ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1 Σκοπός και πεδίο εφαρμογής

Το Πανεπιστημιακό Γενικό Νοσοκομείο Ιωαννίνων, πάροχος υπηρεσιών υγείας και έδρα της εταιρείας στα Ιωάννινα (εφεξής «Νοσοκομείο») δεσμεύεται να προστατεύει τα προσωπικά δεδομένα και να αποφεύγει την κακή χρήση των προσωπικών δεδομένων.

Αυτή η πολιτική ισχύει για όλους τους υπαλλήλους, αντιπροσώπους και εργολάβους της Εταιρείας, συμπεριλαμβανομένων και των εξωτερικών συνεργατών, και δημιουργεί ένα ελάχιστο πρότυπο επεξεργασίας δεδομένων προσωπικού χαρακτήρα καθώς επίσης ορίζει εφεξής και τις αρμοδιότητές τους.

2 Περιεχόμενο

2.1 Νομική βάση

Η πολιτική αυτή είναι σύμφωνη με τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ (ΓΚΠΔ) και το Νόμο 2472/1997 (ΦΕΚ 50/Α'/10.4.1997) καθώς και οποιονδήποτε εκτελεστικό νόμο του Γενικού Κανονισμού Προστασίας Δεδομένων τεθεί σε ισχύ στην ελληνική επικράτεια- για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων, όπως τροποποιήθηκε και ισχύει, καθώς και με κάθε δευτερογενές δίκαιο / γνωμοδοτήσεις / αποφάσεις που εκδόθηκαν από την Ελληνική Αρχή Προστασίας Δεδομένων και οποιαδήποτε σχετική νομοθεσία.

2.2 Ορισμοί

Τα προσωπικά δεδομένα είναι πληροφορίες που μπορούν να σχετίζονται με ένα άτομο – φυσικό πρόσωπο. Τα δεδομένα θεωρούνται προσωπικά εάν ταυτοποιείται το πρόσωπο το οποίο αφορούν.

Ειδικές κατηγορίες δεδομένων (επίσης γνωστές ως ευαίσθητα προσωπικά δεδομένα) αφορούν:

α) Θρησκευτικές, φιλοσοφικές, πολιτικές ή συνδικαλιστικές απόψεις ή δραστηριότητες,
β) την υγεία, γενετική ή βιομετρική πληροφόρηση, το συγγενικό περιβάλλον ή τη φυλετική και εθνική καταγωγή, δεδομένα σχετικά με τη σεξουαλική ζωή ενός ατόμου ή τον σεξουαλικό προσανατολισμό
γ) ποινικές διαδικασίες και καταδίκες

Κατάρτιση προφίλ είναι μια συλλογή δεδομένων που επιτρέπει την εκτίμηση των χαρακτηριστικών ενός ατόμου και συνεπώς σημαντικών πτυχών της προσωπικότητάς του / της.

Παράδειγμα: Κατάρτιση προφίλ μπορεί να αποτελεί μια συλλογή δεδομένων, όπου συνδυάζονται διάφορες πληροφορίες, όπως οι κοινωνικές επαφές του ατόμου, οι πολιτικές και προσωπικές απόψεις, η οικονομική κατάσταση, η κατάσταση της υγείας και άλλες πληροφορίες, ώστε να προκύπτει μια ευρεία εικόνα για το υποκείμενο των δεδομένων.

Το υποκείμενο δεδομένων είναι φυσικό πρόσωπο στο οποίο αφορούν τα προσωπικά δεδομένα.

Η επεξεργασία δεδομένων είναι οποιαδήποτε δραστηριότητα που περιλαμβάνει προσωπικά δεδομένα, ανεξάρτητα από τα μέσα και τη διαδικασία που εφαρμόζεται, π.χ. η συλλογή, αποθήκευση, χρήση, αναθεώρηση, αποκάλυψη, αρχειοθέτηση, προβολή και καταστροφή προσωπικών δεδομένων.

Ως **αρχείο δεδομένων** νοείται κάθε απόθεμα προσωπικών δεδομένων που είναι διαρθρωμένο κατά τρόπο που να επιτρέπει την ταυτοποίηση του εν λόγω προσώπου από τα δεδομένα. Π.χ. οποιοδήποτε εργαλείο πληροφορικής που περιέχει προσωπικά δεδομένα.

