ΠΑΡΑΡΤΗΜΑ 17: ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

1. Βασικές έννοιες- Ορισμοί

Η προστασία των προσωπικών δεδομένων που συλλέγονται και υπόκεινται σε επεξεργασία, καθώς και η διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους σε συνεχή βάση αποτελεί βασική προτεραιότητα της Εταιρείας. Η Εταιρεία σέβεται την ιδιωτικότητα και δεσμεύεται να αντιμετωπίζει με απόλυτη προσοχή και εμπιστευτικότητα τα προσωπικά δεδομένα των εργαζομένων, πελατών, συνεργατών και λοιπών τρίτων μερών τα οποία συλλέγει και επεξεργάζεται. Εκ της φύσης της, η Εταιρεία επεξεργάζεται καθημερινά σημαντικό όγκο προσωπικών δεδομένων τόσο σε έντυπη, όσο και σε ηλεκτρονική μορφή, καθώς αυτό είναι απαραίτητο για την υποστήριξη των βασικών επιχειρηματικών της δραστηριοτήτων και για τη συμμόρφωσή της με νομικές, κανονιστικές και λοιπές υποχρεώσεις της.

Για όλους τους λόγους αυτούς, θέτει σε εφαρμογή την παρούσα Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής «η Πολιτική», «η παρούσα»).

1.1 Σκοπός & πεδίο εφαρμογής

Σκοπός της παρούσας Πολιτικής είναι να προσδιορίσει τα ελάχιστα απαιτούμενα για την επεξεργασία των προσωπικών δεδομένων και να ορίσει τις σχετικές ευθύνες.

Η παρούσα Πολιτική έχει δημιουργηθεί στα πλαίσια της συμμόρφωσης με τον Κανονισμό (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 (Γενικός Κανονισμός για την Προστασία Δεδομένων, εφεξής «ΓΚΠΔ»), τον ν. 4624/2019, τις σχετικές οδηγίες, αποφάσεις και κανονισμούς που τυχόν εκδοθούν από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) στα πλαίσια αυτού, καθώς και με οποιαδήποτε άλλη νομοθεσία ή ρυθμιστικό και κανονιστικό πλαίσιο περί Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που τροποποιούν, αναθεωρούν ή αντικαθιστούν οποιονδήποτε από τους προαναφερθέντες νόμους και κανονισμούς.

Η παρούσα πολιτική αφορά το σύνολο των εργαζομένων της Εταιρείας καθώς και των συνεργαζόμενων τρίτων μερών που εμπλέκονται στην επεξεργασία δεδομένων, στον βαθμό που οφείλουν να συμμορφώνονται με τις διαδικασίες της Εταιρείας.

1.2 Βασικοί Ορισμοί

Προσωπικά Δεδομένα	Κάθε πληροφορία που ταυτοποιεί ή μπορεί να οδηγήσει σε ταυτοποίηση φυσικού προσώπου εν ζωή. Ενδεικτικά και όχι περιοριστικά: Αναγνωριστικά στοιχεία ταυτότητας (ονοματεπώνυμο, αριθμός ταυτότητας, αριθμός πινακίδας ιδιωτικής χρήσης αυτοκινούμενου οχήματος, διεύθυνση και στοιχεία επικοινωνίας κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, επάγγελμα (προϋπηρεσία, εργασιακή συμπεριφορά κλπ.), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), οικογενειακή κατάσταση, ενδιαφέροντα, δραστηριότητες, συνήθειες.

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα προσωπικά δεδομένα)	Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές απόψεις, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή την ιδιότητα μέλους συνδικαλιστικών οργανώσεων και την επεξεργασία γενετικών δεδομένων, βιομετρικά δεδομένα με σκοπό τη μοναδική αναγνώριση φυσικού προσώπου, δεδομένα σχετικά με την υγεία ή δεδομένα που αφορούν τη ερωτική ζωή ενός φυσικού προσώπου ή το γενετήσιο προσανατολισμό καθώς και δεδομένα σχετικά με εκκρεμότητες του φυσικού προσώπου με τη δικαιοσύνη (ποινικό μητρώο).
Υπεύθυνος επεξεργασίας	Το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Για τους σκοπούς της παρούσας Υπεύθυνος επεξεργασίας είναι η Εταιρεία.
Εκτελών την επεξεργασία	Το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.
Επεξεργασία δεδομένων	Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα ανεξάρτητα από τον τρόπο με τον οποίο αυτή πραγματοποιείται, όπως συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή / μεταβολή, ανάκτηση, χρήση, διαβίβαση ή κάθε άλλη μορφή διάθεσης, συσχέτιση / συνδυασμός, περιορισμός, διαγραφή / καταστροφή.
Υποκείμενο των δεδομένων	Το φυσικό πρόσωπο το οποίο αφορούν τα προσωπικά δεδομένα.
ΓΚΠΔ	Ο Ευρωπαϊκός Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ - GDPR) 2016/679, ο οποίος τέθηκε σε εφαρμογή στις 25 Μαΐου 2018 και με τον οποίο καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ.
Υπεύθυνος Προστασίας Δεδομένων	Το πρόσωπο στο οποίο έχει ανατεθεί από την Εταιρεία η συνολική ευθύνη για την ασφάλεια και την προστασία των προσωπικών δεδομένων.
Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner)	Κάθε τμήμα της Εταιρείας που διενεργεί κάθε δραστηριότητα επεξεργασίας προσωπικών δεδομένων στα πλαίσια των αρμοδιοτήτων του, καθορίζοντας τους σκοπούς και τα μέσα της επεξεργασίας.
Παραβίαση δεδομένων προσωπικού χαρακτήρα	Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
Συγκατάθεση του Υποκειμένου των δεδομένων	Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων δηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα προσωπικά δεδομένα που το αφορούν.
Ανωνυμοποίηση	Η επεξεργασία προσωπικών δεδομένων κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων.
Ψευδωνυμοποίηση	Η επεξεργασία προσωπικών δεδομένων κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε τακτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.
Σύστημα αρχειοθέτησης	Κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.
Κατάρτιση Προσωπικού Προφίλ	Οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου. Παράδειγμα: Κατάρτιση προσωπικού προφίλ αποτελεί η συλλογή δεδομένων που περιέχουν πληροφορίες όπως κοινωνικές επαφές του υποκειμένου, πολιτικές και προσωπικές πεποιθήσεις, οικονομική επιφάνεια, κατάσταση υγείας και λοιπές πληροφορίες, οι οποίες συνδυάζονται προκειμένου να παρέχουν γενική εικόνα του υποκειμένου των δεδομένων.

1.3 Αρμοδιότητες - Ευθύνες

Α) Διοικητικό Συμβούλιο

Το Διοικητικό Συμβούλιο της Εταιρείας είναι υπεύθυνο για την έγκριση της παρούσας Πολιτικής και την εξασφάλιση και διάθεση των απαραιτήτων ανθρωπίνων και οικονομικών πόρων για την εφαρμογή της.

Β) Υπεύθυνος Προστασίας Δεδομένων

Ο Υπεύθυνος Προστασίας Δεδομένων είναι υπεύθυνος για:

- την εποπτεία τήρησης της παρούσας πολιτικής και των διαδικασιών που τη συνοδεύουν, καθώς και για την παροχή συμβουλών και καθοδήγησης σχετικά με την ορθή εφαρμογή και τήρησή της.
- την ορθή διαβάθμιση των δεδομένων.
- το συντονισμό της προστασίας των προσωπικών δεδομένων.
- τη χορήγηση έγκρισης σχετικά με τις ενέργειες που απαιτούνται για την ορθή και ασφαλή καταστροφή των δεδομένων.
- την παροχή συμβουλών και καθοδήγησης σχετικά με τις ενέργειες που απαιτούνται για την εξασφάλιση έγκυρης και έγκαιρης (πριν από την έναρξη της επεξεργασίας) λήψης συγκατάθεσης από τα υποκείμενα των δεδομένων. Για την εποπτεία των δραστηριοτήτων επεξεργασίας προκειμένου να διασφαλίζει ότι οι εν λόγω δραστηριότητες συμμορφώνονται με τις υποχρεώσεις του Υπευθύνου επεξεργασίας (Εταιρεία).
- την ανάληψη των ενεργειών που απαιτούνται ώστε να εξασφαλιστεί η ορθή και αποτελεσματική αξιολόγηση, επιλογή και διαχείριση Τρίτων Μερών από την Εταιρεία.
- την επίβλεψη και τον συντονισμό των ενεργειών που απαιτούνται για τη διαχείριση των περιστατικών παραβίασης προσωπικών δεδομένων.
- τη γνωστοποίηση της παραβίασης στην Εποπτεύουσα Αρχή, για την καταγραφή των περιστατικών παραβίασης, για την παρακολούθηση του πλάνου επίλυσης των περιστατικών παραβίασης και την πιστοποίηση της επιτυχούς ολοκλήρωσής του καθώς και για την περιοδική επανεξέταση των περιστατικών παραβίασης.
- την επίβλεψη και το συντονισμό των ενεργειών που απαιτούνται για τη διαχείριση των αιτημάτων των υποκειμένων των δεδομένων.

Γ) Τρίτα Μέρη (εκτελούντες την επεξεργασία)

Τα Τρίτα Μέρη στα οποία ανατίθεται η επεξεργασία των δεδομένων είναι υπεύθυνα για την κατανόηση και την τήρηση της παρούσας πολιτικής και των διαδικασιών που τη συνοδεύουν, διασφαλίζοντας ότι είναι σε θέση να εφαρμόσουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα έτσι ώστε η επεξεργασία να πληροί τις απαιτήσεις του ΓΚΠΔ, να διασφαλίζεται η ασφάλεια και η προστασία των προσωπικών δεδομένων και να αντιμετωπίζονται αποτελεσματικά τα περιστατικά παραβίασης.
Επιπλέον, είναι υπεύθυνα για την επεξεργασία των προσωπικών δεδομένων σύμφωνα με τις οδηγίες που λαμβάνουν από την Εταιρεία, καθώς και για τη λήψη έγκυρης και έγκαιρης (πριν την έναρξη της

επεξεργασίας) συγκατάθεσης από τα υποκείμενα των δεδομένων. Τέλος, έχουν την ευθύνη να ενημερώσουν την Εταιρεία χωρίς αδικαιολόγητη καθυστέρηση, αμέσως μόλις αντιληφθούν παραβίαση προσωπικών δεδομένων.

Δ) Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner)

Ο Υπεύθυνος Δραστηριότητας Επεξεργασίας είναι υπεύθυνος για:

- Την εκτέλεση όλων των απαιτούμενων ενεργειών σχετικά με την καταστροφή των δεδομένων υπό την εποπτεία του, προκειμένου να διασφαλιστεί ότι η καταστροφή των δεδομένων πραγματοποιείται ορθά και σύμφωνα με τα όσα ορίζονται στην παρούσα Πολιτική.
- Την εξασφάλιση της ορθής και αποτελεσματικής αξιολόγησης, επιλογής και διαχείρισης των Τρίτων Μερών στον τομέα της ευθύνης του
- Την εξασφάλιση της έγκυρης και έγκαιρης (πριν από την έναρξη της επεξεργασίας) λήψης συγκατάθεσης από τα υποκείμενα των δεδομένων στον τομέα της ευθύνης του. Επιπλέον, είναι υπεύθυνος για την τήρηση και ανανέωση σε διαρκή βάση του αρχείου συγκαταθέσεων, το οποίο θα πρέπει να καθίσταται άμεσα διαθέσιμο στον Υπεύθυνο Προστασίας Δεδομένων, κατόπιν σχετικού αιτήματος.
- Την παροχή στον Υπεύθυνο Προστασίας Δεδομένων όλης της απαιτούμενης πληροφορίας προκειμένου αυτός να είναι σε θέση να αξιολογήσει οποιοδήποτε περιστατικό παραβίασης και για την εκτέλεση των απαραίτητων ενεργειών περιορισμού και επίλυσης του περιστατικού παραβίασης.
- Την εκτέλεση των ενεργειών που απαιτούνται για τον εντοπισμό και τη συγκέντρωση των προσωπικών δεδομένων τα οποία απαιτούνται για την ικανοποίηση των αιτημάτων των υποκειμένων των δεδομένων, για κάθε δραστηριότητα επεξεργασίας υπό την εποπτεία του.

