ΠΡΟΣ ΕΝΗΜΕΡΩΣΗ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ ΤΟΥ ΦΟΡΕΑ καθώς και κάθε τρίτου.

Σύμφωνα με την υπ΄αρ. 9/22 Απόφαση του Δ.Σ. μέχρι σήμερα έχει οριστεί ΥΠΔ του φορέα μας ο κος Μιχαήλ Ασημαντώνης. Προς διευκόλυνσή σας σας αποστέλλονται κατευθυντήριες γραμμές για τη τήρηση των βασικών κανόνων προστασίας των προσωπικών δεδομένων σε οποιαδήποτε περίπτωση δημοσιοποίησης και επεξεργασίας αυτών είτε στον δημόσιο είτε στον ιδιωτικό τομέα δράσης μας ως υπαλλήλων- συντελεστών πρόσβασης σε τέτοιας φύσεως δεδομένα αυτοματοποιημένα ή μη.

Οι παρούσες οδηγίες έχουν διατυπωθεί σε τρίτο πρόσωπο καθώς οποιαδήποτε μέτρα προστασίας , αποδοχής ή απαγόρευσης επί της επικείμενης επεξεργασίας των προσωπικών δεδομένων θα πρέπει να λαμβάνεται από μέρους σας σε συνεννόηση, όπου απαιτείται, με τον ΥΠΔ.

Όποια αμφιβολία ή αντίρρηση εγερθεί επί των θεμάτων αυτών παρακαλώ να τίθεται υπόψη του ΥΠΔ προς επίλυση. (εσωτ. 129).

<u>Προστασία δεδομένων στο πλαίσιο του ΓΚΠΔ</u>

Ο ΓΚΠΔ καθορίζει λεπτομερώς τις απαιτήσεις για τη συλλογή, την αποθήκευση και τη διαχείριση προσωπικών δεδομένων από επιχειρήσεις και οργανισμούς. Οι απαιτήσεις ισχύουν για ευρωπαϊκούς οργανισμούς που επεξεργάζονται προσωπικά δεδομένα ατόμων στην ΕΕ, αλλά και για οργανισμούς εκτός της ΕΕ οι οποίοι στοχεύουν άτομα που ζουν στην ΕΕ.

Πότε εφαρμόζεται ο γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ);

Ο ΓΚΠΔ εφαρμόζεται εάν:

- η επιχείρηση ή φορέας του Δημοσίου τομέα επεξεργάζεται προσωπικά δεδομένα και εδρεύει στην ΕΕ, ανεξάρτητα από το πού γίνεται η πραγματική επεξεργασία των δεδομένων
- η επιχείρησή ή ο φορέας εδρεύει εκτός της ΕΕ αλλά επεξεργάζεται προσωπικά δεδομένα τα οποία αφορούν την παροχή προϊόντων ή υπηρεσιών σε άτομα εντός της ΕΕ, ή παρακολουθεί τη συμπεριφορά ατόμων εντός της ΕΕ

Επιχειρήσεις ή φορείς που δεν εδρεύουν στην ΕΕ αλλά επεξεργάζονται δεδομένα πολιτών της ΕΕ οφείλουν να διορίζουν εκπρόσωπο στην ΕΕ.

Πότε δεν εφαρμόζεται ο γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ);

Ο ΓΚΠΔ δεν εφαρμόζεται εάν:

- το υποκείμενο των δεδομένων είναι νεκρό
- το υποκείμενο των δεδομένων είναι νομικό πρόσωπο

ΔΗΛΑΔΗ οι κανόνες ισχύουν μόνο για τα δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων, δεν διέπουν τα δεδομένα που αφορούν εταιρείες ή άλλες νομικές οντότητες. Ωστόσο, πληροφορίες που σχετίζονται με μονοπρόσωπες εταιρείες μπορεί να αποτελούν δεδομένα προσωπικού χαρακτήρα όταν καθιστούν δυνατή την ταυτοποίηση ενός φυσικού προσώπου. Οι κανόνες ισχύουν επίσης για όλα τα δεδομένα προσωπικού χαρακτήρα που σχετίζονται με φυσικά πρόσωπα κατά τη διάρκεια επαγγελματικής δραστηριότητας, όπως είναι, π.χ., οι εργαζόμενοι μιας εταιρείας/ενός οργανισμού, οι διευθύνσεις ηλεκτρονικού ταχυδρομείου επιχείρησης του τύπου «όνομα.επώνυμο@εταιρεία.eu» ή οι επαγγελματικοί αριθμοί τηλεφώνου εργαζομένων.