Ως **διαβίβαση** νοείται η πρόσβαση στα προσωπικά δεδομένα, για παράδειγμα επιτρέποντας πρόσβαση, μετάδοση ή δημοσίευση.

Η εκτίμηση αντικτύπου στα προσωπικά δεδομένα είναι μια συστηματική διαδικασία για τον εντοπισμό, την αξιολόγηση και την τεκμηρίωση των κινδύνων και των επιπτώσεων των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Ο υπεύθυνος επεξεργασίας είναι το νομικό πρόσωπο που αποφασίζει για το σκοπό, το περιεχόμενο και τη διαδικασία επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Ο εκτελών την επεξεργασία είναι ένα φυσικό ή νομικό πρόσωπο που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα σύμφωνα με τις οδηγίες του υπεύθυνου επεξεργασίας δεδομένων.

2.3 Γενικές υποχρεώσεις κατά την επεξεργασία προσωπικών δεδομένων

2.3.1 Αρχές επεξεργασίας δεδομένων

Κάθε πρόσωπο που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα πρέπει να συμμορφώνεται με τις ακόλουθες αρχές.

2.3.1.1 Νόμιμη επεξεργασία

Τα προσωπικά δεδομένα μπορούν να υποβάλλονται σε επεξεργασία αποκλειστικά με νόμιμο τρόπο. Ο εκτελών την επεξεργασία πρέπει να διασφαλίζει τη συμμόρφωση με την παρούσα πολιτική και τους σχετικούς νόμους και κανονισμούς.

2.3.1.2 Συναίνεση - Συγκατάθεση

Πριν από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται και να δίνει τη συγκατάθεσή του οικειοθελώς. Η συγκατάθεση μπορεί να δίδεται ρητά ή σιωπηρά, π.χ. με την παροχή προσωπικών δεδομένων στον υπεύθυνο επεξεργασίας δεδομένων. Η συγκατάθεση δεν χρειάζεται απαραίτητα να είναι γραπτή, ωστόσο, προκειμένου να αποδεικνύεται η συναίνεση (π.χ. προς δικαστήρια και αρχές), συνιστάται γραπτή συγκατάθεση ή επιτρεπόμενη καταγραφή κλήσεων. Το υποκείμενο των δεδομένων μπορεί να αποσύρει τη συγκατάθεσή του ανά πάσα στιγμή.

Δεν απαιτείται συγκατάθεση στις ακόλουθες περιπτώσεις:

α) εάν το υποκείμενο των δεδομένων έχει γενικά καταστήσει τα προσωπικά του δεδομένα δημόσια προσβάσιμα, π.χ. πληροφορίες που δίδονται σε εφημερίδα ή τηλεφωνικούς καταλόγους, και δεν έχει απαγορεύσει την επεξεργασία τους,
β) για την εκτέλεση σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος,
γ) προκειμένου να ληφθούν μέτρα σχετικά με το αίτημα του υποκειμένου των δεδομένων πριν από τη σύναψη της σύμβασης,
δ) για τη συμμόρφωση με τις νομικές υποχρεώσεις του υπεύθυνου επεξεργασίας δεδομένων,
ε) για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
στ) εάν τα νόμιμα συμφέροντα που επιδιώκει Εταιρεία ή τρίτος υπερισχύουν των δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα, εκτός εάν τα εν λόγω συμφέροντα υπερισχύουν των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων. Σε περίπτωση αμφιβολίας, επικοινωνήστε με τον Υπεύθυνο Προστασίας Δεδομένων της Εταιρείας.

2.3.1.3 Υποχρέωση πληροφόρησης

Το υποκείμενο δεδομένων πρέπει να γνωρίζει επαρκώς τα προσωπικά δεδομένα που θα συλλεχθούν και του σκοπού της επεξεργασίας τους, πριν δώσει τη συγκατάθεσή του.