Ε) Τμήμα Μηχανογράφησης-Πληροφορικής

Το τμήμα Πληροφορικής είναι υπεύθυνο για την πραγματοποίηση όλων των απαιτούμενων ενεργειών σχετικά με την υποστήριξη καθώς και με τη διασφάλιση του απαραίτητου επιπέδου ασφάλειας κατά τη χρησιμοποίηση προσωπικών συσκευών από τους εργαζόμενους της Εταιρείας.

ΣΤ) Εργαζόμενοι

Οι εργαζόμενοι της Εταιρείας είναι υπεύθυνοι για την κατανόηση και την τήρηση της παρούσας Πολιτικής και των διαδικασιών που τη συνοδεύουν. Αναφέρουν άμεσα κάθε περιστατικό παραβίασης προσωπικών δεδομένων που υποπίπτει στην αντίληψή τους, στον Υπεύθυνο Προστασίας Δεδομένων.

2. Αρχές επεξεργασίας δεδομένων

(α) Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας.
(β) Η αρχή του περιορισμού του σκοπού.

(γ) Η αρχή της αναλογικότητας (ελαχιστοποίηση των δεδομένων).
(δ) Η αρχή της ακρίβειας των δεδομένων (ποιότητα των δεδομένων).
(ε) Η αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας (περιορισμός της περιόδου αποθήκευσης).
(στ) Η αρχή της ακεραιότητας και εμπιστευτικότητας των δεδομένων.
(ζ) Η αρχή της λογοδοσίας του υπευθύνου επεξεργασίας.

Ειδικότερα, οι αρχές επεξεργασίας προσωπικών δεδομένων αναλύονται ως ακολούθως:

2.1 Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας.

Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία με νόμιμο και διαφανή τρόπο. Η Εταιρεία λαμβάνει κάθε πρόσφορο μέτρο ώστε να διασφαλίσει τη συμμόρφωσή της με την παρούσα πολιτική και τους σχετικούς νόμους και κανονισμούς.

2.1.1 Νομικές βάσεις επεξεργασίας

Η επεξεργασία προσωπικών δεδομένων είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,
β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης (προσυμβατικό στάδιο),
γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση της Εταιρείας,
δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στην Εταιρεία.
στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει η Εταιρεία ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Όταν η επεξεργασία για σκοπό άλλο από αυτόν για τον οποίο έχουν αρχικά συλλεγεί τα δεδομένα προσωπικού χαρακτήρα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία, η Εταιρεία, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων:

α) τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού

χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας,
β) το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας,
γ) τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία (ευαίσθητα δεδομένα), ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία,
δ) τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,
ε) την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωανωνυμοποίηση.

2.1.2 Ειδικές κατηγορίες δεδομένων

Η Εταιρεία δεν προβαίνει σε επεξεργασία προσωπικών δεδομένων ειδικών κατηγοριών (ήτοι δεδομένων που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό)

2.1.3 Συγκατάθεση

Όταν η επεξεργασία βασίζεται στη συγκατάθεση πριν από την επεξεργασία προσωπικών δεδομένων, το υποκείμενο των δεδομένων ενημερώνεται καταλλήλως και δίνει τη συγκατάθεσή του ελεύθερα, με τρόπο σαφή και διακριτό. Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης. Η συγκατάθεση μπορεί να δοθεί ρητά ή σιωπηρά, π.χ. με την παροχή προσωπικών δεδομένων στην Εταιρεία. Η συγκατάθεση δε χρειάζεται απαραίτητα να είναι γραπτή, ωστόσο, σε περιπτώσεις κατά τις οποίες είναι ισχυρό το δυνητικό ενδεχόμενο να απαιτηθεί η απόδειξη της παροχής της (π.χ. προς δικαστήρια και αρχές), ενδέχεται να ζητηθεί από το υποκείμενο των δεδομένων να την παράσχει γραπτώς ή μέσω επιτρεπόμενων ηχογραφήσεων. Το υποκείμενο των δεδομένων είναι πάντοτε σε θέση να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή, με μεθοδολογία αντίστοιχης ευκολίας με την παροχή της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά.
Η παροχή συγκατάθεσης δεν απαιτείται στις ακόλουθες περιπτώσεις όπου η επεξεργασία είναι απαραίτητη για:

- Την εκτέλεση σύμβασης με το υποκείμενο των δεδομένων.
- Τη συμμόρφωση με έννομη υποχρέωση της Εταιρείας.
- Τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
- Την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στην Εταιρεία.

- Τους σκοπούς των εννόμων συμφερόντων που επιδιώκει η Εταιρεία. Εξαίρεση αποτελεί η περίπτωση κατά την οποία έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των προσωπικών δεδομένων, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.
- Όταν το υποκείμενο των δεδομένων έχει δώσει γενικά πρόσβαση στα προσωπικά του δεδομένα, π.χ. πληροφορίες που έχουν διατεθεί σε εφημερίδες ή τηλεφωνικούς καταλόγους και για τις οποίες δεν έχει απαγορεύσει την επεξεργασία τους.

Σε περίπτωση αμφιβολίας, τα υποκείμενα των δεδομένων (λ.χ. εργαζόμενοι, πελάτες Κ.Ο.) επικοινωνούν με τον Υπεύθυνο Προστασίας Δεδομένων. Για περισσότερες πληροφορίες τίθεται στη διάθεσή τους το Κεφ. 3 της παρούσας («Λήψη συγκατάθεσης υποκειμένων»).

2.1.4 Διαφάνεια κατά την επεξεργασία

Κατά τη συλλογή προσωπικών δεδομένων παρέχεται στο υποκείμενο των δεδομένων επαρκής πληροφόρηση με τρόπο συνοπτικό, διαφανή και κατανοητό, σχετικά με τα προσωπικά δεδομένα που συλλέγονται καθώς και για το σκοπό της επεξεργασίας τους, σύμφωνα με τα ειδικότερα προβλεπόμενα στον ΓΚΠΔ.

2.2 Η αρχή του περιορισμού του σκοπού

Τα προσωπικά δεδομένα που συλλέγονται τυγχάνουν επεξεργασίας αποκλειστικά και μόνο για το σκοπό που δηλώθηκε κατά τη στιγμή της συλλογής και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Εξαίρεση αποτελεί η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς.

2.3 Η αρχή της αναλογικότητας (ελαχιστοποίηση των δεδομένων)

Τα δεδομένα που συλλέγονται είναι κατάλληλα, συναφή και περιορίζονται, ως προς την έκταση και το πλήθος τους, στο αναγκαίο για τους σκοπούς της επεξεργασίας.

2.4 Η αρχή της ακρίβειας των δεδομένων (ποιότητα των δεδομένων)

Τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία είναι ακριβή και όταν είναι αναγκαίο επικαιροποιούνται. Η Εταιρεία λαμβάνει όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση προσωπικών δεδομένων τα οποία διαπιστώνεται ότι είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

2.5 Η αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας (περιορισμός της περιόδου αποθήκευσης)

Τα προσωπικά δεδομένα αποθηκεύονται και διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση

των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για την εκπλήρωση του σκοπού για τον οποίο συλλέχθηκαν. Εξαίρεση αποτελεί η αποθήκευση για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς (βλ. σχετικά: «Τήρηση & καταστροφή δεδομένων»).

2.6 Η αρχή της ακεραιότητας και εμπιστευτικότητας των δεδομένων

Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλειά τους, μεταξύ άλλων την προστασία από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια καθώς και την καταστροφή ή φθορά.
Φυσικά ή νομικά πρόσωπα τα οποία, λόγω της επαγγελματικής σχέσης τους με την Εταιρεία και στα πλαίσια των αρμοδιοτήτων τους, λαμβάνουν γνώση και στα οποία περιέρχονται εις γνώση τους εμπιστευτικές πληροφορίες και προσωπικά δεδομένα για λογαριασμό και υπό τις οδηγίες της Εταιρείας, οφείλουν να τηρούν το επαγγελματικό απόρρητο και να επιδεικνύουν απόλυτη εχεμύθεια στη χρήση των πληροφοριών αυτών. Η πρόσβαση των προσώπων αυτών στα τηρούμενα με οποιονδήποτε τρόπο ή μέσο αρχεία της Εταιρείας, στα οποία περιέχονται εμπιστευτικές πληροφορίες ή προσωπικά δεδομένα, απαγορεύεται εκτός εάν η πρόσβαση αυτή είναι αναγκαία για την παροχή υπηρεσιών από την Εταιρεία προς τον πελάτη.
Η ανωτέρω υποχρέωση τήρησης εχεμύθειας και εμπιστευτικότητας των προσωπικών δεδομένων καταλαμβάνει και τη διαβίβαση αυτών μεταξύ των λειτουργικών τμημάτων της Εταιρείας. Εξαιρείται μόνο η περίπτωση όπου η διαβίβαση των δεδομένων είναι απαραίτητη για την παροχή υπηρεσιών της Εταιρείας προς τον πελάτη ή για την άσκηση εποπτείας από τα αρμόδια όργανα. Εάν εκ παραδρομής έρθουν σε γνώση αναρμόδιων προσώπων προσωπικά δεδομένα, απαγορεύεται στα πρόσωπα αυτά η καθοιονδήποτε τρόπο χρησιμοποίηση και επεξεργασία των δεδομένων αυτών.
Για το σκοπούς αυτούς μεταξύ άλλων, η Εταιρεία έχει προχωρήσει στη διαβάθμιση των δεδομένων που επεξεργάζεται και στην εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων προστασίας ανά επίπεδο διαβάθμισης, σύμφωνα με την πολιτική ασφαλείας δεδομένων που διαθέτει, καθώς και στον καθορισμό ρυθμίσεων σχετικά με τη διαβίβαση δεδομένων (βλ. σχετικά: «Διαβάθμιση δεδομένων», «Διαβίβαση δεδομένων» & «Πολιτική Ασφαλείας Δεδομένων»).

2.7 Η αρχή της λογοδοσίας του υπεύθυνου επεξεργασίας

2.7.1 Αρχείο Δραστηριοτήτων Επεξεργασίας Προσωπικών Δεδομένων

Η Εταιρεία τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνη, στο οποίο περιλαμβάνονται κατ' ελάχιστο οι προβλεπόμενες στον ΓΚΠΔ πληροφορίες. Η Εταιρεία τηρεί χωριστό αρχείο δραστηριοτήτων για όλες τις περιπτώσεις για τις οποίες ενεργεί ως «εκτελών την επεξεργασία».
Με την επίβλεψη του Υπευθύνου Προστασίας Δεδομένων, σε κάθε περίπτωση μεταβολής των δραστηριοτήτων επεξεργασίας ενημερώνεται καταλλήλως το σχετικό αρχείο, με όλες τις προβλεπόμενες πληροφορίες. Ο Υπεύθυνος Εσωτερικού Ελέγχου και Κανονιστικής Συμμόρφωσης Κινδύνων επισκοπεί σε τακτική ή σε έκτακτη βάση εφόσον απαιτείται την επικαιροποίηση του αρχείου.