- η επεξεργασία γίνεται από πρόσωπο που ενεργεί για σκοπούς εκτός του εμπορικού, επιχειρηματικού ή επαγγελματικού του πεδίου ή των σκοπών στους οποίους αποβλέπουν στο Δημόσιο Τομέα.

Κάθε δημόσια διοίκηση υπόκειται στους κανόνες του ΓΚΠΔ όταν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που αφορούν φυσικό πρόσωπο. Οι εθνικές αρχές είναι υπεύθυνες για την υποστήριξη των περιφερειακών και τοπικών αρχών κατά την προετοιμασία τους για την εφαρμογή του ΓΚΠΔ.

Η πλειονότητα των δεδομένων προσωπικού χαρακτήρα που τηρούνται από δημόσιες διοικήσεις συνήθως τίθενται σε επεξεργασία με βάση μια νομική υποχρέωση ή στον βαθμό που τούτο είναι απαραίτητο για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί σε αυτές.Κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, κάθε δημόσια διοίκηση οφείλει να τηρεί ορισμένες βασικές αρχές, στις οποίες περιλαμβάνονται οι εξής:

- δίκαιη και νόμιμη επεξεργασία·
- περιορισμός σκοπού·
- ελαχιστοποίηση δεδομένων και διατήρηση δεδομένων.

Σε περίπτωση επεξεργασίας με βάση το δίκαιο, το εν λόγω δίκαιο θα πρέπει ήδη να διασφαλίζει ότι αυτές οι αρχές τηρούνται (π.χ. είδη δεδομένων, περίοδος αποθήκευσης και κατάλληλες εγγυήσεις).

Πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρέπει να ενημερώνονται τα φυσικά πρόσωπα σχετικά με την επεξεργασία, π.χ. για τους σκοπούς της, τα είδη δεδομένων που συλλέγονται, τους αποδέκτες, καθώς και για τα δικαιώματά τους όσον αφορά την προστασία των δεδομένων.

Κάθε δημόσια διοίκηση πρέπει να διορίσει έναν υπεύθυνο προστασίας δεδομένων (ΥΠΔ), Πρέπει να διασφαλίζει ότι έχει εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα τα οποία καθιστούν ασφαλή τα δεδομένα προσωπικού χαρακτήρα. Σε περίπτωση εξωτερικής ανάθεσης μέρους της επεξεργασίας σε οργανισμό (που αποκαλείται «εκτελών την επεξεργασία»), πρέπει να υφίσταται σύμβαση ή άλλη νομική πράξη που να εγγυάται ότι ο εκτελών την επεξεργασία παρέχει επαρκείς

εγγυήσεις για την υλοποίηση κατάλληλων τεχνικών και οργανωτικών μέτρων που να ανταποκρίνονται στα πρότυπα του ΓΚΠΔ.

Σε περίπτωση που δεδομένα προσωπικού χαρακτήρα που κατέχει μια δημόσια διοίκηση κοινολογηθούν τυχαία ή παράνομα σε μη εξουσιοδοτημένους αποδέκτες ή είναι προσωρινά μη διαθέσιμα ή έχουν αλλοιωθεί, πρέπει να ειδοποιηθεί η αρχή προστασίας δεδομένων (ΑΠΔ) σχετικά με την παραβίαση χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 72 ωρών από τη στιγμή που διαπιστώνεται η παραβίαση. Επίσης, ενδέχεται να πρέπει η δημόσια διοίκηση να ενημερώσει τα άτομα σχετικά με την παραβίαση

Τι είναι τα προσωπικά δεδομένα;

Προσωπικά δεδομένα είναι όλες οι πληροφορίες που αφορούν έναν ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο, το οποίο καλείται υποκείμενο των δεδομένων. Τα προσωπικά δεδομένα περιέχουν πληροφορίες όπως:

- όνομα
- διεύθυνση
- αριθμός δελτίου ταυτότητας/διαβατηρίου
- εισόδημα
- πολιτισμικό προφίλ
- κωδικός πρωτοκόλλου διαδικτύου (IP)
- δεδομένα που διατηρούν νοσοκομεία ή γιατροί (με αποκλειστικό σκοπό την ταυτοποίηση προσώπου για ιατρικούς λόγους).