Το υποκείμενο δεδομένων πρέπει να ενημερώνεται, τουλάχιστον, σχετικά με:

α) τη ταυτότητα του υπευθύνου επεξεργασίας δεδομένων, δηλ. της Εταιρείας (στις περισσότερες περιπτώσεις),
β) τα στοιχεία επικοινωνίας του DPO,
γ) το είδος των επεξεργαζόμενων προσωπικών δεδομένων,
δ) το σκοπό της επεξεργασίας,
ε) το έννομο συμφέρον της Εταιρείας για την επεξεργασία των προσωπικών δεδομένων, κατά περίπτωση,
στ) τις κατηγορίες του παραλήπτη δεδομένων εάν έχει προγραμματιστεί αποκάλυψη,
ζ) τις λεπτομέρειες μίας σχεδιαζόμενης διασυνοριακής μεταφοράς,
η) την περίοδο διατήρησης των δεδομένων ή κριτήριων που χρησιμοποιήθηκαν για τον καθορισμό τους,
θ) εάν εφαρμόζεται αυτοματοποιημένη λήψη αποφάσεων και τη σημασία της επεξεργασίας για το υποκείμενο των δεδομένων,
ι) οδηγίες σχετικά με τα δικαιώματα του υποκειμένου των δεδομένων.

2.3.1.4 Σκοπός επεξεργασίας

Τα προσωπικά δεδομένα μπορούν να υποβάλλονται σε επεξεργασία μόνο για τον σκοπό που υποδεικνύεται κατά τη στιγμή της συλλογής, ή για το σκοπό που προβλέπεται από το νόμο. Βλέπε, επίσης, την παράγραφο 2.3.1.2 σχετικά με τη συγκατάθεση.

Η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται με καλή πίστη και τα δεδομένα που συλλέγονται ή αποθηκεύονται πρέπει να είναι απαραίτητα για την εκπλήρωση του σκοπού της επεξεργασίας τους.

Κάθε πρόσωπο που επεξεργάζεται δεδομένα είναι υπεύθυνο να διασφαλίσει ότι η επεξεργασία είναι νόμιμη και συνεπής με το σκοπό για τον οποίο συλλέχθηκαν τα δεδομένα.

2.3.1.5 Αρχεία προσωπικού

Ο φάκελος προσωπικού και τα προσωπικά δεδομένα που αφορούν τους υπαλλήλους της Εταιρείας ταξινομούνται ως «εμπιστευτικές» πληροφορίες.

Οι υπάλληλοι των εταιρειών της Εταιρείας μπορούν να ελέγξουν τον ατομικό τους φάκελο και να ζητήσουν πληροφορίες σχετικά με άλλα προσωπικά δεδομένα που τους αφορούν. Το αίτημα πληροφόρησης ή ελέγχου μπορεί να υποβληθεί προφορικά ή γραπτώς.

2.3.1.6 Ποιότητα δεδομένων

Κάθε πρόσωπο που επεξεργάζεται προσωπικά δεδομένα πρέπει να διασφαλίζει ότι τα δεδομένα είναι ορθά και πλήρη.

Η Εταιρεία πρέπει να λαμβάνει κάθε τεχνικό και οργανωτικό μέτρο προκειμένου να διασφαλίσει ότι τα προσωπικά δεδομένα, που είναι λανθασμένα ή ελλιπή, διορθώνονται ή καταστρέφονται.

2.3.1.7 *Εκτίμηση αντικτύπου στα προσωπικά δεδομένα*

Κάθε πρόσωπο που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα διεξάγει εκτίμηση αντικτύπου στα προσωπικά δεδομένα, κάθε φορά που η προγραμματισμένη δραστηριότητα επεξεργασίας μπορεί να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων.

Σκοπός της εκτίμησης του αντικτύπου είναι να αξιολογηθούν και να μετριαστούν οι κίνδυνοι για το απόρρητο των δεδομένων. Η αξιολόγηση πρέπει να διενεργείται πριν ξεκινήσουν οι εργασίες επεξεργασίας υψηλού κινδύνου.

Οι δραστηριότητες επεξεργασίας υψηλού κινδύνου περιλαμβάνουν:

α) συστηματική και εκτενή αξιολόγηση των προσωπικών στοιχείων του υποκειμένου των δεδομένων. Ειδικότερα, εάν τα προσωπικά δεδομένα υποβάλλονται αυτόματα σε επεξεργασία, εάν η επεξεργασία περιλαμβάνει τη διαμόρφωση της προσωπικότητας και εάν οι αποφάσεις που επηρεάζουν τα δικαιώματα και τις υποχρεώσεις του υποκειμένου των δεδομένων βασίζονται στην αξιολόγηση αυτή,
β) επεξεργασία ευαίσθητων προσωπικών δεδομένων σε μεγάλη κλίμακα,
γ) συστηματική και ευρείας κλίμακας παρακολούθηση μίας προσβάσιμης στο κοινό περιοχής, π.χ. παρακολούθηση με βίντεο ενός δημόσιου χώρου.

