είναι ο Υπεύθυνος Προστασίας Δεδομένων (DPO);

Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) διορίζεται από τον Υπεύθυνο Επεξεργασίας και είναι αρμόδιος να επιβλέπει την εφαρμογή της στρατηγικής και των πολιτικών για την προστασία των δεδομένων ώστε να διασφαλίζεται η συμμόρφωση με την ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων.

16 Σε ποιες περιπτώσεις είναι υποχρεωτικός ο ορισμός DPO;

Ο ορισμός του DPO καθίσταται υποχρεωτικός σε κάθε περίπτωση όπου: α. Η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα. Εξαιρούνται τα δικαστήρια όταν ασκούν δικαιοδοτικό έργο, β. Απαιτείται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, γ. Διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα. Ειδική κατηγορία δεδομένων συνιστούν τα δεδομένα υγείας και επομένως, οι ιατροί και οι λοιποί επαγγελματίες του κλάδου υγείας ενδέχεται να εμπίπτουν στην περίπτωση γ’ κατά την οποία λαμβάνει χώρα επεξεργασία δεδομένων υγείας σε μεγάλη κλίμακα.

17 Εκτίμηση Αντικτύπου στην προστασία των προσωπικών δεδομένων

Εκτίμηση αντικτύπου είναι μια μελέτη που υπερβαίνει την απλή ανάλυση των κινδύνων προστασίας προσωπικών δεδομένων. Περιλαμβάνει τουλάχιστον τα εξής:

a) Συστηματική περιγραφή των πράξεων επεξεργασίας και των σκοπών

b) Εκτίμηση της αναγκαιότητας και της αναλογικότητας της επεξεργασίας σε σχέση με τους σκοπούς που επιδιώκονται

c) Εκτίμηση των κινδύνων που δημιουργεί η επεξεργασία στα υποκείμενα των δεδομένων

d) Την καταγραφή των προβλεπόμενων μέτρων αντιμετώπισης των κινδύνων.

Η διεξαγωγή της Εκτίμησης Αντικτύπου προβλέπεται ρητώς στο Άρθρο 35 του ΓΚΠΔ, απορρέει όμως και από την αρχή της λογοδοσίας, που αποτελεί βασική αρχή η οποία διατρέχει τον Κανονισμό. Οι επιχειρήσεις πρέπει να είναι σε θέση να αποδείξουν ότι οι αρχές της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων εξετάζονται και λαμβάνονται σοβαρά υπόψη. Η διενέργεια Εκτίμησης Αντικτύπου απαιτείται ιδίως στην περίπτωση μεγάλης κλίμακας επεξεργασίας δεδομένων υγείας.

18 Ποια είναι τα δικαιώματα του υποκειμένου των δεδομένων στο πλαίσιο του ΓΚΠΔ;

Το υποκείμενο των δεδομένων έχει τα ακόλουθα δικαιώματα σύμφωνα με το νομικό πλαίσιο ΓΚΠΔ:

- Δικαίωμα Πρόσβασης στα Προσωπικά σας Δεδομένα: Σας δίνεται η δυνατότητα να λάβετε ένα αντίγραφο του αρχείου των προσωπικών δεδομένων που διατηρούμε για εσάς
- Δικαίωμα Διόρθωσης: Σας δίνεται η δυνατότητα να αιτηθείτε να διορθωθούν πληροφορίες που χρήζουν είτε επικαιροποίησης είτε διόρθωσης.
- Δικαίωμα Διαγραφής (ή «Λήθης»): Σας δίνεται η δυνατότητα να αιτηθείτε να διαγραφούν τα προσωπικά σας δεδομένα (όπου αυτό είναι εφικτό).
- Δικαίωμα Εναντίωσης στην Επεξεργασία των Δεδομένων σας: Σας δίνεται η δυνατότητα να αντιταχθείτε, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή σας, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που σας αφορούν.
- Δικαίωμα Περιορισμού στην Επεξεργασία: Σας δίνεται το δικαίωμα να υποβάλετε αίτημα για να περιορίσετε την επεξεργασία και να διατηρήσετε μόνο τις αποθηκευμένες πληροφορίες μέχρι να επιλυθεί η βάση του αιτήματός σας. Η κοινοποίηση εσφαλμένων πληροφοριών που θα διατηρηθούν θα περιορίσει αυτόματα την επεξεργασία των προσωπικών σας δεδομένων μέχρι να διορθωθούν αυτές οι πληροφορίες. Έχετε το δικαίωμα ρητά και εγγράφως να ζητήσετε από τον Όμιλο να κρατήσει εκ μέρους σας τα προσωπικά σας στοιχεία, τα οποία δεν επεξεργαζόμαστε πλέον.
- Δικαίωμα στη Φορητότητα: Σας δίνεται η δυνατότητα να αιτηθείτε την λήψη αντιγράφου των προσωπικών δεδομένων που σας αφορούν είτε άμεσα σε εσάς είτε σε οποιοδήποτε οργανισμό επιθυμείτε.
- Δικαίωμα Αναίρεσης της Συναίνεσης σας: Σε περίπτωση που μας δώσετε τη συναίνεσή σας για συγκεκριμένη επεξεργασία, έχετε το δικαίωμα να την αναιρέσετε ανά πάσα στιγμή.