2.7.2 Εκτίμηση αντικτύπου για την προστασία των δεδομένων

Η Εταιρεία διεξάγει εκτίμηση αντικτύπου για την προστασία των δεδομένων, κάθε φορά που ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Ο σκοπός της εκτίμησης αντικτύπου για την προστασία των δεδομένων είναι να αξιολογηθούν και να μετριαστούν οι κίνδυνοι που σχετίζονται με την προστασία των προσωπικών δεδομένων. Η εκτίμηση αντικτύπου για την προστασία των δεδομένων διεξάγεται πριν από την έναρξη της επεξεργασίας ή μετά την καθ' οιονδήποτε τρόπο επικαιροποίησή της.

Ως υψηλού κινδύνου δραστηριότητες επεξεργασίας ορίζονται οι κάτωθι:

- Η συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών του υποκειμένου των δεδομένων, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο.
- Η επεξεργασία ευαίσθητων προσωπικών δεδομένων σε μεγάλη κλίμακα.
- Η συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα, π.χ. βιντεοσκόπηση ενός δημόσιου χώρου.

Περαιτέρω καθοδήγηση ως προς τις μορφές επεξεργασίας, οι οποίες ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων δίδει η Αρχή προστασίας Δεδομένων Προσωπικού Χαρακτήρα ('ΑΠΔΠΧ») με την 65/2018 Απόφασή της, διαθέσιμη στο: http://www.dpa.gr/portal/page?_pageid=33,223264&_dad=portal&_schema=PORTAL, όπως αυτή κάθε φορά ισχύει.

Η εκτίμηση αντικτύπου για την προστασία των δεδομένων τεκμηριώνεται επαρκώς και διεξάγεται υπό τη γενικότερη καθοδήγηση και επίβλεψη του Υπευθύνου Προστασίας Δεδομένων.

Όταν η εκτίμηση αντικτύπου για την προστασία των δεδομένων οδηγεί στο συμπέρασμα ότι υφίσταται υψηλός κίνδυνος για τα υποκείμενα των δεδομένων, η Εποπτεύουσα Αρχή (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) ενημερώνεται και ζητείται η γνώμη της πριν από την έναρξη της επεξεργασίας. Οι οδηγίες που θα λαμβάνονται από την Εποπτεύουσα Αρχή υιοθετούνται από την Εταιρεία.

2.7.3 Προστασία δεδομένων ήδη από το σχεδιασμό και εξ' ορισμού

Για την εξασφάλιση της προστασίας των προσωπικών δεδομένων, λαμβάνονται υπόψη οι ακόλουθες αρχές όταν αξιολογούνται οι τρέχουσες επιχειρηματικές διαδικασίες ή τα συστήματα επεξεργασίας δεδομένων ή όταν εισάγονται νέα συστήματα:

(α) Όταν εισάγονται νέα συστήματα επεξεργασίας δεδομένων, η Εταιρεία διασφαλίζει από το σχεδιασμό ("by design") ένα υψηλό επίπεδο προστασίας των δεδομένων. Ιδιαίτερα, κάθε νέο σύστημα και κάθε νέα διαδικασία που υιοθετείται συμμορφώνεται με τις ακόλουθες αρχές:

- Λήψη τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της συστηματικής και ασφαλούς διαχείρισης των προσωπικών δεδομένων κατά τον κύκλο ζωής τους δηλαδή από τη συλλογή, την επεξεργασία έως τη διαγραφή.

- Μετρίαση στο ελάχιστο δυνατό των προσωπικών δεδομένων που συλλέγονται και τίθενται υπό επεξεργασία για την εκπλήρωση του σκοπού για τον οποίο αρχικά συλλέγονται.
- Όταν η τεχνική της ανωνυμοποίησης των προσωπικών δεδομένων δεν παρεμποδίζει το σκοπό της επεξεργασίας τους, εφαρμόζεται έτσι ώστε το φυσικό πρόσωπο στο οποίο αναφέρονται να μη μπορεί πλέον να ταυτοποιηθεί.
- Εφόσον τα δεδομένα προσωπικού χαρακτήρα δε μπορούν να καταστούν ανώνυμα και εφόσον είναι δυνατό, εφαρμόζονται μέτρα ασφαλείας όπως η ψευδωανωνυμοποίηση, η κρυπτογράφηση ή ο περιορισμός πρόσβασης.
- Η πρόσβαση σε προσωπικά δεδομένα σε άλλα πρόσωπα της Εταιρείας επιτρέπεται μόνο όταν αυτή είναι απολύτως απαραίτητη για την τέλεση των ρόλων, καθηκόντων και αρμοδιοτήτων τους.
- Ο συστηματικός έλεγχος της ποιότητας των προσωπικών δεδομένων αποτελεί μέρος της διαχείρισης του κύκλου ζωής των δεδομένων.
- Τα συστήματα επεξεργασίας δεδομένων προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση μέσω τεχνικών και οργανωτικών μέτρων.

(β) Τα συστήματα επεξεργασίας δεδομένων της Εταιρείας σχεδιάζονται κατά τέτοιο τρόπο ώστε να διασφαλίζονται οι αυστηρότερες ρυθμίσεις απορρήτου εξ' ορισμού.

Η εκτενέστερη επεξεργασία προσωπικών δεδομένων επιτρέπεται μόνο εάν το υποκείμενο των δεδομένων επιλέξει ή συμφωνεί σε ένα χαμηλότερο επίπεδο προστασίας. Παράδειγμα: με τη χειροκίνητη αλλαγή των ρυθμίσεων απορρήτου στον ιστότοπο της Εταιρείας, όπου επιλέγεται από το υποκείμενο μια λιγότερο περιοριστική επιλογή με την οποία δίνει τη ρητή συγκατάθεσή του στην εκτεταμένη επεξεργασία ("opt-in").

3. Λήψη συγκατάθεσης των υποκειμένων

Η Εταιρεία αναγνωρίζει τη σπουδαιότητα και τις απαιτήσεις για διασφάλιση της ύπαρξης ορθής νόμιμης βάσης για την επεξεργασία των προσωπικών δεδομένων, και τις σχετικές της υποχρεώσεις, καθώς και την ανάγκη λήψης της συγκατάθεσης του υποκειμένου των δεδομένων, πριν από την έναρξη της επεξεργασίας, σε όλες τις περιπτώσεις όπου η συγκατάθεση αποτελεί τη νόμιμη βάση επεξεργασίας. Για τους λόγους αυτούς, διαθέτει και εφαρμόζει ρυθμίσεις και διαδικασίες στα πλαίσια της παρούσας πολιτικής, που αφορούν τη Λήψη Συγκατάθεσης των Υποκείμενων προσώπων.

3.1 Προϋποθέσεις για λήψη έγκυρης συγκατάθεσης

Στις περιπτώσεις κατά τις οποίες η συγκατάθεση αποτελεί τη νόμιμη βάση επεξεργασίας, η Εταιρεία διασφαλίζει την ύπαρξη των παρακάτω προϋποθέσεων:

- Η συγκατάθεση δίδεται ελεύθερα, το οποίο προϋποθέτει ότι το υποκείμενο των δεδομένων έχει αληθινή και ελεύθερη επιλογή ενώ είναι σε θέση να αρνηθεί τη συγκατάθεσή του χωρίς να ζημιωθεί. Για τη διατύπωση ελεύθερης βούλησης για παροχή συγκατάθεσης το υποκείμενο θα πρέπει να μην απειλείται, εξαπατάται ή πλανάται. Κατά την εκτίμηση του κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως

προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

- Το υποκείμενο των δεδομένων πρέπει να συμφωνεί στην επεξεργασία κατά τρόπο συγκεκριμένο, δηλαδή αναφορικά με έναν εξειδικευμένο σκοπό επεξεργασίας και όχι γενικά και αόριστα. Επομένως, όταν η επεξεργασία έχει πολλαπλούς σκοπούς, το υποκείμενο των δεδομένων θα πρέπει να συγκατατίθεται ξεχωριστά για κάθε έναν από αυτούς τους σκοπούς έτσι ώστε να εξασφαλίζεται η διαφάνεια και η δυνατότητα ελέγχου της επεξεργασίας των δεδομένων. Μία «γενική συγκατάθεση» στην επεξεργασία των προσωπικών του δεδομένων ενδέχεται να περιλαμβάνει σκοπούς επεξεργασίας που αν το υποκείμενο είχε αντιληφθεί, πιθανότατα δε θα είχε συναινέσει.
- Όλες οι απαραίτητες πληροφορίες παρέχονται στο υποκείμενο των δεδομένων σε απλή και κατανοητή γλώσσα. Μακροσκελή κείμενα με ακατανόητες εκφράσεις δε θεωρούνται πως πληρούν αυτήν την προϋπόθεση (π.χ. όροι πολιτικής απορρήτου τους οποίους το υποκείμενο των δεδομένων δεν είναι σε θέση να κατανοήσει, αλλά συναινεί για να προχωρήσει στη χρήση μιας υπηρεσίας).
- Το υποκείμενο των δεδομένων πρέπει να συμφωνεί στην επεξεργασία κατά τρόπο ρητό και σαφή, δηλαδή με δήλωση ή με σαφή θετική ενέργεια (π.χ. με συμπλήρωση τετραγωνιδίου σε αίτηση, με γραπτή ή προφορική δήλωση, κλπ.). Επομένως, προσυμπληρωμένα τετραγωνίδια, αδράνεια ή σιωπή δεν συνεπάγονται λήψη έγκυρης συγκατάθεσης.
- Η συγκατάθεση θα πρέπει να παρέχεται από το υποκείμενο των δεδομένων πριν από την έναρξη της σε επεξεργασίας.
- Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δε θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά και η ανάκληση της συγκατάθεσης πραγματοποιείται εξίσου εύκολα με την παροχή της, ακολουθώντας την ίδια μεθοδολογία προς την αντίθετη όμως κατεύθυνση.

3.2 Διαδικασία λήψης συγκατάθεσης

Η λήψη της συγκατάθεσης από τα υποκείμενα των δεδομένων πραγματοποιείται από την Εταιρεία ακολουθώντας τα παρακάτω βήματα:

- Βήμα 1: Εκτίμηση χρήσης συγκατάθεσης ως νόμιμης βάση επεξεργασίας
- Βήμα 2: Λήψη έγκυρης και έγκαιρης συγκατάθεσης
- Βήμα 3: Τήρηση αρχείου συγκαταθέσεων

Λίστα ελέγχου

(α) Λήψη έγκυρης και έγκαιρης συγκατάθεσης

- Έχουμε ελέγξει ότι η συγκατάθεση είναι η πιο κατάλληλη νόμιμη βάση επεξεργασίας.
- Έχουμε διατυπώσει τη συγκατάθεση διακριτά και ξεχωριστά από άλλα θέματα, όπως όρους και προϋποθέσεις (π.χ. ξεχωριστά από τους όρους χρήσης που σχετίζονται με την υπηρεσία που

προσφέρουμε).

• Διασφαλίζουμε ότι η συγκατάθεση λαμβάνεται από τα υποκείμενα των δεδομένων ελεύθερα (το υποκείμενο των δεδομένων έχει αληθινή και ελεύθερη επιλογή και δε δίνει τη συγκατάθεσή του επειδή απειλείται, εξαπατάται ή πλανάται).

• Ζητάμε από τα υποκείμενα των δεδομένων να συμμετέχουν ενεργά και θετικά. Δεν χρησιμοποιούμε τη σιωπή, προσημειωμένα πεδία ή την αδράνεια ως συγκατάθεση.

• Χρησιμοποιούμε σαφή και απλή γλώσσα που είναι εύκολο να κατανοηθεί.

• Καθορίζουμε με σαφήνεια και ξεχωριστά κάθε σκοπό επεξεργασίας.

• Παρέχουμε όλες τις απαραίτητες πληροφορίες στα υποκείμενα των δεδομένων όπως αυτές αναφέρονται στο εδάφιο 2.3 του παρόντος κεφαλαίου.