Η εκτίμηση του αντικτύπου στα προσωπικά δεδομένα πρέπει να τεκμηριώνεται δεόντως και να πραγματοποιείται με τη βοήθεια του υπευθύνου προστασίας δεδομένων. Όταν η εκτίμηση του αντικτύπου στα προσωπικά δεδομένα οδηγεί στο συμπέρασμα ότι υπάρχει υψηλός κίνδυνος για τα υποκείμενα των δεδομένων, η εποπτική αρχή πρέπει να ενημερώνεται και να γνωμοδοτεί σχετικά με τα κατάλληλα μέτρα για τη μείωση των κινδύνων.

2.3.1.8 *Διαβίβαση σε τρίτους*

Τα δεδομένα προσωπικού χαρακτήρα αποκαλύπτονται σε τρίτους μόνον εφόσον είναι απαραίτητο. Τα δεδομένα προσωπικού χαρακτήρα πρέπει να παρέχονται ανωνύμως, εφόσον κρίνεται σκόπιμο.

Τρίτος εκτελών την επεξεργασία για λογαριασμό της Εταιρείας, π.χ. ένας εργολάβος ή πάροχος υπηρεσιών, πρέπει να συμφωνήσει συμβατικά για την επεξεργασία προσωπικών δεδομένων σύμφωνα με την παρούσα πολιτική. Οι όροι αυτής της πολιτικής συμπεριλαμβάνονται με παραπομπή στις σχετικές συμβάσεις.

2.3.1.9 *Διασυνοριακή αποκάλυψη προσωπικών δεδομένων*

Τα δεδομένα προσωπικού χαρακτήρα αποκαλύπτονται στο εξωτερικό μόνο εάν ο αλλοδαπός νόμος προβλέπει επαρκές επίπεδο προστασίας των δεδομένων. Σε περίπτωση που ο αλλοδαπός νόμος δεν παρέχει επαρκές επίπεδο προστασίας δεδομένων, τα δεδομένα προσωπικού χαρακτήρα μπορούν να μεταφερθούν σε αυτή τη χώρα μόνον εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει συναινέσει ρητά στη μεταφορά ή εάν η προστασία δεδομένων προβλέπεται από την κατάλληλη συμφωνία περί μεταφοράς δεδομένων.

Η Εταιρεία θα λαμβάνει το κατάλληλο προσωπικό, τεχνικά και οργανωτικά μέτρα για την ελαχιστοποίηση του κινδύνου ακούσιας ή σκόπιμης παραβίασης, καταστροφής ή απώλειας προσωπικών δεδομένων.

Συγκεκριμένα, η Εταιρεία θα λαμβάνει διασφαλίσεις για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση και επεξεργασία. Με τον τρόπο αυτό θα ληφθούν υπόψη οι

τεχνολογικές καινοτομίες και θα καθοριστούν διαδικασίες ασφαλείας προσαρμοσμένες στις ιδιαιτερότητες της επεξεργασίας.

2.3.1.10 Αποθήκευση και διατήρηση δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα αποθηκεύονται για όσο χρόνο απαιτείται για την εκπλήρωση του σκοπού για τον οποίο συλλέχθηκαν τα δεδομένα. Τα στοιχεία της αποθήκευσης δεδομένων και των περιόδων διατήρησης καθορίζονται στην Πολιτική Διατήρησης Δεδομένων της Εταιρείας.

2.3.2 Δικαιώματα των υποκειμένων των δεδομένων

Κάθε υποκείμενο δεδομένων έχει τα ακόλουθα δικαιώματα σύμφωνα με το ΓΚΠΔ:

α) Το δικαίωμα ενημέρωσης,
β) Το δικαίωμα πρόσβασης,
γ) Το δικαίωμα διόρθωσης,
δ) Το δικαίωμα διαγραφής,
ε) Το δικαίωμα περιορισμού της επεξεργασίας,
στ) Το δικαίωμα στη φορητότητα δεδομένων,
ζ) Το δικαίωμα αντίρρησης,
η) Δικαιώματα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ.