19 Ποιες είναι οι γενικές αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων;

Τα σωματεία πρέπει να διασφαλίσουν ότι η επεξεργασία των προσωπικών δεδομένων συμμορφώνεται με τις έξι ακόλουθες γενικές αρχές που ορίζονται από τη νομοθεσία προστασίας των προσωπικών δεδομένων:

- Νομιμότητα, δικαιοσύνη και διαφάνεια - Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε νόμιμη, δίκαιη και διαφανή επεξεργασία.
- Περιορισμός του σκοπού - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται για συγκεκριμένους, σαφείς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο ασυμβίβαστο προς τους σκοπούς αυτούς (με εξαιρέσεις για δημόσιο συμφέρον, επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς).

- Ελαχιστοποίηση δεδομένων - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι επαρκή, συναφή και να περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- Ακρίβεια / ποιότητα δεδομένων - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή και, όπου χρειάζεται, να ενημερώνονται. Ανακριβή προσωπικά δεδομένα που πρέπει να διαγραφούν ή να διορθωθούν χωρίς καθυστέρηση.
- Διατήρηση - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να φυλάσσονται σε αναγνωρίσιμη μορφή για όχι περισσότερο από ό, τι είναι απαραίτητο (με εξαιρέσεις για δημόσιο συμφέρον, επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς)
- Ακεραιότητα και εμπιστευτικότητα - Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να διασφαλίζει την κατάλληλη ασφάλεια των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και κατά τυχαίας καταστροφής ή ζημίας, χρησιμοποιώντας κατάλληλα τεχνικά ή οργανωτικά μέτρα.

20 Ποια είναι τα κατάλληλα τεχνικά και οργανωτικά μέτρα;

Ο Κανονισμός δεν ορίζει συγκεκριμένα τεχνικά μέτρα που πρέπει να λαμβάνονται (αν και σε σχετικές οδηγίες προτείνει τα μέτρα από το ISO 27002) για την ασφάλεια της προστασίας προσωπικών δεδομένων, όπως είναι εύλογο, καθώς το ποια μέτρα είναι κατάλληλα εξαρτάται από πολλούς παράγοντες και κυρίως από τον κίνδυνο που συνδέεται με κάθε επεξεργασία (ανάλογα με το είδος και το εύρος των δεδομένων), το σκοπό της επεξεργασίας κ.ο.κ..

Ο Κανονισμός αναφέρεται ενδεικτικά στην ψευδωνυμοποίηση και την κρυπτογράφηση. Πέραν αυτού, εστιάζει κυρίως στο επιδιωκόμενο αποτέλεσμα αφήνοντας κάθε υπόχρεο (υπεύθυνο ή εκτελούντα την επεξεργασία) να σταθμίσει όλους τους παράγοντες και να επιλέξει τα κατάλληλα μέτρα ασφάλειας. Τα μέτρα ασφάλειας πρέπει να είναι κατάλληλα ώστε να διασφαλίζεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα και η αξιοπιστία των συστημάτων επεξεργασίας σε συνεχή βάση. Ενδεικτικά, σε ένα μικρό σωματείο που χρησιμοποιεί κοινό υπολογιστή, τέτοια μέτρα περιλαμβάνουν τη χρήση λογισμικού που αποτρέπει κακόβουλες επιθέσεις, τον περιορισμό της πρόσβασης στα συστήματα μέσω κωδικών, την τήρηση αντιγράφων ασφαλείας – back up, κλπ.