• Διασφαλίζουμε ότι τα υποκείμενα των δεδομένων μπορούν να αρνηθούν τη συγκατάθεσή τους χωρίς να έχουν κάποιο αντίκτυπο.

• Δεν καθιστούμε τη συγκατάθεση ως προαπαιτούμενο για την παροχή μιας υπηρεσίας. 3

• Διασφαλίζουμε ότι η συγκατάθεση λαμβάνεται από τα υποκείμενα των δεδομένων πριν την έναρξη της επεξεργασίας.

• Διασφαλίζουμε ότι τα υποκείμενα των δεδομένων μπορούν να ανακαλέσουν τη συγκατάθεσή τους ανά πάσα στιγμή και τα ενημερώνουμε σχετικά.

• Διασφαλίζουμε ότι η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.

(β) Τήρηση αρχείου συγκαταθέσεων

• Διατηρούμε αρχείο και αποδεικτικά στοιχεία για το πότε και πώς αποκτήσαμε τη συγκατάθεση από τα υποκείμενα των δεδομένων.

• Διατηρούμε αρχείο ανακλήσεων συγκαταθέσεων.

4. Δικαιώματα υποκειμένων & διαχείριση των αιτημάτων τους

Κάθε υποκείμενο των δεδομένων έχει τα ακόλουθα δικαιώματα σύμφωνα με τον ΓΚΠΔ:

- ► Το δικαίωμα ενημέρωσης και πρόσβασης.
- ► Το δικαίωμα διόρθωσης.
- ► Το δικαίωμα διαγραφής («δικαίωμα στη λήθη»).
- ► Το δικαίωμα περιορισμού της επεξεργασίας.
- ► Το δικαίωμα στη φορητότητα των δεδομένων.
- ► Το δικαίωμα εναντίωσης.
- ► Δικαιώματα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ.

Στα αιτήματα που λαμβάνονται από το υποκείμενο των δεδομένων και αφορούν την άσκηση των παραπάνω δικαιωμάτων, η Εταιρεία απαντά το αργότερο εντός ενός (1) μήνα από τη λήψη του αιτήματος με δυνατότητα παράτασης δύο (2) επιπλέον μηνών σε περίπτωση πολύπλοκων ή πολυάριθμων αιτημάτων. Σε αυτή την περίπτωση, η Εταιρεία ενημερώνει το υποκείμενο των δεδομένων σχετικά με

την επέκταση της προθεσμίας και εξηγεί τους λόγους εντός ενός (1) μήνα από την υποβολή του αιτήματος.

4.1 Δικαιώματα υποκειμένων

4.1.1 Δικαίωμα ενημέρωσης και πρόσβασης.

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει από την Εταιρεία επιβεβαίωση για το κατά πόσον ή όχι προσωπικά δεδομένα που το αφορούν υφίστανται επεξεργασία και σε περίπτωση που αυτό συμβαίνει, να έχει πρόσβαση στα προσωπικά του δεδομένα και στις ακόλουθες πληροφορίες :

- Τους σκοπούς της επεξεργασίας,
- τις σχετικές κατηγορίες προσωπικών δεδομένων,
- τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα προσωπικά δεδομένα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,
- το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα προσωπικά δεδομένα εάν είναι δυνατόν ή όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,
- την ύπαρξη του δικαιώματος υποβολής αιτήματος στην Εταιρεία για διόρθωση ή διαγραφή προσωπικών δεδομένων ή περιορισμό της επεξεργασίας των προσωπικών δεδομένων που το αφορούν ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία,
- το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής Εποπτεύουσα Αρχή),
- κάθε διαθέσιμη πληροφορία σχετικά με την προέλευση των προσωπικών δεδομένων, όταν τα προσωπικά δεδομένα δε συλλέγονται από το υποκείμενο των δεδομένων,
- την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, και στις περιπτώσεις αυτές κατ' ελάχιστον σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων,
- το δικαίωμα να ενημερώνεται για τις κατάλληλες εγγυήσεις σχετικά με τη διαβίβαση των προσωπικών του δεδομένων, στις περιπτώσεις που τα προσωπικά του δεδομένα διαβιβάζονται σε τρίτη χώρα ή διεθνή οργανισμό.

  Το πρώτο αντίγραφο των προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία παρέχεται από την Εταιρεία χωρίς χρέωση. Σε περίπτωση που ζητηθούν επιπλέον αντίγραφα από το υποκείμενο των δεδομένων, η Εταιρεία διατηρεί το δικαίωμα να επιβάλλει συγκεκριμένη χρέωση, σε λογικά πλαίσια με βάση τα διαχειριστικά κόστη.

  Στις περιπτώσεις που το αίτημα υποβληθεί με ηλεκτρονικά μέσα, η ενημέρωση παρέχεται στην ηλεκτρονική μορφή που χρησιμοποιείται συνήθως, εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό. Η λήψη αντιγράφου των προσωπικών δεδομένων από ένα υποκείμενο αυτών, δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων υποκειμένων. Τέλος, στις περιπτώσεις κατά τις οποίες η Εταιρεία επεξεργάζεται μεγάλο όγκο πληροφοριών σχετικά με το υποκείμενο των δεδομένων, μπορεί να ζητήσει από το υποκείμενο των δεδομένων να προσδιορίσει τις πληροφορίες ή τις δραστηριότητες επεξεργασίας στις οποίες αναφέρεται το αίτημά του, προτού διατεθούν οι πληροφορίες.

Παραδείγματα άσκησης δικαιώματος ενημέρωσης και πρόσβασης:

- Το υποκείμενο των δεδομένων επιθυμεί να επαληθεύσει για ποιους σκοπούς χρησιμοποιούνται τα προσωπικά του δεδομένα και ζητάει πρόσβαση σε αυτές τις πληροφορίες.
- Το υποκείμενο των δεδομένων ζητάει από την Εταιρεία να του παρασχεθούν όλα τα προσωπικά δεδομένα που έχει στην κατοχή της και τα οποία το αφορούν.

4.1.2 Δικαίωμα διόρθωσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από την Εταιρεία χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών προσωπικών δεδομένων που το αφορούν. Επιπλέον, έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών προσωπικών δεδομένων που το αφορούν, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

Στις περιπτώσεις κατά τις οποίες τα προσωπικά δεδομένα έχουν κοινοποιηθεί σε τρίτα μέρη (αποδέκτες), το αίτημα για τη διόρθωση των προσωπικών δεδομένων γνωστοποιείται από την Εταιρεία στα εν λόγω τρίτα μέρη προκειμένου να προχωρήσουν στη διόρθωση των προσωπικών δεδομένων. Εξαίρεση αποτελούν οι περιπτώσεις όπου η γνωστοποίηση είναι ανέφικτη ή συνεπάγεται δυσανάλογη προσπάθεια. Εφόσον ζητηθεί από το υποκείμενο των δεδομένων, η Εταιρεία το ενημερώνει, σχετικά με τα εν λόγω τρίτα μέρη.

Παραδείγματα άσκησης δικαιώματος διόρθωσης:

►Το υποκείμενο των δεδομένων, του οποίου η διεύθυνση έχει μεταβληθεί, ζητάει από την Εταιρεία να αλλαχθεί η πληροφορία αυτή.

►Το υποκείμενο των δεδομένων ζητάει τη διόρθωση το ονοματεπωνύμου του, το οποίο έχει καταγραφεί από την Εταιρεία ανορθόγραφα.

4.1.3 Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από την Εταιρεία τη διαγραφή των προσωπικών δεδομένων που το αφορούν. Η Εταιρεία διαγράφει τα προσωπικά δεδομένα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

►Τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

►Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία.

►Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία, ασκώντας το σχετικό δικαίωμά του, και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία.

►Το προσωπικά δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα.

►Τα προσωπικά δεδομένα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του δικαίου στο οποίο υπόκειται η Εταιρεία.

►Τα προσωπικά δεδομένα έχουν συλλεχθεί για την παροχή υπηρεσιών της κοινωνίας των

πληροφοριών απευθείας σε παιδί το οποίο είναι λιγότερο από 16 ετών.

Στις περιπτώσεις κατά τις οποίες τα προσωπικά δεδομένα έχουν κοινοποιηθεί σε τρίτα μέρη (αποδέκτες), το αίτημα για τη διαγραφή των προσωπικών δεδομένων γνωστοποιείται από την Εταιρεία στα εν λόγω τρίτα μέρη προκειμένου να προχωρήσουν στη διαγραφή των προσωπικών δεδομένων. Εξαίρεση αποτελούν οι περιπτώσεις όπου η γνωστοποίηση είναι ανέφικτη ή συνεπάγεται δυσανάλογη προσπάθεια. Εφόσον ζητηθεί από το υποκείμενο των δεδομένων, η Εταιρεία το ενημερώνει, σχετικά με τα εν λόγω τρίτα μέρη.

Στις περιπτώσεις κατά τις οποίες η Εταιρεία έχει δημοσιοποιήσει τα προσωπικά δεδομένα και υποχρεούται να τα διαγράψει, προβαίνει στη λήψη εύλογων μέτρων –λαμβανομένης υπόψη της διαθέσιμης τεχνολογίας και του κόστους εφαρμογής και συμπεριλαμβανομένων τεχνικών μέτρων- για να ενημερώσει τους Υπευθύνους επεξεργασίας που επεξεργάζονται τα προσωπικά δεδομένα ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω προσωπικών δεδομένων.

Η Εταιρεία αρνείται να προβεί στις παραπάνω ενέργειες οι οποίες αφορούν το δικαίωμα διαγραφής, στις περιπτώσεις κατά τις οποίες η επεξεργασία των προσωπικών δεδομένων είναι αναγκαία:

►Για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση.

►Για τη συμμόρφωση με νομική υποχρέωση βάσει του δικαίου στο οποίο υπόκειται η Εταιρεία.

►Για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στην Εταιρεία.

►Για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας.

►Για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, στο βαθμό που η διαγραφή είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη των σκοπών της εν λόγω επεξεργασίας.

►Για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. Παραδείγματα άσκησης δικαιώματος διαγραφής:

- Το υποκείμενο των δεδομένων, το οποίο έχει παράσχει τα προσωπικά του δεδομένα στην Εταιρεία κατόπιν συγκατάθεσης, ανακαλεί τη συγκατάθεσή του και ζητάει τη διαγραφή των προσωπικών του δεδομένων. Η Εταιρεία ελέγχει το κατά πόσο υπάρχει άλλη νόμιμη βάση επεξεργασίας και αν όχι προχωράει στη διαγραφή των προσωπικών δεδομένων και στην ενημέρωση του υποκειμένου των δεδομένων.
- Το υποκείμενο των δεδομένων (προμηθευτής), μεταξύ του οποίου και της Εταιρείας υπάρχει σύμβαση, ζητάει τη διαγραφή των προσωπικών του δεδομένων. Η Εταιρεία ενημερώνει το υποκείμενο των δεδομένων ότι δε θα προχωρήσει στη διαγραφή των προσωπικών του δεδομένων καθώς η επεξεργασία είναι απαραίτητη για την εκτέλεση της σύμβασης.

4.1.4 <u>Δικαίωμα περιορισμού της επεξεργασίας.</u>

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από την Εταιρεία τον περιορισμό της επεξεργασίας των προσωπικών του δεδομένων, όταν ισχύει ένα από τα ακόλουθα:

- Η ακρίβεια των προσωπικών δεδομένων αμφισβητείται από το υποκείμενο των δεδομένων. Η Εταιρεία προχωράει στον περιορισμό της επεξεργασίας για χρονικό διάστημα που της

επιτρέπει να επαληθεύσει την ακρίβεια των προσωπικών δεδομένων.