Ειδικές κατηγορίες δεδομένων

Δεν επιτρέπεται η επεξεργασία προσωπικών δεδομένων σχετικά με τα εξής χαρακτηριστικά ενός προσώπου:

- φυλετική ή εθνοτική καταγωγή
- σεξουαλικός προσανατολισμός
- πολιτικά φρονήματα
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- συμμετοχή σε συνδικαλιστικές οργανώσεις
- γενετικά ή βιομετρικά δεδομένα και δεδομένα υγείας, εξαιρουμένων ειδικών περιπτώσεων (π.χ. όταν έχετε δώσει την πλήρη συγκατάθεσή σας ή όταν η επεξεργασία απαιτείται για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει της νομοθεσίας της ΕΕ ή της εθνικής νομοθεσίας)

- *<u>ΣΗΜΕΙΩΤΕΟΝ ότι :</u>*"δεδομένα προσωπικού χαρακτήρα είναι κάθε είδους πληροφορίες που αναφέρονται στο υποκείμενο των δεδομένων ", β).., γ).., δ) "επεξεργασία κάθε εργασία ή σειρά εργασιών που πραγματοποιείται από το

Δημόσιο ή από νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση, η αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή", ε) (όπως ήδη αντικαταστάθηκε το εδάφιο αυτό με την παρ. 2 του άρθρου 18 του ν. 3471/2006) "αρχείο δεδομένων προσωπικού χαρακτήρα ("αρχείο") κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια", στ)..., ζ) "υπεύθυνος επεξεργασίας οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, η) ..., θ) ..., ι) "αποδέκτης το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν είναι τρίτος ή όχι".... Εξ ετέρου, κατά τη διάταξη του άρθρου 3 παρ. 1 του ανωτέρω νόμου, οι διατάξεις του παρόντος νόμου εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία, καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν στο αρχείο.(ΑΠ 76/2020)

- προσωπικά δεδομένα που σχετίζονται με ποινικές καταδίκες και αδικήματα, εκτός αν αυτό επιτρέπεται από τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία

Ποιος επεξεργάζεται τα προσωπικά δεδομένα;

Κατά την επεξεργασία τους, τα προσωπικά δεδομένα μπορεί να περάσουν από διάφορες επιχειρήσεις ή οργανισμούς. Μέσα σ΄αυτόν τον κύκλο, υπάρχουν δύο βασικά προφίλ που ασχολούνται με την επεξεργασία των προσωπικών δεδομένων:

- ο υπεύθυνος επεξεργασίας, οποίος αποφασίζει τον σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων
- ο εκτελών την επεξεργασία, ο οποίος φυλάσσει και επεξεργάζεται τα δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας.

Ποιος παρακολουθεί μέσα στην επιχείρηση τον τρόπο επεξεργασίας των προσωπικών δεδομένων;

Ο υπεύθυνος προστασίας δεδομένων (ΥΠΔ) που μπορεί να έχει οριστεί από την επιχείρηση/φορέα, είναι αρμόδιος να παρακολουθεί την επεξεργασία των προσωπικών δεδομένων, καθώς και να ενημερώνει και να συμβουλεύει τους υπαλλήλους επεξεργασίας των προσωπικών δεδομένων σχετικά με τις υποχρεώσεις τους. Ο ΥΠΔ συνεργάζεται επίσης με την Αρχή Προστασίας Δεδομένων (ΑΠΔ), λειτουργώντας ως σημείο επαφής μεταξύ της ΑΠΔ και μεμονωμένων ατόμων.

Πότε πρέπει να ορίζεται έναν υπεύθυνο προστασίας δεδομένων;

Οφείλεται να οριστεί ένας ΥΠΔ εάν η επιχείρηση/φορέας:

- παρακολουθεί άτομα, σε τακτική ή συστηματική βάση, ή επεξεργάζεται ειδικές κατηγορίες δεδομένων
- έχει ως μία από τις κύριες επιχειρηματικές/κρατικές της δραστηριότητες την επεξεργασία δεδομένων
- επεξεργάζεται δεδομένα σε ευρεία κλίμακα.

Για παράδειγμα, αν επεξεργάζεστε προσωπικά δεδομένα για να στοχοθετήσετε διαφημίσεις μέσω μηχανών αναζήτησης βάσει της συμπεριφοράς των ατόμων στο διαδίκτυο, οφείλετε να ορίσετε έναν ΥΠΔ. Αν, αντίθετα, στέλνετε στους πελάτες σας διαφημιστικό υλικό μόνο μία φορά τον χρόνο, δεν χρειάζεται να ορίσετε ΥΠΔ.