21 Γνωστοποίηση Παραβίασης Προσωπικών Δεδομένων

Οι υποχρεώσεις γνωστοποίησης (στις εποπτικές αρχές και στα πρόσωπα στα οποία αναφέρονται τα δεδομένα) ενεργοποιούνται όταν διαπιστώνεται "τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη γνωστοποίηση προσωπικών δεδομένων ή πρόσβαση σε αυτά". Το πεδίο εφαρμογής του Κανονισμού καταλαμβάνει μόνο τις πραγματικές παραβιάσεις και όχι τις δυνητικές.

Ο Κανονισμός απαιτεί από τους υπεύθυνους επεξεργασίας δεδομένων να γνωστοποιούν την παραβίαση στις αρμόδιες αρχές προστασίας δεδομένων (εν προκειμένω για την Ελλάδα αρμόδια είναι η "Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα") χωρίς καθυστέρηση και, εν πάση περιπτώσει, εντός 72 ωρών από τη στιγμή που έχουν λάβει γνώση της παραβίασης αυτής. Ειδικότερα, ο Υπεύθυνος Επεξεργασίας οφείλει:

Να γνωστοποιήσει μια παραβίαση στην ΑΠΔΠΧ εάν η παραβίαση ενδέχεται να προκαλέσει κίνδυνο για τα υποκείμενα των δεδομένων

Να ενημερώσει τα ίδια τα υποκείμενα των δεδομένων που θίγονται, εάν η παραβίαση ενδέχεται να τους προκαλέσει υψηλό κίνδυνο.

21.1 Παραδείγματα
Απώλεια λίστας με ονοματεπώνυμα και τηλέφωνα αθλητών που διατηρεί ένα σωματείο. Η λίστα περιέχει προσωπικά δεδομένα, επομένως η διαρροή ή απώλειά της συνιστά παραβίαση. Ωστόσο, η παραβίαση αυτή δεν δημιουργεί κάποιο κίνδυνο για τους αθλητές των οποίων τα στοιχεία περιλαμβάνονται στη λίστα. Δεν απαιτείται γνωστοποίηση στην ΑΠΔΠΧ ούτε ενημέρωση των ατόμων που περιλαμβάνονται στη λίστα.
Αν ένα σωματείο τηρεί δελτία υγείας αθλητών και αυτά παραβιαστούν θα πρέπει να γίνει.
Το φορητό μέσο αποθήκευσης στο οποίο αποθηκεύονται μεταξύ άλλων και δεδομένα υγείας αθλητών κλέβεται. Τα αρχεία είναι κρυπτογραφημένα και δεν υπάρχει πρόσβαση στο κλειδί της αποκρυπτογράφησης.. Θα πρέπει να αξιολογηθεί εάν υπάρχει πιθανότητα αποκρυπτογράφησης των αρχείων (λαμβάνοντας υπ' όψιν τα δεδομένα κάθε περίπτωσης). Εάν τα αρχεία δεν μπορούν να τύχουν επεξεργασίας από μη εξουσιοδοτημένο τρίτο, δεν απαιτείται γνωστοποίηση στην ΑΠΔΠΧ.
Η εν λόγω υποχρέωση επιβαρύνει σημαντικά τον Υπεύθυνο Επεξεργασίας, ο οποίος θα έχει χρονικούς περιορισμούς προκειμένου να εκτιμήσει την σοβαρότητα και το εύρος της παραβίασης. Σε ορισμένες περιπτώσεις, οι υπεύθυνοι επεξεργασίας δεδομένων ενδέχεται να δεσμεύονται να ενημερώσουν τα υποκείμενα των δεδομένων σχετικά με μια τέτοια παραβίαση.
Η παράλειψη γνωστοποίησης παραβίασης, όταν απαιτείται, μπορεί να οδηγήσει σε πρόστιμο.