Οι υπάλληλοι της Εταιρείας οφείλουν να σέβονται το αίτημα πρόσβασης του υποκειμένου των δεδομένων και, εφόσον απαιτείται, να ζητούν τη συμβουλή του DPO. Για περισσότερες πληροφορίες σχετικά με το περιεχόμενο κάθε δικαιώματος, ανατρέξτε στην Πολιτική της Εταιρείας για θέματα χειρισμού των αιτημάτων των υποκειμένων των δεδομένων.

2.3.3 Καταγραφή παραβίασης δεδομένων

Κάθε παράβαση αυτής της πολιτικής, των σχετικών νόμων και κανονισμών προστασίας δεδομένων συνιστά παραβίαση προσωπικών δεδομένων. Ενδεικτικά συμβάντα είναι η παράνομη καταστροφή, απώλεια, αλλοίωση, η μη εξουσιοδοτημένη αποκάλυψη, καθώς και η επεξεργασία δεδομένων χωρίς συναίνεση ή για σκοπούς άλλους από εκείνους που υποδεικνύονται τη στιγμή της συλλογής.

Το πρόσωπο που ανακαλύπτει την παραβίαση προσωπικών δεδομένων λαμβάνει τα κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων από περαιτέρω επιπτώσεις και αναφέρει την παραβίαση στον DPO χωρίς καθυστέρηση.

Ο DPO συστηματικά καταγράφει τις παραβιάσεις που του αποκαλύφθηκαν και αξιολογεί τους λόγους των παραβιάσεων. Επιπλέον, ο DPO λαμβάνει περαιτέρω απαιτούμενα μέτρα για την αποκατάσταση της κατάστασης και την αποτροπή της επανάληψης των παραβιάσεων. Για περισσότερες πληροφορίες, ανατρέξτε στην Πολιτική Διαχείρισης Παραβιάσεων Δεδομένων της Εταιρείας.

2.3.4 Ειδοποίηση για παραβίαση δεδομένων

Η Εταιρεία πρέπει να ειδοποιήσει την αρμόδια εποπτική αρχή για την παραβίαση δεδομένων εντός 72 ωρών από τη στιγμή που λαμβάνει γνώση.

Επιπλέον, εάν η παραβίαση των προσωπικών δεδομένων είναι πιθανό να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, το υποκείμενο των δεδομένων πρέπει

να ενημερώνεται χωρίς καθυστέρηση. Για περισσότερες πληροφορίες, ανατρέξτε στην Πολιτική Διαχείρισης Παραβιάσεων Δεδομένων της Εταιρείας.

2.3.5 Τεκμηρίωση των αρχείων δεδομένων

Η Εταιρεία τηρεί κατάλογο όλων των βάσεων δεδομένων και των αρχείων που περιέχουν προσωπικά δεδομένα. Ο κατάλογος περιλαμβάνει τις ακόλουθες ελάχιστες πληροφορίες:

α) το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας δεδομένων και κάθε κοινού υπεύθυνου επεξεργασίας δεδομένων,
β) όνομα και στοιχεία επικοινωνίας του DPO,
γ) περιγραφή της βάσης δεδομένων ή του αρχείου,
δ) σκοπός της βάσης δεδομένων ή του αρχείου,
ε) περιγραφή των κατηγοριών επεξεργαζόμενων προσωπικών δεδομένων, π.χ. διεύθυνση, πληροφορίες για την υγεία κ.λπ.,
στ) περιγραφή των κατηγοριών των προσώπων στα οποία αναφέρονται τα δεδομένα,
ζ) περιγραφή των κατηγοριών των αποδεκτών δεδομένων, στους οποίους έχουν διαβιβαστεί ή πρόκειται να γνωστοποιηθούν τα προσωπικά δεδομένα, συμπεριλαμβανομένων των αποδεκτών σε τρίτες χώρες,
η) περιγραφή της διασυνοριακής μεταφοράς δεδομένων,
θ) τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων, όπου είναι δυνατόν,
ι) γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας, όπου είναι δυνατόν,
κ) τις λεπτομέρειες μεταφοράς δεδομένων εκτός της ΕΕ.