Ο/Η ΥΠΔ μπορεί να προέρχεται από το προσωπικό του οργανισμού/φορέα ή να είναι εξωτερικός συνεργάτης βάσει σύμβασης παροχής υπηρεσιών. Ο ΥΠΔ μπορεί να είναι μεμονωμένο άτομο ή μέρος οργανισμού.

Επεξεργασία δεδομένων για άλλη επιχείρηση

Ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να αναθέσει την επεξεργασία δεδομένων μόνο σε άτομο που παρέχει επαρκείς εγγυήσεις, οι οποίες θα πρέπει να περιλαμβάνονται σε γραπτή σύμβαση μεταξύ των ενδιαφερόμενων μερών. Η σύμβαση αυτή πρέπει επίσης να περιέχει ορισμένες υποχρεωτικές ρήτρες, π.χ., ότι ο εκτελών την επεξεργασία θα επεξεργάζεται προσωπικά δεδομένα μόνον όταν του δίδεται σχετική εντολή από τον υπεύθυνο επεξεργασίας δεδομένων.

Μεταφορά δεδομένων εκτός της ΕΕ

Όταν προσωπικά δεδομένα μεταφέρονται εκτός της ΕΕ, η προστασία που παρέχει ο ΓΚΠΔ εξακολουθεί να ισχύει για τα εν λόγω δεδομένα. Αυτό σημαίνει ότι αν εξάγετε δεδομένα στο εξωτερικό, η επιχείρηση/φορέας πρέπει να διασφαλίζει ότι τηρείται ένα από τα παρακάτω μέτρα:

- η χώρα εκτός της ΕΕ εφαρμόζει κανόνες που κρίνονται επαρκείς από την ΕΕ
- η επιχείρηση/φορέας λαμβάνει τα αναγκαία μέτρα για να παράσχει τις κατάλληλες διασφαλίσεις, όπως να περιλάβει συγκεκριμένες ρήτρες στη συμφωνηθείσα σύμβαση με τον εκτός της ΕΕ εισαγωγέα προσωπικών δεδομένων
- η επιχείρηση/φορέας βασίζεται σε συγκεκριμένα επιχειρήματα για την μεταφορά (παρεκκλίσεις), όπως η συγκατάθεση του υποκειμένου των δεδομένων.

Πότε επιτρέπεται η επεξεργασία δεδομένων;

Σύμφωνα με τους κανόνες της ΕΕ για την προστασία δεδομένων, η επεξεργασία πρέπει να γίνεται με θεμιτό και σύννομο τρόπο, για έναν συγκεκριμένο και νόμιμο σκοπό και να καλύπτει μόνο τα δεδομένα που είναι αναγκαία για την επίτευξη αυτού του σκοπού. Για να επεξεργάζεστε προσωπικά δεδομένα πρέπει να διασφαλίσετε ότι πληροίτε έναν από τους παρακάτω όρους :

- έχετε τη συγκατάθεση του συγκεκριμένου υποκειμένου των δεδομένων
- χρειάζεστε τα προσωπικά δεδομένα για να τηρήσετε συμβατική υποχρέωση έναντι του υποκειμένου των δεδομένων
- χρειάζεστε τα προσωπικά δεδομένα για να εκπληρώσετε νομική υποχρέωση
- χρειάζεστε τα προσωπικά δεδομένα για να προστατεύσετε ζωτικά συμφέροντα του υποκειμένου των δεδομένων
- επεξεργάζεστε προσωπικά δεδομένα για να διεκπεραιώσετε αποστολή δημοσίου συμφέροντος
- ενεργείτε προς όφελος των νομίμων συμφερόντων της επιχείρησης/φοοέα, εφόσον δεν θίγονται σοβαρά τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επεξεργάζεστε. Αν τα δικαιώματα του υποκειμένου υπερισχύουν των συμφερόντων της επιχείρησης/φορέα, δεν μπορείτε να επεξεργαστείτε τα προσωπικά του δεδομένα.