- ► Η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντί αυτής, τον περιορισμό της χρήσης τους.
- ► Η Εταιρεία δε χρειάζεται πλέον τα προσωπικά δεδομένα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.
- ► Το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι της Εταιρείας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

Η Εταιρεία εφαρμόζει μεθόδους περιορισμού της επεξεργασίας προσωπικών δεδομένων οι οποίες, μεταξύ άλλων, περιλαμβάνουν την προσωρινή μετακίνηση των επιλεγμένων δεδομένων σε άλλο σύστημα επεξεργασίας, την αφαίρεση της προσβασιμότητας των επιλεγμένων δεδομένων προσωπικού χαρακτήρα από τους χρήστες ή την προσωρινή αφαίρεση δημοσιευμένων δεδομένων από ιστοσελίδα.
Προσωπικά δεδομένα για τα οποία έχει ασκηθεί το δικαίωμα περιορισμού, υπόκεινται σε επεξεργασία (με εξαίρεση την αποθήκευση) μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους. Πριν από την άρση του περιορισμού επεξεργασίας, η Εταιρεία ενημερώνει σχετικά το υποκείμενο των δεδομένων.
Στις περιπτώσεις κατά τις οποίες τα προσωπικά δεδομένα έχουν κοινοποιηθεί σε τρίτα μέρη (αποδέκτες), το αίτημα για τον περιορισμό της επεξεργασίας των προσωπικών δεδομένων γνωστοποιείται από την Εταιρεία στα εν λόγω τρίτα μέρη προκειμένου να προχωρήσουν στον περιορισμό της επεξεργασίας των προσωπικών δεδομένων. Εξαίρεση αποτελούν οι περιπτώσεις όπου η γνωστοποίηση είναι ανέφικτη ή συνεπάγεται δυσανάλογη προσπάθεια. Εφόσον ζητηθεί από το υποκείμενο των δεδομένων, η Εταιρεία το ενημερώνει, σχετικά με τα εν λόγω τρίτα μέρη.

4.1.5 Δικαίωμα στη φορητότητα των δεδομένων

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από την Εταιρεία:
►Να λάβει τα προσωπικά δεδομένα που το αφορούν και τα οποία έχει παράσχει στην Εταιρεία σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο.
►Να ζητήσει από την Εταιρεία να διαβιβάσει τα προσωπικά δεδομένα που τηρεί και τα οποία το αφορούν, σε άλλον υπεύθυνο επεξεργασίας (σε περίπτωση που αυτό είναι τεχνικά εφικτό).

Το δικαίωμα στη φορητότητα των δεδομένων μπορεί να ασκηθεί μόνο εάν η επεξεργασία βασίζεται σε συγκατάθεση ή σε σύμβαση καθώς και εάν η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα. Αντιθέτως, το δικαίωμα στη φορητότητα των δεδομένων δεν εφαρμόζεται στην περίπτωση που η επεξεργασία βασίζεται σε νόμιμη υποχρέωση ή σε έννομο συμφέρον της Εταιρείας.
Το δικαίωμα στη φορητότητα των δεδομένων δεν επηρεάζει άμεσα και δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων (π.χ. η Εταιρεία, στα πλαίσια της ικανοποίησης του δικαιώματος στη φορητότητα των δεδομένων, δεν κοινοποιεί προσωπικά δεδομένα που σχετίζονται με άλλα υποκείμενα των δεδομένων).
Τέλος, η φορητότητα δεδομένων δε σημαίνει αυτομάτως και τη διαγραφή των εν λόγω δεδομένων. Η

Εταιρεία μπορεί να συνεχίσει να επεξεργάζεται τα εν λόγω δεδομένα εφόσον συνεχίζει να υφίσταται νόμιμη βάση επεξεργασίας.

4.1.6 Δικαίωμα εναντίωσης

Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται ανά πάσα στιγμή στην επεξεργασία των προσωπικών του δεδομένων, περιλαμβανομένης της κατάρτισης προφίλ, η οποία:

► Βασίζεται σε σκοπούς έννομου συμφέροντος που επιδιώκεται από την Εταιρεία ή από τρίτο μέρος,

► Βασίζεται στην εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον.

Σε αυτή την περίπτωση, η Εταιρεία θα πρέπει να σταματήσει την επεξεργασία των προσωπικών δεδομένων εκτός εάν:

►Καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων,

►Καταδείξει ότι η επεξεργασία απαιτείται για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Επιπλέον, το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται ανά πάσα στιγμή στην επεξεργασία προσωπικών του δεδομένων η οποία εκτελείται για σκοπούς απευθείας εμπορικής προώθησης, περιλαμβανομένης της κατάρτισης προφίλ, σε περίπτωση που σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

Το δικαίωμα εναντίωσης περιέχεται ρητά εις γνώσιν του υποκειμένου των δεδομένων και παρουσιάζεται σαφώς και ξεχωριστά από κάθε άλλη πληροφορία, το αργότερο κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων και, τουλάχιστον, στα πλαίσια της προσυμβατικής πληροφόρησής του.

4.1.7 Δικαίωμα άρνησης υπαγωγής σε αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο. Ενδεικτικά παραδείγματα τέτοιων περιπτώσεων οι οποίες θεωρούνται πως

επηρεάζουν σημαντικά το υποκείμενο των δεδομένων είναι η αυτόματη απόρριψη μιας διαδικτυακής αίτησης εργασίας ή πρακτικές διαδικτυακής πρόσληψης χωρίς ανθρώπινη διαμεσολάβηση.

Ωστόσο, το συγκεκριμένο δικαίωμα δε μπορεί να εξασκηθεί όταν η απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας:

►Είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και της Εταιρείας.

►Βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

►Επιτρέπεται βάσει του δικαίου στο οποίο υπόκειται η Εταιρεία και το οποίο προβλέπει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

Για παράδειγμα, εάν η απόφαση λαμβάνεται στο πλαίσιο αποτροπής φοροδιαφυγής ή αποφυγής/πρόληψης νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες ή χρηματοδότηση της

τρομοκρατίας ή για σκοπούς ελέγχου απάτης, η Εταιρεία δεν είναι σε θέση να παρέχει στο υποκείμενο των δεδομένων το δικαίωμα να μην υπόκειται σε λήψη απόφασης που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία. Ωστόσο, η Εταιρεία εφαρμόζει κατάλληλα μέτρα για να διασφαλίσει τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Πιο συγκεκριμένα, η Εταιρεία παρέχει στο υποκείμενο των δεδομένων τουλάχιστον το δικαίωμα να περιληφθεί ανθρώπινη παρέμβαση, να εκφράσει τη δική του οπτική γωνία ή να αμφισβητήσει την απόφαση.

4.2 Διαδικασία διαχείρισης αιτημάτων υποκειμένων των δεδομένων

Στα αιτήματα που λαμβάνονται από το υποκείμενο των δεδομένων και αφορούν την άσκηση των παραπάνω δικαιωμάτων θα πρέπει να παρέχεται απάντηση από την Εταιρεία, ακολουθώντας τα βήματα που περιγράφονται παρακάτω.

Βήμα 1ο : Παραλαβή του αιτήματος.

Τα αιτήματα υποβάλλονται από το υποκείμενο των δεδομένων στα ειδικά διαμορφωμένα κανάλια επικοινωνίας (τηλέφωνο, email, ταχυδρομική διεύθυνση) τα οποία έχει δημιουργήσει η Εταιρεία. Η διαχείριση των συγκεκριμένων καναλιών επικοινωνίας πραγματοποιείται από Υπεύθυνο Προστασίας Δεδομένων.

Οι εργαζόμενοι της Εταιρείας ενημερώνουν τα υποκείμενα των δεδομένων σε κάθε σχετική επικοινωνία, ότι τα συγκεκριμένα κανάλια επικοινωνίας αποτελούν το μοναδικό μέσο για την υποβολή των σχετικών αιτημάτων. Σε περίπτωση που κάποιο αίτημα ληφθεί από άλλο μέσο, όπως διαφορετικό τηλέφωνο, e-mail, κλπ.), τότε ο αρμόδιος εργαζόμενος (λήπτης του αιτήματος):

- ► Είτε κατευθύνει το υποκείμενο των δεδομένων ώστε να υποβάλλει το αίτημα με έναν από τους παραπάνω τρόπους,
- ► είτε αναλαμβάνει ο ίδιος να αποτυπώσει γραπτώς και να προωθήσει το αίτημα εντός τριών (3) ημερών από τη λήψη του στον Υπεύθυνο Προστασίας Δεδομένων.

Τα σχετικά αιτήματα υποβάλλονται από το υποκείμενο των δεδομένων εγγράφως είτε σε έγχαρτα είτε σε ηλεκτρονική μορφή, μέσω της προ διατυπωμένης «Φόρμας Άσκησης Δικαιωμάτων αναφορικά με Προσωπικά Δεδομένα» που διαθέτει η Εταιρεία.

Βήμα 2ο : Εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων.

Έπειτα από τη λήψη του σχετικού αιτήματος και πριν την καταχώρησή του και την περαιτέρω επεξεργασία του, ο Υπεύθυνος Προστασίας Δεδομένων προχωρά στην ταυτοποίηση του υποκειμένου των δεδομένων. Η ταυτοποίηση του υποκειμένου των δεδομένων πραγματοποιείται μέσω της ζήτησης παροχής πληροφοριών από το υποκείμενο των δεδομένων οι οποίες αναφέρονται σε αυτό, όπως ημερομηνία γέννησης, αριθμός ταυτότητα/διαβατηρίου, τηλέφωνο, διεύθυνση, κλπ.

Σε περίπτωση που υπάρχουν βάσιμες αμφιβολίες όσον αφορά την ταυτότητα του υποκειμένου των δεδομένων το οποίο υποβάλει το αίτημα, δύναται να ζητηθεί να παρασχεθούν επιπλέον πληροφορίες, απαραίτητες για την εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων. Τέτοιες πληροφορίες μπορεί να περιλαμβάνουν ενδεικτικά και όχι περιοριστικά την παροχή κάποιου έγκυρου εγγράφου, όπως Δελτίο Αστυνομικής Ταυτότητας ή Διαβατήριο.

Τα στοιχεία/έγγραφα που συλλέγονται για την επαλήθευση της ταυτότητας, διατηρούνται για περιορισμένο χρονικό διάστημα και σε καμία περίπτωση περισσότερο από το διάστημα το οποίο απαιτείται για την ικανοποίηση του αιτήματος του υποκειμένου των δεδομένων. Μετά το πέρας του εν λόγω διαστήματος, τα στοιχεία/έγγραφα καταστρέφονται. (βλ. σχετικά: «Τήρηση & καταστροφή δεδομένων»).
Έπειτα από την εξακρίβωση της ταυτότητας, ο Υπεύθυνος Προστασίας Δεδομένων αποστέλλει στο υποκείμενο των δεδομένων βεβαίωση παραλαβής, σύμφωνα με τη σχετική προδιατυπωμένη φόρμα, ώστε να του γνωστοποιηθεί ότι το αίτημά του παραλήφθηκε και βρίσκεται υπό επεξεργασία, ενώ παράλληλα ενημερώνεται για το χρονικό διάστημα εντός του οποίου πρόκειται να λάβει απάντηση στο αίτημά του.

Βήμα 3ο : Προώθηση του αιτήματος.
Έπειτα από την εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων, το σχετικό αίτημα προωθείται εντός σαράντα οκτώ (48) ωρών από τον Υπεύθυνο Προστασίας Δεδομένων στον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner). Παράλληλα, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) ενημερώνεται σχετικά με την ημερομηνία λήψης του αιτήματος.