Τα αρχεία δεδομένων ταξινομούνται ανάλογα με την ανάγκη προστασίας τους. Τα αρχεία δεδομένων με ειδική ανάγκη προστασίας, όπως συλλογές που περιέχουν ευαίσθητα προσωπικά δεδομένα ή προφίλ προσωπικότητας, πρέπει να καταχωρούνται σε ξεχωριστούς φακέλους, να σημειώνονται αντίστοιχα και να υπόκεινται σε εκτίμηση αντικτύπου στα προσωπικά δεδομένα, όπως ορίζεται στην παράγραφο 2.3.1.7.

2.3.6 Κατάρτιση και ευαισθητοποίηση

Κάθε υπάλληλος της Εταιρείας εκπαιδεύεται σε θέματα προστασίας δεδομένων και ασφάλειας δεδομένων. Μια πρώτη εκπαιδευτική συνεδρία θα ακολουθήσει κατά την έναρξη της απασχόλησης εντός της Εταιρείας και οι επακόλουθες εκπαιδεύσεις θα πραγματοποιούνται σε τακτά χρονικά διαστήματα.

2.4 Υποχρεώσεις για την ανάπτυξη συστημάτων και νέων επιχειρηματικών διαδικασιών

Η προστασία δεδομένων αποτελεί αναπόσπαστο μέρος της τεχνολογικής ανάπτυξης και της οργανωτικής δομής της Εταιρείας. Κατά συνέπεια, πρέπει να λαμβάνονται υπόψη οι ακόλουθες αρχές όταν αξιολογούνται οι τρέχουσες επιχειρηματικές διαδικασίες ή τα συστήματα επεξεργασίας δεδομένων ή όταν εισάγονται νέα.

2.4.1 Εκτίμηση του αντικτύπου στα προσωπικά δεδομένα αναφορικά με νέες δραστηριότητες επεξεργασίας

Η εκτίμηση του αντικτύπου στα προσωπικά δεδομένα πρέπει να διεξάγεται κάθε φορά που εισάγονται νέες τεχνολογίες ή δραστηριότητες επεξεργασίας δεδομένων οι οποίες ενδέχεται να οδηγήσουν σε επεξεργασία δεδομένων προσωπικού χαρακτήρα υψηλού κινδύνου.

Οι λεπτομέρειες της εκτίμησης του αντικτύπου στα προσωπικά δεδομένα καθορίζονται στην παράγραφο 2.3.1.7 της παρούσας πολιτικής.

2.4.2 Αρχές προστασίας των δεδομένων από τον σχεδιασμό

Όταν εισάγονται νέα συστήματα επεξεργασίας δεδομένων, ο υπεύθυνος πρέπει να εξασφαλίζει υψηλό επίπεδο προστασίας δεδομένων. Ιδιαίτερα, κάθε νέο σύστημα και διαδικασία πρέπει να συμμορφώνεται με τις ακόλουθες αρχές:

α) Πρέπει να λαμβάνονται τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της συστηματικής και ασφαλούς διαχείρισης του κύκλου ζωής των προσωπικών δεδομένων από τη συλλογή έως την επεξεργασία έως τη διαγραφή.
β) Τα συστήματα επεξεργασίας δεδομένων πρέπει να αποσκοπούν στη συλλογή όσο το δυνατόν λιγότερων προσωπικών δεδομένων για την εκπλήρωση του σκοπού για τον οποίο συλλέχθηκαν τα δεδομένα.
γ) Όταν η ανωνυμοποίηση των δεδομένων δεν παρεμποδίζει τον σκοπό της επεξεργασίας δεδομένων, τα προσωπικά δεδομένα πρέπει να καταστούν ανώνυμα κατά τρόπο που το πρόσωπο στο οποίο αναφέρονται τα δεδομένα να μη μπορεί πλέον να ταυτοποιείται.