Συγκατάθεση για την επεξεργασία δεδομένων

Ο ΓΚΠΔ ορίζει αυστηρούς κανόνες για την επεξεργασία δεδομένων βάσει συγκατάθεσης. Σκοπός των κανόνων αυτών είναι να διασφαλιστεί ότι το υποκείμενο των δεδομένων κατανοεί για τι πραγματικά έχει δώσει τη συγκατάθεσή του. Αυτό σημαίνει ότι η συγκατάθεση πρέπει να δίνεται ελεύθερα, συγκεκριμένα και χωρίς ασάφειες με δήλωση διατυπωμένη σε απλή και κατανοητή γλώσσα. Η συγκατάθεση πρέπει να δίνεται με καταφατική πράξη, π.χ. με την επιλογή τετραγωνιδίου σε ιστοσελίδα ή με την υπογραφή δήλωσης.

Όταν έχει δοθεί συγκατάθεση για την επεξεργασία προσωπικών δεδομένων, μπορείτε να επεξεργαστείτε τα δεδομένα μόνο για τους σκοπούς για τους οποίους δόθηκε η συγκατάθεση. Πρέπει επίσης να δίνετε στο υποκείμενο των δεδομένων τη δυνατότητα να αποσύρει τη συγκατάθεσή του.

Παροχή διαφανών πληροφοριών

Πρέπει να παρέχετε στα υποκείμενα των δεδομένων σαφείς πληροφορίες σχετικά με το ποιος επεξεργάζεται τα προσωπικά τους δεδομένα και γιατί. Οφείλετε να παρέχετε τουλάχιστον τις παρακάτω πληροφορίες:

- ποιος είστε
- γιατί επεξεργάζεστε τα προσωπικά δεδομένα
- ποια είναι η νομική βάση
- ποιος θα λάβει τα δεδομένα (αν υπάρχει).

Σε ορισμένες περιπτώσεις, πρέπει επίσης να δίνονται οι παρακάτω πληροφορίες:

- ποια είναι τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων (ΥΠΔ), εφόσον υπάρχει,
- ποιο νόμιμο συμφέρον επιδιώκει η επιχείρηση/φορέας, όταν για την επεξεργασία βασίζεστε σε αυτό το νομικό επιχείρημα
- ποια μέτρα ισχύουν για τη μεταφορά δεδομένων σε μια χώρα εκτός της ΕΕ

- για πόσο διάστημα αποθηκεύονται τα δεδομένα
- ποια είναι τα δικαιώματα του υποκειμένου των δεδομένων σχετικά με την προστασία των δεδομένων του (π.χ. δικαίωμα πρόσβασης, διόρθωσης, διαγραφής, περιορισμού, απαγόρευσης της χρήσης, φορητότητας, κ.λπ).
- πώς μπορεί να αποσυρθεί η συγκατάθεση (όταν αυτή είναι το νομικό επιχείρημα για την επεξεργασία)
- αν υπάρχει καταστατική ή συμβατική υποχρέωση για την παροχή των δεδομένων
- ποιο είναι το σκεπτικό, η σημασία και οι επιπτώσεις της απόφασης, στην περίπτωση αυτοματοποιημένης λήψης απόφασης.

Πρέπει να δίνετε αυτές τις πληροφορίες σε σαφή και κατανοητή γλώσσα.

Ειδικοί κανόνες για τα παιδιά

Αν συλλέγετε προσωπικά δεδομένα από παιδί βάσει συγκατάθεσης, για παράδειγμα από λογαριασμό μέσων κοινωνικής δικτύωσης ή λογαριασμό τηλεφόρτωσης, οφείλετε να λάβετε πρώτα γονική συγκατάθεση, π.χ. στέλνοντας ειδοποίηση στον γονέα ή στον κηδεμόνα του παιδιού. Η ηλικία μέχρι την οποία ένα πρόσωπο θεωρείται παιδί διαφέρει ανάλογα με τη χώρα κατοικίας, αλλά συνήθως είναι μεταξύ 13 και 16 ετών.

Δικαίωμα πρόσβασης και δικαίωμα φορητότητας των δεδομένων

Πρέπει να διασφαλίζετε ότι τα υποκείμενα των δεδομένων έχουν το δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα, δωρεάν. Αν λάβετε σχετικό αίτημα, οφείλετε:

- να ενημερώσετε το υποκείμενο των δεδομένων αν επεξεργάζεστε τα προσωπικά του δεδομένα ή όχι
- να του δώσετε πληροφορίες για την επεξεργασία (σκοπός, κατηγορίες προσωπικών δεδομένων που υπόκεινται σε επεξεργασία, αποδέκτες των δεδομένων, κλπ.)
- να του δώσετε αντίγραφο των προσωπικών του δεδομένων που επεξεργάζεστε (σε προσβάσιμο μορφότυπο)

Όταν η επεξεργασία βασίζεται σε συγκατάθεση ή σε σύμβαση, το υποκείμενο των δεδομένων μπορεί επίσης να σας ζητήσει να του επιστρέψετε τα προσωπικά του δεδομένα ή να τα διαβιβάσετε σε άλλη επιχείρηση. Πρόκειται για το γνωστό ως δικαίωμα φορητότητας των δεδομένων. Πρέπει να παρέχετε τα δεδομένα σε έναν ευρέως χρησιμοποιούμενο και μηχαναγνώσιμο μορφότυπο.