Βήμα 4ο : Έλεγχος βασιμότητας αιτήματος.
Έπειτα από την παραλαβή του σχετικού αιτήματος ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) διερευνά τη βασιμότητα του εν λόγω αιτήματος.
Κατά τον έλεγχο βασιμότητας, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) αρχικά προχωράει στον έλεγχο του Αρχείου Δραστηριοτήτων Επεξεργασίας Προσωπικών Δεδομένων προκειμένου να διαπιστωθεί κατά πόσο τηρούνται προσωπικά δεδομένα του υποκειμένου των δεδομένων το οποίο υποβάλλει το αίτημα καθώς και σε ποια μορφή (έντυπη / ηλεκτρονική μορφή). Έπειτα από τον συγκεκριμένο έλεγχο, και εφόσον διαπιστωθεί ότι όντως τηρούνται προσωπικά δεδομένα του υποκειμένου των δεδομένων το οποίο υποβάλλει το αίτημα, ελέγχεται η ουσιαστική βασιμότητα του αιτήματος. Η συγκεκριμένη ενέργεια πραγματοποιείται από τον Υπεύθυνο Προστασίας Δεδομένων , σε συνεργασία με τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner).

Ο έλεγχος ουσιαστικής βασιμότητας του υποβληθέντος αιτήματος διενεργείται ως ακολούθως:
(α) Δικαίωμα ενημέρωσης και πρόσβασης.
Το αίτημα είναι πάντα βάσιμο εκτός και αν συντρέχουν λόγοι περιορισμού του δικαιώματος όπως:

- ►Αποφυγή παρακώλυσης ή της συσκότισης διεξαγόμενων ερευνών, αναγκαίων πράξεων και διαδικασιών για την επίτευξη σκοπών προστασίας δικαιωμάτων και ελευθεριών των φυσικών προσώπων.
- ►Αποφυγή αποτροπής ή παρεμπόδισης της πρόληψης, διαπίστωσης, διερεύνησης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων.
- ►Προστασία της δημόσιας ασφάλειας.
- ►Προστασία της εθνικής ασφάλειας.
- ►Προστασία των δικαιωμάτων και των ελευθεριών τρίτων.

(β) Δικαίωμα διόρθωσης.
Το αίτημα είναι βάσιμο όταν τα δεδομένα είναι ανακριβή ή ελλιπή.

(γ) Δικαίωμα διαγραφής («δικαίωμα στη λήθη»).

Το αίτημα είναι βάσιμο όταν:

►Τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

►Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,

►Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία, ασκώντας το σχετικό δικαίωμά του, και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία,

►Το προσωπικά δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα,

►Τα προσωπικά δεδομένα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του δικαίου στο οποίο υπόκειται η Εταιρεία,

►Τα προσωπικά δεδομένα έχουν συλλεχθεί για την παροχή υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε παιδί το οποίο είναι λιγότερο από 16 ετών.

(δ) Δικαίωμα περιορισμού της επεξεργασίας.

Το αίτημα είναι βάσιμο όταν:

►Η ακρίβεια των προσωπικών δεδομένων αμφισβητείται από το υποκείμενο των δεδομένων.

►Η επεξεργασία των προσωπικών δεδομένων είναι παράνομη και το υποκείμενο των δεδομένων ζητάει τον περιορισμό της χρήσης τους αντί για τη διαγραφή τους.

► Η Εταιρεία δε χρειάζεται πλέον τα προσωπικά δεδομένα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

(ε) Δικαίωμα στη φορητότητα των δεδομένων.

Το αίτημα είναι βάσιμο όταν:

►Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών δεδομένων.

►Η επεξεργασία των προσωπικών δεδομένων είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία το υποκείμενο των δεδομένων είναι μέρος.

►Η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

(στ) Δικαίωμα εναντίωσης.

Το αίτημα είναι βάσιμο όταν:

►Τα προσωπικά δεδομένα του υποκειμένου των δεδομένων γίνονται αντικείμενο επεξεργασίας για λόγους απευθείας εμπορικής προώθησης,

►Η επεξεργασία προσωπικών δεδομένων είναι απαραίτητη για λόγους δημοσίου συμφέροντος ή για λόγους άσκησης δημόσιας εξουσίας εκ μέρους της Εταιρείας και αυτή δεν μπορεί να αποδείξει ότι το δικαίωμα της να επεξεργάζεται τα δεδομένα υπερτερεί των δικαιωμάτων του υποκειμένου των δεδομένων,

►Η επεξεργασία προσωπικών δεδομένων είναι απαραίτητη για λόγους εννόμου συμφέροντος της Εταιρείας ή τρίτου μέρους και δεν μπορούν να αποδείξουν ότι το δικαίωμα τους να

επεξεργάζονται τα δεδομένα υπερτερεί των δικαιωμάτων του υποκειμένου.

(ζ) Δικαίωμα άρνησης υπαγωγής σε αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ.

Το αίτημα είναι πάντα βάσιμο εκτός και αν συντρέχουν λόγοι περιορισμού του δικαιώματος όπως:

►Η απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και της Εταιρείας.

►Η απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

►Η απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας επιτρέπεται βάσει του δικαίου στο οποίο υπόκειται η Εταιρεία και το οποίο προβλέπει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων. Ωστόσο, ακόμα και σε αυτή την περίπτωση η Εταιρεία θα πρέπει να παρέχει στο υποκείμενο των δεδομένων τουλάχιστον το δικαίωμα να περιληφθεί ανθρώπινη παρέμβαση, να εκφράσει τη δική του οπτική γωνία ή να αμφισβητήσει την απόφαση.

Βήμα 5ο : Εκτέλεση απαιτούμενων ενεργειών.

Έπειτα από την ολοκλήρωση του ελέγχου βασιμότητας του αιτήματος του υποκειμένου των δεδομένων, η Εταιρεία προχωράει στην εκτέλεση των απαιτούμενων ενεργειών όπως αυτές περιγράφονται παρακάτω.

- Το αίτημα δεν είναι βάσιμο.

Στην περίπτωση κατά την οποία το αίτημα του υποκειμένου των δεδομένων δεν είναι βάσιμο, η Εταιρεία αρνείται την ικανοποίηση του εν λόγω αιτήματος και το ενημερώσει εγγράφως για τους σχετικούς λόγους της άρνησης εντός ενός (1) μήνα από τη λήψη του, κάνοντας χρήση του σχετικού υποδείγματος απαντήσεων σε αιτήματα των υποκειμένων των δεδομένων, που διαθέτει η Εταιρεία.

- Το αίτημα είναι βάσιμο.

Στην περίπτωση κατά την οποία το αίτημα του υποκειμένου των δεδομένων είναι βάσιμο, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) προβαίνει στις ακόλουθες ενέργειες:

►Εντοπισμός της μορφής στην οποία τηρούνται τα σχετικά προσωπικά δεδομένα (έντυπη/ηλεκτρονική μορφή).

►Εντοπισμός του φυσικού μέρους και/ή του ηλεκτρονικού μέσου στο οποίο τηρούνται τα εν λόγω προσωπικά δεδομένα.

►Εντοπισμός άλλου Υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία οι οποίοι επεξεργάζονται τα σχετικά προσωπικά δεδομένα και διαβίβαση του αιτήματος ζητώντας τη συνεργασία τους.

►Συγκέντρωση των απαιτούμενων πληροφοριών, όπως προσωπικά δεδομένα που παρέχονται απευθείας από το υποκείμενο των δεδομένων, δεδομένα που παράγονται με βάση τα πρωτογενή δεδομένα που έχει παράσχει το υποκείμενο των δεδομένων, δεδομένα σε ηλεκτρονική μορφή, δεδομένα σε έντυπη μορφή εφόσον είναι οργανωμένα σε αρχείο και/ή εκτέλεση των απαιτούμενων ενεργειών.

(α) Δικαίωμα ενημέρωσης και πρόσβασης.
Εκτός από τα ίδια τα προσωπικά δεδομένα, οι ακόλουθες πληροφορίες συλλέγονται από τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner) και παρέχονται στο υποκείμενο των δεδομένων:

- ►Οι σκοποί και η νόμιμη βάση επεξεργασίας,
- ►Οι κατηγορίες προσωπικών δεδομένων,
- ►Οι αποδέκτες, συμπεριλαμβανομένων τρίτων χωρών,
- ►Το χρονικό διάστημα αποθήκευσης των προσωπικών δεδομένων,
- ►Η ύπαρξη του δικαιώματος υποβολής αιτήματος για διόρθωση, διαγραφή, περιορισμό της επεξεργασίας,
- ►Η ύπαρξη του δικαιώματος υποβολής καταγγελίας στην Εποπτεύουσα Αρχή,
- ►Η προέλευση των προσωπικών δεδομένων σε περίπτωση που συλλέγονται από τρίτα μέρη,
- ►Τη λήψη αποφάσεων με αυτοματοποιημένα μέσα, συμπεριλαμβανομένης και της κατάρτισης προφίλ,
- ►Την ύπαρξη επαρκών εγγυήσεων για τη διαβίβαση δεδομένων σε τρίτες χώρες.

(β) Δικαίωμα διόρθωσης.
Ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) προχωράει στη διόρθωση των προσωπικών δεδομένων του υποκειμένου των δεδομένων. Στην περίπτωση κατά την οποία η επεξεργασία πραγματοποιείται από εκτελούντα την επεξεργασία, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) διαβιβάζει το αίτημα μαζί με συγκεκριμένες οδηγίες και η διόρθωση γίνεται από τον εκτελούντα την επεξεργασία. Ο εκτελών την επεξεργασία οφείλει να ενημερώνει τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner) ότι τα δεδομένα διορθώθηκαν εντός της ορισμένης προθεσμίας και να παρέχει αντίγραφο των δεδομένων που διορθώθηκαν.

(γ) Δικαίωμα διαγραφής («δικαίωμα στη λήθη»).
Ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) προχωράει στη διαγραφή των προσωπικών δεδομένων του υποκειμένου των δεδομένων, από κάθε πληροφοριακό σύστημα και έντυπο υλικό. Η διαγραφή πραγματοποιείται σύμφωνα με τα περιεχόμενα στο Κεφ. 8 της παρούσας.
Στην περίπτωση κατά την οποία η επεξεργασία πραγματοποιείται από εκτελούντα την επεξεργασία, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) διαβιβάζει το αίτημα μαζί με συγκεκριμένες οδηγίες και η διαγραφή γίνεται από τον εκτελούντα την επεξεργασία. Ο εκτελών την επεξεργασία οφείλει να ενημερώνει τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner) ότι τα δεδομένα διαγράφηκαν εντός ορισμένης προθεσμίας.

(δ) Δικαίωμα περιορισμού της επεξεργασίας.
Στην περίπτωση κατά την οποία αμφισβητείται από το υποκείμενο των δεδομένων η ακρίβεια των προσωπικών του δεδομένων, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) περιορίζει την επεξεργασία των εν λόγω προσωπικών δεδομένων, σε όλα τα πληροφοριακά συστήματα στα οποία πραγματοποιείται επεξεργασία, για το χρονικό διάστημα που απαιτείται για την εξακρίβωση της ακρίβειας των προσωπικών δεδομένων. Για τις λοιπές περιπτώσεις, πραγματοποιείται πλήρης περιορισμός της επεξεργασίας των εν λόγω προσωπικών δεδομένων σε όλα τα πληροφοριακά

συστήματα στα οποία πραγματοποιείται επεξεργασία.
Τα εν λόγω προσωπικά δεδομένα λαμβάνουν κατάλληλη επισήμανση, έτσι ώστε όλα τα τμήματα/διευθύνσεις της Εταιρείας που εμπλέκονται στην επεξεργασία να λαμβάνουν επαρκή ενημέρωση σχετικά με τον περιορισμό.
Τέλος, στην περίπτωση κατά την οποία η επεξεργασία πραγματοποιείται από εκτελούντα την επεξεργασία, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) διαβιβάζει το αίτημα στον εκτελούντα την επεξεργασία προκειμένου να προχωρήσει στον περιορισμό της επεξεργασίας.