22 Οδηγίες Απαιτούμενων Ενεργειών Σωματείων
Κάθε σωματείο θα πρέπει κατ' ελάχιστο να:
1. Να τηρεί Αρχείο Επεξεργασίας για τα προσωπικά δεδομένα αθλητών που συλλέγει και επεξεργάζεται.
2. Να διαθέτει έντυπο ενημέρωσης επεξεργασίας δεδομένων αθλητών και να λαμβάνει συναίνεση των αθλητών του εάν πρόκειται να κάνει χρήση δεδομένων και για άλλους σκοπούς
3. Να αναγνωρίζει και να σέβεται τα δικαιώματα των Αθλητών:
a. Δικαίωμα πρόσβασης στα δεδομένα του: Το δικαίωμα να γνωρίζει αν τα δεδομένα του υφίστανται επεξεργασία, πώς και για ποιο σκοπό.
b. Δικαίωμα διόρθωσης των δεδομένων του: Το δικαίωμα να ζητήσει διόρθωση των προσωπικών του δεδομένων αν αυτά είναι ανακριβή ή ελλιπή.
c. Δικαίωμα διαγραφής των δεδομένων του: Το δικαίωμα να ζητήσει διαγραφή ή κατάργηση των προσωπικών του δεδομένων υπό ορισμένες προϋποθέσεις.
d. Δικαίωμα περιορισμού της επεξεργασίας των δεδομένων του: Το δικαίωμα να ζητάει τον περιορισμό της επεξεργασίας των προσωπικών του δεδομένων όταν συντρέχουν ορισμένες προϋποθέσεις.
e. Δικαίωμα στη φορητότητα των δεδομένων του: Το δικαίωμα του αθλητή να ζητήσει να αποσταλούν τα στοιχεία του σε τρίτο

4. Όταν ένας αθλητής υποβάλλει ένα αίτημα ασκώντας κάποιο από τα παραπάνω δικαιώματα, το σωματείο οφείλει να απαντήσει εντός 1 μηνός είτε ικανοποιώντας το δικαίωμα (π.χ. δίνοντας στον αθλητή αντίγραφο των ζητηθέντων δεδομένων) είτε απορρίπτοντας αιτιολογημένα το αίτημα (π.χ. αρνούμενος αίτημα διαγραφής, λόγω του ότι ο νόμος υποχρεώνει το σωματείο να το διατηρήσει για Χ χρόνια) είτε εξηγώντας τους λόγους

καθυστέρησης. Σε περίπτωση καθυστέρησης οφείλει πάντως να απαντήσει θετικά ή αρνητικά εντός 3 μηνών από το αίτημα.
5. Να εφαρμόζει τεχνικά μέτρα ασφαλείας:

a. Να χρησιμοποιεί ισχυρό - δύσκολο password (π.χ. όχι «1234») για την είσοδο στα συστήματα και στις εφαρμογές και ανά τακτά χρονικά διαστήματα αλλαγή τους.
b. Απενεργοποίηση λειτουργίας μέσων αποθήκευσης (π.χ. USB) όπου αυτή δεν χρειάζεται (π.χ. PC γραμματείας).
c. Χρήση μοντέρνων λειτουργικών συστημάτων υπολογιστή και συνεχόμενη ενημέρωσή τους.
d. Χρήση λογισμικού προστασίας από κακόβουλο λογισμικό (antivirus).
e. Ενεργοποίηση Τείχους Προστασίας (Firewall) στον υπολογιστή.
f. Αποφυγή χρήσης λογισμικού ελεύθερης χρήσης (free download).
g. Αποφυγή χρήσης και παραχώρησης προνομιακών δικαιωμάτων πρόσβασης στον απλό χρήστη (δικαιώματα Local Administrator).
h. Λήψη αντιγράφων ασφάλειας σε τακτά χρονικά διαστήματα.
i. Αποφυγή χρήσης ελευθέρων e-mail, π.χ. Yahoo, για αποστολή και λήψη ευαίσθητων δεδομένων, π.χ. ιατρικών εξετάσεων.
j. Κρυπτογράφηση τοπικού δίσκου υπολογιστή μέσω του λειτουργικού συστήματος.
k. Κρυπτογράφηση εξωτερικών μονάδων αποθήκευσης (π.χ. εξωτερικός σκληρός δίσκος, USB κ.ο.κ.).

*ΠΡΟΣΟΧΗ: Τα παραπάνω είναι οι ελάχιστες υποχρεώσεις κάθε σωματείου. Σας συμβουλεύουμε να εξετάσετε τα ανωτέρω ως ενδεικτικά μέτρα, καθώς και να λάβετε υπ’ όψιν ότι έχει μεγάλη σημασία και η σωστή εφαρμογή τους. Ενδεικτικά, η χρήση ισχυρού password αποτελεί ενδεδειγμένο μέτρο, αλλά εάν το password δεν φυλάσσεται σωστά και βρίσκεται σημειωμένο δίπλα στον υπολογιστή ή σε σημείο εύκολα προσβάσιμο, δεν προσφέρει κάποια πρόσθετη εξασφάλιση.

Πηγές:

1. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr)
2. Ιατρικός Σύλλογος Αθηνών (www.isathens.gr)