Δικαίωμα διόρθωσης και δικαίωμα προβολής αντιρρήσεων

Αν ένα υποκείμενο δεδομένων πιστεύει ότι τα προσωπικά του δεδομένα είναι εσφαλμένα, ελλιπή ή ανακριβή, έχει το δικαίωμα να ζητήσει τη διόρθωση ή τη συμπλήρωσή τους χωρίς καμία καθυστέρηση.

Στην περίπτωση αυτή, οφείλετε να ενημερώσετε όλους τους παραλήπτες των προσωπικών δεδομένων ότι κάποια από τα προσωπικά δεδομένα που τους κοινοποιήσατε έχουν μεταβληθεί ή διαγραφεί. Αν διαβιβάσατε εσφαλμένα προσωπικά δεδομένα, οφείλετε, ενδεχομένως, να ενημερώσετε σχετικά οποιονδήποτε τα είδε (εκτός αν αυτό προϋποθέτει δυσανάλογες προσπάθειες).

Το υποκείμενο των δεδομένων μπορεί επίσης να αντιταχθεί - ανά πάσα στιγμή - στην επεξεργασία των προσωπικών του δεδομένων για μια συγκεκριμένη χρήση, όταν η επιχείρηση/φορέας τα επεξεργάζεται βάσει του νόμιμου συμφέροντός της, ή για λόγους δημοσίου συμφέροντος. Στην περίπτωση αυτή οφείλετε να διακόψετε την επεξεργασία των προσωπικών δεδομένων, εκτός αν έχετε νόμιμο συμφέρον που υπερισχύει των συμφερόντων του υποκειμένου των δεδομένων.

Ομοίως, το υποκείμενο των δεδομένων μπορεί να ζητήσει την περιορισμένη επεξεργασία των προσωπικών του δεδομένων εφόσον έχει οριστεί κατά πόσον το νόμιμο συμφέρον σας υπερισχύει των δικών του συμφερόντων. Ωστόσο, σε περίπτωση άμεσης εμπορικής προώθησης, υποχρεούστε πάντα να διακόψετε την επεξεργασία των προσωπικών δεδομένων εφόσον το ζητήσει το υποκείμενο των δεδομένων.

Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

Σε ορισμένες περιπτώσεις, το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας να διαγράψει τα προσωπικά του δεδομένα, π.χ. όταν τα δεδομένα αυτά δεν χρειάζονται πλέον για την επίτευξη του σκοπού της επεξεργασίας. Ωστόσο, η επιχείρηση/φορέας δεν υποχρεούται να πράξει κάτι τέτοιο, εφόσον:

- η επεξεργασία είναι απαραίτητη προκειμένου να τηρηθεί η ελευθερία της έκφρασης και της πληροφόρησης
- οφείλετε να αποθηκεύσετε τα προσωπικά δεδομένα προκειμένου να συμμορφωθείτε με νομική υποχρέωση
- υπάρχουν άλλοι λόγοι δημόσιου συμφέροντος για την αποθήκευση των προσωπικών δεδομένων, όπως σκοποί δημόσιας υγείας ή επιστημονικής και ιστορικής έρευνας
- οφείλετε να αποθηκεύσετε τα προσωπικά δεδομένα προκειμένου να εγείρετε νομική αξίωση

Εάν οι φωτογραφίες-αρχεία έχουν υποβληθεί σε επεξεργασία σε άλλους ιστότοπους, πρέπει να λάβει εύλογα μέτρα για να τους ενημερώσει ότι έχει υποβληθεί αίτημα διαγραφής των φωτογραφιών.