(ε) Δικαίωμα στη φορητότητα των δεδομένων.
Ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner), αρχικά εντοπίζει και ανακτά τα προσωπικά δεδομένα του υποκειμένου των δεδομένων και εν συνεχεία τα οργανώνει / αποθηκεύει σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, όπως USB, CD ROM, DVD ROM.
Τα προσωπικά δεδομένα παραδίδονται στο υποκείμενο των δεδομένων χωρίς χρέωση, το οποίο επίσης ενημερώνεται ότι μπορεί να τα διαβιβάσει ελεύθερα σε άλλον υπεύθυνο επεξεργασίας. Εάν είναι εφικτό τεχνικά, η μεταφορά των προσωπικών δεδομένων μπορεί να πραγματοποιηθεί απευθείας σε άλλον υπεύθυνο επεξεργασίας.
Το δικαίωμα στη φορητότητα των δεδομένων περιλαμβάνει προσωπικά δεδομένα που έχουν συλλεγεί απευθείας από το υποκείμενο των δεδομένων αλλά και προσωπικά δεδομένα που προκύπτουν από τη δραστηριότητα του όταν χρησιμοποιεί κάποια υπηρεσία ή συσκευή, όπως γεωφυσική θέση, δεδομένα περιήγησης, κλπ. Ωστόσο, δεν περιλαμβάνονται δεδομένα που προκύπτουν με βάση πρωτογενή δεδομένα που έχει παράσχει το υποκείμενο των δεδομένων, όπως αναλύσεις και αξιολογήσεις.

(στ) Δικαίωμα εναντίωσης.
Ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner), σταματάει την επεξεργασία των προσωπικών δεδομένων του υποκειμένου των δεδομένων. Στην περίπτωση κατά την οποία η επεξεργασία πραγματοποιείται από εκτελούντα την επεξεργασία, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) διαβιβάζει το αίτημα μαζί με συγκεκριμένες οδηγίες και η παύση της επεξεργασίας γίνεται από τον εκτελούντα την επεξεργασία. Ο εκτελών την επεξεργασία οφείλει να ενημερώνει τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner) σχετικά με την παύση της επεξεργασίας εντός ορισμένης προθεσμίας.

(ζ) Δικαίωμα άρνησης υπαγωγής σε αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ.
Ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner), μεριμνά για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε, σε περίπτωση που ζητηθεί από το υποκείμενο των δεδομένων, να μπορεί να εξασφαλίσει ότι η απόφαση που αρχικά λήφθηκε με αυτοματοποιημένα μέσα θα εξεταστεί και από κάποιο φυσικό πρόσωπο. Στην περίπτωση κατά την οποία η επεξεργασία πραγματοποιείται από εκτελούντα την επεξεργασία, ο Υπεύθυνος Δραστηριότητας Επεξεργασίας (Owner) διαβιβάζει το αίτημα μαζί με συγκεκριμένες οδηγίες έτσι ώστε η εξασφάλιση της ανθρώπινης παρέμβασης να γίνει από τον εκτελούντα την επεξεργασία. Ο εκτελών την επεξεργασία οφείλει να ενημερώνει τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner) εντός ορισμένης προθεσμίας ότι η απόφαση που αρχικά λήφθηκε με αυτοματοποιημένα μέσα έχει εξεταστεί από κάποιο φυσικό πρόσωπο.

Βήμα 6ο : Απάντηση στο υποκείμενο των δεδομένων

Έπειτα από την εκτέλεση των απαιτούμενων ενεργειών, οι απαραίτητες πληροφορίες/στοιχεία που συγκεντρώθηκαν προωθούνται από τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner) στον Υπεύθυνο Προστασίας Δεδομένων, ο οποίος είναι υπεύθυνος να απαντήσει στο αίτημα του υποκειμένου των δεδομένων. Σε κάθε περίπτωση η απάντηση παρέχεται το αργότερο εντός ενός (1) μήνα από τη λήψη του αιτήματος και την ταυτοποίηση του υποκειμένου με δυνατότητα παράτασης δύο (2) επιπλέον μηνών σε περίπτωση πολύπλοκων ή πολυάριθμων αιτημάτων.
Η απάντηση αποστέλλεται μέσω των διαθέσιμων καναλιών επικοινωνίας (e-mail, φυσική αποστολή, παραλαβή αυτοπροσώπως, προφορικά εφόσον το ζητήσει το υποκείμενο των δεδομένων), τα οποία έχουν δηλωθεί από το υποκείμενο των δεδομένων στη «Φόρμα Άσκησης Δικαιωμάτων αναφορικά με Προσωπικά Δεδομένα». Η απάντηση παρέχεται χρησιμοποιώντας σαφή και απλή γλώσσα και πάντα στη γλώσσα που χρησιμοποιεί το υποκείμενο των δεδομένων στην αίτησή του, εκτός εάν επιθυμεί κάτι διαφορετικό. Για πρακτικούς λόγους τα υποκείμενα των δεδομένων μπορούν να υποβάλλουν τα αιτήματα τους είτε στα Ελληνικά είτε στα Αγγλικά.

Βήμα 7ο : Ενημέρωση και διατήρηση αρχείου

Ο Υπεύθυνος Προστασίας Δεδομένων είναι υπεύθυνος για την ενημέρωση και τη διατήρηση του «Αρχείου Καταγραφής Αιτημάτων Υποκειμένων των Δεδομένων».

Απαιτούμενο έντυπο για τη διαχείριση των υποβαλλόμενων αιτημάτων των υποκειμένων αποτελεί η Φόρμα Άσκησης Δικαιωμάτων αναφορικά με Προσωπικά Δεδομένα η οποία επισυνάπτεται ως παράρτημα στην Παρούσα.

5. Διαβίβαση προσωπικών δεδομένων σε τρίτα μέρη

5.1 Διαβιβάσεις σε τρίτα μέρη & διασυνοριακές διαβιβάσεις

(α) Τα προσωπικά δεδομένα διαβιβάζονται σε τρίτα μέρη μόνο εφόσον αυτό είναι απαραίτητο. Τα δεδομένα προσωπικού χαρακτήρα ανωνυμοποιούνται, αν αυτό κρίνεται κατάλληλο.
Ένα τρίτο μέρος το οποίο ενεργεί ως εκτελών την επεξεργασία για λογαριασμό της Εταιρείας, π.χ. ανάδοχος ή πάροχος υπηρεσιών, θα πρέπει να δεσμεύεται συμβατικά ότι η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται σύμφωνα με την παρούσα πολιτική, μέσω ρητής αναφοράς στη σχετική σύμβαση.
(β) Τα προσωπικά δεδομένα μπορούν να διαβιβαστούν σε τρίτη χώρα (χώρα εκτός ΕΕ) 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 διαβιβαστούν στη χώρα αυτή μόνον εάν το υποκείμενο στο οποίο αναφέρονται τα δεδομένα έχει συναινέσει ρητά στη μεταφορά ή εάν η προστασία δεδομένων διασφαλίζεται μέσα από κατάλληλη συμφωνία μεταφοράς δεδομένων.

Η Εταιρεία λαμβάνει τα απαραίτητα τεχνικά και οργανωτικά μέτρα για την ελαχιστοποίηση του κινδύνου ακούσιας ή σκόπιμης παραβίασης, καταστροφής ή απώλειας των προσωπικών δεδομένων.

5.2 Διαδικασία αξιολόγησης, επιλογής & διαχείρισης τρίτων μερών.

Η Εταιρεία κατά την εκτέλεση και για την υποστήριξη των επιχειρησιακών λειτουργιών της χρησιμοποιεί εξωτερικούς προμηθευτές/παρόχους, οι οποίοι λειτουργούν ως «εκτελούντες την επεξεργασία» για λογαριασμό της (εφεξής «Τρίτα Μέρη»). Η Εταιρεία έχει αναγνωρίσει τη σπουδαιότητα της ορθής και ασφαλούς επεξεργασίας των προσωπικών δεδομένων η οποία πραγματοποιείται για λογαριασμό της από τα Τρίτα Μέρη και, για το λόγο αυτό, διαθέτει και έχει θέσει σε εφαρμογή ρυθμίσεις και διαδικασίες σχετικά με επιλογή και αξιολόγηση Τρίτων Μερών.

5.2.1 Επεξεργασία προσωπικών δεδομένων από Τρίτα Μέρη (Εκτελούντες την Επεξεργασία)

Στις περιπτώσεις κατά τις οποίες η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό της Εταιρείας από Τρίτο Μέρος, η Εταιρεία χρησιμοποιεί Τρίτα Μέρη τα οποία παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων μέτρων ώστε η επεξεργασία να πληροί τις απαιτήσεις του ΓΚΠΔ και να διασφαλίζεται η προστασία των δικαιωμάτων των υποκειμένων των δεδομένων.

Σε καμία περίπτωση το Τρίτο Μέρος δεν προσλαμβάνει άλλο τρίτο μέρος (εφεξής «υπεργολάβο») προκειμένου να εκτελέσει την εν λόγω επεξεργασία, χωρίς την προηγούμενη ειδική ή γενική γραπτή άδεια της Εταιρείας. Σε περίπτωση γενικής γραπτής άδειας, το Τρίτο Μέρος ενημερώνει την Εταιρεία για τυχόν σκοπούμενες αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση υπεργολάβων, παρέχοντας με τον τρόπο αυτό τη δυνατότητα στην Εταιρεία να αντιταχθεί στις αλλαγές αυτές.

Η επεξεργασία από το Τρίτο Μέρος διέπεται από γραπτή σύμβαση ή άλλη νομική πράξη, η οποία δεσμεύει το Τρίτο Μέρος σε σχέση με την Εταιρεία και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και το σκοπό της επεξεργασίας, το είδος των προσωπικών δεδομένων και τις κατηγορίες των υποκειμένων των δεδομένων καθώς και τις υποχρεώσεις και τα δικαιώματα της Εταιρείας, σύμφωνα με τα ειδικότερα προβλεπόμενα στον ΓΚΠΔ. Στις περιπτώσεις κατά τις οποίες το Τρίτο Μέρος προσλαμβάνει υπεργολάβο για τη διενέργεια συγκεκριμένων δραστηριοτήτων επεξεργασίας για λογαριασμό της Εταιρείας, οι ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων που προβλέπονται στη σύμβαση ή στην άλλη νομική πράξη μεταξύ της Εταιρείας και του Τρίτου Μέρους επιβάλλονται και στον υπεργολάβο μέσω σχετικής σύμβασης ή άλλης νομικής πράξης. Όταν ο υπεργολάβος αδυνατεί να ανταποκριθεί στις σχετικές με την προστασία των δεδομένων υποχρεώσεις του, το Τρίτο Μέρος παραμένει πλήρως υπόλογο έναντι της Εταιρείας σχετικά με την εκπλήρωση των υποχρεώσεων του υπεργολάβου.

Τέλος, το Τρίτο Μέρος καθώς και κάθε πρόσωπο που ενεργεί υπό την εποπτεία της Εταιρείας ή του Τρίτου Μέρους και το οποίο έχει πρόσβαση σε προσωπικά δεδομένα, επεξεργάζεται τα εν λόγω δεδομένα μόνον κατ' εντολή της Εταιρείας εκτός εάν υπάρχει σχετική νομική / κανονιστική υποχρέωση.

5.2.2 Διαδικασία αξιολόγησης, επιλογής και διαχείρισης Τρίτων Μερών (Εκτελούντες της επεξεργασία)

Η αξιολόγηση, επιλογή και διαχείριση των Τρίτων Μερών πραγματοποιείται από την Εταιρεία ακολουθώντας τα παρακάτω βήματα:

- ►Βήμα 1: Αξιολόγηση και Επιλογή Τρίτου Μέρους
- ►Βήμα 2: Έναρξη της συμβατικής σχέσης.

► Βήμα 3: Ενέργειες κατά τη διάρκεια της συμβατικής σχέσης.
► Βήμα 4: Ενέργειες στη λήξη της συμβατικής σχέσης.