δ) Εφόσον τα προσωπικά δεδομένα δεν μπορούν να είναι ανώνυμα, πρέπει να λαμβάνονται μέτρα ασφαλείας ανάλογα με τη φύση των δεδομένων, όπως η ψευδωνυμία, η κρυπτογράφηση ή ο περιορισμός πρόσβασης.
ε) Η πρόσβαση σε δεδομένα προσωπικού χαρακτήρα χορηγείται σύμφωνα με την αρχή «πρέπει-να-γνωρίζω», πράγμα που σημαίνει ότι τα προσωπικά δεδομένα καθίστανται προσβάσιμα μόνο σε εκείνα τα πρόσωπα που την απαιτούν για να εκτελούν καθορισμένους ρόλους και ευθύνες.
στ) Ο συστηματικός έλεγχος ποιότητας των προσωπικών δεδομένων πρέπει να αποτελεί μέρος της διαχείρισης του κύκλου ζωής των δεδομένων, ώστε να εξασφαλίζεται υψηλή ποιότητα δεδομένων. Ειδικότερα, πρέπει να δημιουργούνται διαδικασίες για την ανίχνευση και διόρθωση ψευδών ή ελλιπών προσωπικών δεδομένων.
ζ) Τα συστήματα επεξεργασίας δεδομένων πρέπει να προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση μέσω τεχνικών και οργανωτικών μέτρων.
η) Τα υποκείμενα των δεδομένων πρέπει να διαθέτουν διαφανή, φιλικά προς το χρήστη και αποτελεσματικά μέσα ελέγχου σχετικά με τα προσωπικά τους δεδομένα.

2.4.3 Αρχές προστασίας δεδομένων εξ ορισμού

Τα συστήματα επεξεργασίας δεδομένων πρέπει να ρυθμίζονται κατά τρόπον ώστε να εφαρμόζονται αυτομάτως οι αυστηρότερες ρυθμίσεις απορρήτου, δηλαδή εξ ορισμού.

Εκτενέστερη επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο εάν το υποκείμενο των δεδομένων επιλέξει ή συμφωνεί με ένα χαμηλότερο επίπεδο προστασίας, π.χ. με τη χειροκίνητη αλλαγή των ρυθμίσεων απορρήτου σε έναν ιστότοπο, ένα εργαλείο πληροφορικής ή σε κάτι παρόμοιο με μια λιγότερο περιοριστική επιλογή και συνεπώς δίνει τη ρητή συγκατάθεσή του στην εκτεταμένη επεξεργασία ("opt-in").

2.5 Αρμοδιότητες

2.5.1 Υπεύθυνος επεξεργασίας δεδομένων

Ο υπεύθυνος επεξεργασίας δεδομένων, ο οποίος αναμένεται να υπάρχει στις περισσότερες περιπτώσεις της Εταιρείας, είναι υπεύθυνος για την ορθή επεξεργασία των προσωπικών δεδομένων και την τήρηση των απαιτήσεων προστασίας δεδομένων και ασφάλειας δεδομένων όπως ορίζεται στην παρούσα πολιτική ή σύμφωνα με την ισχύουσα νομοθεσία. Συγκεκριμένα, για:

α) την τήρηση των αρχών «προστασία των δεδομένων από τον σχεδιασμό» και «προστασία των δεδομένων εξ ορισμού» κατά την ανάπτυξη νέων δραστηριοτήτων επεξεργασίας δεδομένων,
β) τη σωστή κατανομή των δικαιωμάτων των υποκειμένων των δεδομένων,
γ) διεξαγωγή εκτιμήσεων αντικτύπου για την προστασία των προσωπικών δεδομένων με τη βοήθεια του υπεύθυνου προστασίας δεδομένων,
δ) διορίζει τον εκτελούντα την επεξεργασία,
ε) την κοινοποίηση παραβίασης των προσωπικών δεδομένων στην εποπτική αρχή και στο υποκείμενο των δεδομένων (κατά περίπτωση).

2.5.2 Ο εκτελών της επεξεργασία

Ο εκτελών την επεξεργασία είναι υπεύθυνος για την επεξεργασία των προσωπικών δεδομένων σύμφωνα με τις οδηγίες που λαμβάνει από τον υπεύθυνο επεξεργασίας δεδομένων. Επιπλέον, ο εκτελών την επεξεργασία είναι υπεύθυνος να ενημερώνει χωρίς αδικαιολόγητη καθυστέρηση τον υπεύθυνο επεξεργασίας δεδομένων σχετικά με την παραβίαση της προστασίας δεδομένων.