Αυτοματοποιημένη λήψη αποφάσεων και δημιουργία προφίλ

Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση η οποία βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία. Ωστόσο, υπάρχουν ορισμένες εξαιρέσεις από αυτόν τον κανόνα, όπως όταν το υποκείμενο των

δεδομένων έχει δώσει ρητή συγκατάθεση για απόφαση βάσει αυτοματοποιημένης επεξεργασίας. Εκτός εάν η αυτοματοποιημένη απόφαση βασίζεται σε νομοθετική πράξη, η επιχείρηση φορέας οφείλει:

- να ενημερώνει το υποκείμενο των δεδομένων για την αυτοματοποιημένη λήψη αποφάσεων
- να του παρέχει το δικαίωμα να αναθέτει την εξέταση της αυτοματοποιημένης απόφασης σε συγκεκριμένο άτομο
- να του δίνει τη δυνατότητα να αμφισβητήσει την αυτοματοποιημένη απόφαση

Για παράδειγμα, αν μία τράπεζα λάβει αυτοματοποιημένη απόφαση σχετικά με τη χορήγηση δανείου σε συγκεκριμένο άτομο, το εν λόγω άτομο πρέπει να ενημερωθεί για την αυτοματοποιημένη απόφαση και να έχει τη δυνατότητα να αμφισβητήσει την απόφαση και να ζητήσει ανθρώπινη παρέμβαση.

Παραβιάσεις δεδομένων - παροχή κατάλληλης ειδοποίησης

Παραβίαση δεδομένων έχουμε όταν τα προσωπικά δεδομένα για τα οποία είστε υπεύθυνος δημοσιοποιούνται, κατά τύχη ή παράνομα, σε μη εξουσιοδοτημένους παραλήπτες, καθίστανται προσωρινά μη διαθέσιμα ή αλλοιώνονται.

Αν συμβεί όντως παραβίαση δεδομένων και η παραβίαση θέτει σε κίνδυνο τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, οφείλετε να ειδοποιήσετε την Αρχή Προστασίας Δεδομένων εντός 72 ωρών αφότου αντιληφθείτε την παραβίαση.

Ανάλογα με το κατά πόσο η παραβίαση των δεδομένων δημιουργεί υψηλό κίνδυνο για τους θιγομένους, μπορεί να ζητηθεί από την επιχείρηση/φορέα να τους ενημερώσει.

Διεκπεραίωση αιτήσεων

Αν η επιχείρηση/φορέας λάβει αίτηση από υποκείμενο δεδομένων που επιθυμεί να ασκήσει τα δικαιώματά του, οφείλετε να απαντήσετε χωρίς καθυστέρηση και οπωσδήποτε εντός 1 μηνός από τη λήψη της αίτησης. Ο χρόνος της απάντησής σας μπορεί να παραταθεί κατά 2 μήνες για πολύπλοκα ή πολλαπλά αιτήματα, εφόσον το υποκείμενο των δεδομένων ενημερωθεί για την παράταση. Η διεκπεραίωση των αιτήσεων γίνεται δωρεάν.

Αν μία αίτηση απορριφθεί, πρέπει να ενημερώσετε το υποκείμενο των δεδομένων για τους λόγους της απόρριψης καθώς και για το δικαίωμά του να υποβάλει καταγγελία στην Αρχή Προστασίας Δεδομένων.

Εκτίμηση επιπτώσεων

Η διενέργεια εκτίμησης επιπτώσεων σχετικά με την προστασία δεδομένων (DPIA) είναι υποχρεωτική όταν η επικείμενη επεξεργασία θέτει σε μεγάλο κίνδυνο τα

δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, π.χ. κατά τη χρήση νέων τεχνολογιών.

Τέτοιος μεγάλος κίνδυνος προκύπτει όταν:

- χρησιμοποιούνται, κατά την αξιολόγηση ατόμων, αυτοματοποιημένοι μηχανισμοί επεξεργασίας δεδομένων και δημιουργίας προφίλ
- παρακολουθείται δημόσιος χώρος σε μεγάλη έκταση (π.χ. κάμερες CCTV)
- γίνεται επεξεργασία, σε μεγάλη κλίμακα, ειδικών κατηγοριών δεδομένων ή προσωπικών δεδομένων που σχετίζονται με ποινικές καταδίκες και αδικήματα (π.χ. δεδομένα υγείας)

Σημείωση: οι Αρχές Προστασίας Δεδομένων μπορούν επίσης να θεωρήσουν και άλλες κατηγορίες επεξεργασίας δεδομένων ως υψηλού κινδύνου.

Αν τα μέτρα που ορίζονται στην DPIA αδυνατούν να εξαλείψουν όλους τους εντοπισμένους υψηλούς κινδύνους, πρέπει να ζητηθεί η γνώμη της Αρχής Προστασίας Δεδομένων προτού πραγματοποιηθεί η σχεδιαζόμενη επεξεργασία δεδομένων.

Τήρηση αρχείων

Πρέπει να μπορείτε να αποδείξετε ότι η επιχείρηση/φορέας ενεργεί σύμφωνα με τον ΓΚΠΔ και πληροί όλες τις υποχρεώσεις της - κυρίως μετά από σχετικό αίτημα ή στο πλαίσιο επιθεώρησης από την Αρχή Προστασίας Δεδομένων.

Ένας τρόπος για να γίνει αυτό είναι να τηρείτε λεπτομερή αρχεία στοιχείων, όπως:

- το όνομα και τα στοιχεία επικοινωνίας της επιχείρησης που εμπλέκεται στην επεξεργασία δεδομένων
- τους λόγους επεξεργασίας των προσωπικών δεδομένων
- την περιγραφή των κατηγοριών των ατόμων που παρέχουν προσωπικά δεδομένα
- τις κατηγορίες των οργανισμών που είναι παραλήπτες προσωπικών δεδομένων
- τη μεταφορά προσωπικών δεδομένων σε άλλη χώρα ή οργανισμό
- την περίοδο αποθήκευσης των προσωπικών δεδομένων
- την περιγραφή των μέτρων ασφαλείας που εφαρμόζονται κατά την επεξεργασία προσωπικών δεδομένων

Επίσης, η επιχείρηση/φορέας πρέπει να τηρεί - και να επικαιροποιεί τακτικά - γραπτές διαδικασίες και οδηγίες και να τις γνωστοποιεί στο προσωπικό της.

Προειδοποίηση

Αν η επιχείρηση/φορέας είναι ΜΜΕ ή μικρότερη, δεν χρειάζεται να τηρείτε αρχεία για τις δραστηριότητες επεξεργασίας που πραγματοποιείτε, εφόσον αυτές:

- δεν γίνονται σε τακτική βάση
- δεν θίγουν τα δικαιώματα ή τις ελευθερίες των εκάστοτε προσώπων
- δεν αφορούν ευαίσθητα δεδομένα ή ποινικό μητρώο

Προστασία δεδομένων εκ σχεδιασμού και εξ ορισμού

Προστασία δεδομένων εκ σχεδιασμού σημαίνει ότι η επιχείρηση/φορέας πρέπει να λάβει υπόψη την προστασία δεδομένων στα πρώτα στάδια του σχεδιασμού ενός νέου τρόπου επεξεργασίας των προσωπικών δεδομένων. Σύμφωνα με αυτή την αρχή, ένας υπεύθυνος επεξεργασίας δεδομένων οφείλει να προβαίνει σε όλες τις τεχνικές και οργανωτικές ενέργειες που απαιτούνται για την εφαρμογή των αρχών που διέπουν την προστασία δεδομένων και την προστασία των δικαιωμάτων των υποκειμένων τους. Στις ενέργειες αυτές θα μπορούσε να περιλαμβάνεται, μεταξύ άλλων, η ψευδωνυμοποίηση.

Προστασία δεδομένων εξ ορισμού σημαίνει ότι η επιχείρηση/φορέας πρέπει πάντα να επιλέγει τις πλέον ευνοϊκές για την προστασία της ιδιωτικής ζωής ρυθμίσεις ως προεπιλεγμένες ρυθμίσεις. Για παράδειγμα, αν είναι δυνατές δύο ρυθμίσεις σχετικά με την προστασία της ιδιωτικής ζωής και μία από τις ρυθμίσεις εμποδίζει την πρόσβαση τρίτων σε προσωπικά δεδομένα, αυτή η ρύθμιση θα πρέπει να χρησιμοποιείται ως προεπιλεγμένη ρύθμιση.

Παραβίαση των κανόνων και ποινές

Η μη τήρηση των κανόνων του ΓΚΠΔ μπορεί να οδηγήσει σε σημαντικά πρόστιμα που μπορούν να φθάσουν μέχρι τα 20 εκατομμύρια ευρώ ή το 4% του συνολικού κύκλου εργασιών της επιχείρησης/φορέα για ορισμένες παραβάσεις. Η Αρχή Προστασίας Δεδομένων μπορεί επίσης να επιβάλει συμπληρωματικά διορθωτικά μέτρα, π.χ., να μας διατάξει να διακόψουμε την επεξεργασία προσωπικών δεδομένων.

Ο ΥΠΔ