Ο εκτελών την επεξεργασία πρέπει να επιτρέπει συμβατικά σε οποιονδήποτε ενδεχόμενο υπεργολάβο, που λαμβάνει εντολή να εκτελέσει την επεξεργασία δεδομένων, να συμμορφώνεται με τις ίδιες οδηγίες που λαμβάνει από τον υπεύθυνο επεξεργασίας δεδομένων.

2.5.3 Γραφείο Προστασίας Δεδομένων

Το Γραφείο Προστασίας Δεδομένων (DPO) είναι υπεύθυνο για το συντονισμό της προστασίας δεδομένων. Αποτελείται από εκπροσώπους του τμήματος πληροφορικής, της νομικής υπηρεσίας και των επιχειρηματικών μονάδων. Το DPO πρέπει:

α) να παρακολουθεί τη συμμόρφωση της Εταιρείας με τους ισχύοντες νόμους και κανονισμούς περί προστασίας δεδομένων,
β) να παρακολουθεί και να εφαρμόζει μελλοντικά επεξηγηματικά έγγραφα της Επιτροπής της Ευρωπαϊκής Ένωσης σχετικά με την εκτέλεση των διατάξεων του ΓΚΠΔ (GDPR),
γ) να υποστηρίζει την εκτελεστική διοίκηση για τη διασφάλιση της συμμόρφωσης με το νόμο στο πλαίσιο της προστασίας δεδομένων,
δ) να παρακολουθεί τακτικά την τήρηση της πολιτικής αυτής,
ε) να διατηρεί τον κατάλογο βάσεων δεδομένων και τον κατάλογο των παραβιάσεων της προστασίας δεδομένων,
στ) να παρακολουθεί και να βοηθά στην εκτίμηση του αντικτύπου στα προσωπικά δεδομένα,
ζ) να είναι υπεύθυνος για την απάντηση στα αιτήματα πληροφόρησης του υποκειμένου των δεδομένων,
η) να είναι υπεύθυνος για την διοργάνωση εκδηλώσεων κατάρτισης για την ευαισθητοποίηση αναφορικά με την προστασία των δεδομένων και την παροχή συμβουλών περί επεξεργασίας δεδομένων και υποχρεώσεων προσωπικού, ιδίως στους υπαλλήλους της Εταιρείας,
θ) να ενεργεί ως πρόσωπο επικοινωνίας των εποπτικών αρχών σε θέματα που σχετίζονται με την επεξεργασία προσωπικών δεδομένων, καθώς και να συνεργάζεται με τις αρχές σε οποιοδήποτε άλλο θέμα.

2.5.4 Εκτελεστική διοίκηση

Η εκτελεστική διοίκηση της Εταιρείας είναι υπεύθυνη για την εφαρμογή αυτής της πολιτικής και πρέπει να παρέχει το απαραίτητο προσωπικό και τους οικονομικούς πόρους. Οι managers της Εταιρείας υποχρεούνται να εφαρμόζουν την πολιτική στον τομέα ευθύνης τους και να διασφαλίζουν ότι οι υπάλληλοι, τα άτομα και οι οντότητες για τις οποίες είναι υπεύθυνοι γνωρίζουν, κατανοούν και τηρούν τις απαιτήσεις αυτής της πολιτικής και είναι κατάλληλα εκπαιδευμένοι να εκπληρώσουν πλήρως αυτό το καθήκον τους.

2.6 Παραβίαση της πολιτικής προστασίας δεδομένων

Οι πιθανές κυρώσεις και ζημίες που απορρέουν από την παραβίαση προστασίας δεδομένων είναι σοβαρές τόσο για το πρόσωπο που διαπράττει την παραβίαση όσο και για την Εταιρεία.

Κάθε παραβίαση αυτής της πολιτικής προστασίας δεδομένων μπορεί να οδηγήσει σε πειθαρχικές κυρώσεις έως και την απόλυση. Οι παραβιάσεις νομικών ή κανονιστικών υποχρεώσεων μπορούν να αναφέρονται σε εξωτερικές αρχές και μπορεί να έχουν ως αποτέλεσμα ποινικές, αστικές ή κανονιστικές κυρώσεις.