Βήμα 1ο: Αξιολόγηση και επιλογή Τρίτου Μέρους
Η συγκεκριμένη ενέργεια πραγματοποιείται από τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner), υπό τη γενικότερη επίβλεψη και καθοδήγηση του Υπευθύνου Προστασίας Δεδομένων, όπου απαιτείται. Η επιλογή του Τρίτου Μέρους πραγματοποιείται λαμβάνοντας υπόψη το επίπεδο συμμόρφωσής του με τον ΓΚΠΔ καθώς και την εφαρμογή όλων των απαιτούμενων μέτρων για τη διασφάλιση της ασφάλειας και της προστασίας των προσωπικών δεδομένων. Όπου είναι εφικτό, προτεραιότητα δίνεται σε Τρίτα Μέρη τα οποία μπορούν να επεξεργάζονται τα προσωπικά δεδομένα εντός Ε.Ε.
Κατά το στάδιο αυτό, κανένα προσωπικό δε μεταφέρεται/διαβιβάζεται σε οποιοδήποτε Τρίτο Μέρος.
Τα μόνα δεδομένα που μπορούν να μεταφερθούν / διαβιβαστούν είναι ανωνυμοποιημένα δεδομένα.

Βήμα 2ο : Έναρξη της συμβατικής σχέσης
Έπειτα από την επιλογή του Τρίτου Μέρους, το επόμενο βήμα περιλαμβάνει τη σύναψη της συμβατικής σχέσης. Η συγκεκριμένη ενέργεια πραγματοποιείται από τους νομίμους εκπροσώπους της Εταιρείας, κατόπιν ελέγχου που πραγματοποιείται από τον Νομικό Σύμβουλο με τη συνδρομή ως προς το επιχειρηματικό τμήμα του Υπεύθυνου Δραστηριότητας Επεξεργασίας (Owner), υπό τη γενικότερη επίβλεψη και καθοδήγηση του Υπευθύνου Προστασίας Δεδομένων.
Η επεξεργασία των προσωπικών δεδομένων από το Τρίτο Μέρος πραγματοποιείται σύμφωνα με τα όσα περιγράφονται στην παρούσα και διέπεται από γραπτή σύμβαση ή άλλη νομική πράξη, η οποία συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ.
Για το συγκεκριμένο σκοπό, χρησιμοποιούνται οι τυποποιημένες ρήτρες συμφωνητικού επεξεργασίας προσωπικών δεδομένων, οι οποίες έχουν δημιουργηθεί από τον Νομικό Σύμβουλο της Εταιρείας.
Σε περίπτωση που τα προσωπικά δεδομένα διαβιβάζονται σε Τρίτο Μέρος εκτός Ε.Ε. ή σε συνδεδεμένες με το Τρίτο Μέρος εταιρίες (π.χ. υπεργολάβους, συμβούλους) εκτός Ε.Ε., η διαβίβαση καλύπτεται από κατάλληλους μηχανισμούς νόμιμης διαβίβασης, όπως τυποποιημένες συμβατικές ρήτρες που έχουν καθοριστεί από την Ευρωπαϊκή Επιτροπή. Ο μηχανισμός νόμιμης διαβίβασης πρέπει να υπάρχει και να τίθεται σε εφαρμογή πριν από την πραγματοποίηση οποιασδήποτε διαβίβασης.
Οι τυποποιημένες συμβατικές ρήτρες ή/και οι άλλοι μηχανισμοί νόμιμης διαβίβασης θα πρέπει να διανεμηθούν και στα άλλα τρίτα μέρη (π.χ. υπεργολάβους), τα οποία χρησιμοποιούνται από το Τρίτο Μέρος. Όπου αυτό δεν είναι δυνατό, η Εταιρεία διατηρεί το δικαίωμα να αξιολογεί και να απαγορεύει τη χρήση υπεργολάβων από το Τρίτο Μέρος όταν υπάρχει κίνδυνος για την προστασία των προσωπικών δεδομένων. Έπειτα από την ολοκλήρωση του σταδίου αυτού, τα προσωπικά δεδομένα μπορούν να διαβιβαστούν στο Τρίτο Μέρος.

Βήμα 3ο : Ενέργειες κατά τη διάρκεια της συμβατικής σχέσης
Η συμμόρφωση του Τρίτου Μέρους με τις συμβατικές ρήτρες επεξεργασίας προσωπικών δεδομένων ελέγχεται σε περιοδική βάση καθ' όλη τη διάρκεια της συμβατικής σχέσης. Η συγκεκριμένη ενέργεια πραγματοποιείται από τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner), υπό τη γενικότερη επίβλεψη και καθοδήγηση του Υπευθύνου Προστασίας Δεδομένων.

Οι έλεγχοι διακρίνονται σε τακτικούς (π.χ. ετήσιους) καθώς και σε κατά περίπτωση (ad-hoc) και περιλαμβάνουν διάφορες μορφές, όπως:

- ►Αποστολή και συμπλήρωση ερωτηματολογίου από το Τρίτο Μέρος.
- ►Επιτόπιους ελέγχους στις εγκαταστάσεις του Τρίτου Μέρους από εργαζόμενους της Εταιρείας.
- ►Ελέγχους από εξωτερικό ελεγκτή εντεταλμένο από την Εταιρεία.
- ►Εξέταση εγκυρότητας και ισχύος πιστοποιητικών (π.χ. πιστοποίηση ISO) του Τρίτου Μέρους. Σε περίπτωση διαπίστωσης περιστατικών μη συμμόρφωσης ήσσονος και μέσης σημασίας, η Εταιρεία αρχικά προχωράει σε σχετικές συστάσεις προς το Τρίτο Μέρος προκειμένου αυτό να προχωρήσει στη διόρθωσή τους. Εάν το Τρίτο Μέρος δεν προβεί στη διόρθωσή τους εντός εύλογου χρονικού διαστήματος τότε η Εταιρεία προχωράει σε περαιτέρω ενέργειες, οι οποίες ενδέχεται να φτάσουν και μέχρι την καταγγελία της σύμβασης.

Σε περίπτωση διαπίστωσης σοβαρών περιστατικών μη συμμόρφωσης από την πλευρά του Τρίτου Μέρους, οι οποίες θέτουν σε σοβαρό κίνδυνο την ασφάλεια και την προστασία των προσωπικών δεδομένων, η Εταιρεία προχωράει άμεσα στην καταγγελία της σύμβασης.

Βήμα 4ο : Ενέργειες στη λήξη της συμβατικής σχέσης

Σε κάθε περίπτωση λήξης συνεργασίας με Τρίτο Μέρος, η Εταιρεία εφαρμόζει όλες τις απαραίτητες ενέργειες προκειμένου να διασφαλιστεί η άμεση και οριστική διακοπή της επεξεργασίας των προσωπικών δεδομένων από το Τρίτο Μέρος. Οι συγκεκριμένες ενέργειες πραγματοποιούνται το αργότερο κατά τη λήξη της σύμβασης ή όταν τεθεί σε ισχύ η καταγγελία της σύμβασης και περιλαμβάνουν ενδεικτικά και όχι περιοριστικά:

- ►Διασφάλιση ασφαλούς επιστροφής του συνόλου των προσωπικών δεδομένων από το Τρίτο Μέρος στην Εταιρεία.
- ►Διασφάλιση ασφαλούς καταστροφής του συνόλου των προσωπικών δεδομένων από το Τρίτο Μέρος.
- ►Απενεργοποίηση των δικαιωμάτων πρόσβασης τα οποία έχουν χορηγηθεί από την Εταιρεία στο Τρίτο Μέρος.

Οι παραπάνω ενέργειες πραγματοποιούνται από τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner), υπό τη γενικότερη επίβλεψη και καθοδήγηση του Υπευθύνου Προστασίας Δεδομένων.

6. Παραβίαση προσωπικών δεδομένων

6.1 Διαπίστωση και γνωστοποίηση περιστατικών παραβίασης προσωπικών δεδομένων

Κάθε παράβαση της παρούσας πολιτικής καθώς και των σχετικών νόμων και κανονισμών περί προστασίας προσωπικών δεδομένων συνιστούν παραβίαση προσωπικών δεδομένων. Ενδεικτικά παραδείγματα αποτελούν η παράνομη καταστροφή, η απώλεια, η αλλοίωση, η μη εξουσιοδοτημένη διαβίβαση / πρόσβαση, καθώς και η επεξεργασία δεδομένων χωρίς τη συγκατάθεση του υποκειμένου ή για σκοπούς διαφορετικούς από εκείνους που δηλώθηκαν κατά τη στιγμή της συλλογής τους.

Το πρόσωπο, από το προσωπικό της Εταιρείας που ανακαλύπτει την παραβίαση προσωπικών δεδομένων λαμβάνει τα κατάλληλα μέτρα προκειμένου να προστατεύσει τα προσωπικά δεδομένα από περαιτέρω αντίκτυπο και να αναφέρει άμεσα και χωρίς αδικαιολόγητη καθυστέρηση την παραβίαση στον Υπεύθυνο Προστασίας Δεδομένων.

Ο Υπεύθυνος Προστασίας Δεδομένων παρακολουθεί και καταγράφει συστηματικά τις παραβιάσεις προσωπικών δεδομένων, ενώ παράλληλα αξιολογεί τους λόγους των παραβιάσεων. Επιπλέον, ο Υπεύθυνος Προστασίας Δεδομένων θέτει σε εφαρμογή πρόσθετα μέτρα που απαιτούνται για την αποκατάσταση του περιστατικού παραβίασης και την αποτροπή της επανάληψης παραβιάσεων.

6.2 Παραβίαση προσωπικών δεδομένων

Η παραβίαση προσωπικών δεδομένων αφορά αρχεία τόσο σε ηλεκτρονική όσο και σε έντυπη μορφή.
Παραδείγματα περιστατικών παραβίασης:

- ►Χαμένο USB stick ή μονάδα δίσκου.
- ►Κλεμμένος φορητός υπολογιστής.
- ►Ηλεκτρονική πειρατεία (Computer hacking).
- ►Μόλυνση κακόβουλου λογισμικού (malware infection).
- ►Καταστροφή, όπως πυρκαγιά σε ένα κέντρο δεδομένων (data center).
- ►Αποστολή ηλεκτρονικού μηνύματος μάρκετινγκ σε μεγάλο αριθμό πελατών με όλα τα ονόματα των παραληπτών αναγνώσιμα.
- ►Χαμένη ή κλεμμένη βάση δεδομένων πελατών της Εταιρείας.

6.2.1 <u>Γνωστοποίηση στην Εποπτεύουσα Αρχή.</u>

Στις περιπτώσεις κατά τις οποίες η παραβίαση των προσωπικών δεδομένων ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η Εταιρεία ενημερώνει την Εποπτεύουσα Αρχή (για την Ελλάδα, Αρχή προστασίας Δεδομένων προσωπικού Χαρακτήρα- «ΑΠΔΠΧ») χωρίς αδικαιολόγητη καθυστέρηση και, εάν είναι εφικτό, το αργότερο εντός 72 ωρών από τη στιγμή που έχει λάβει γνώση της παραβίασης των προσωπικών δεδομένων. Σε περίπτωση όπου η γνωστοποίηση δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Σε περίπτωση όπου η επεξεργασία πραγματοποιείται από τρίτο μέρος (εκτελών την επεξεργασία), ο εκτελών την επεξεργασία ενημερώνει την Εταιρεία χωρίς αδικαιολόγητη καθυστέρηση, αμέσως μόλις αντιληφθεί παραβίαση προσωπικών δεδομένων. Οι σχετικές υποχρεώσεις καθορίζονται στις συμβάσεις μεταξύ της Εταιρείας και του εκάστοτε εκτελούντος την επεξεργασία.
Η γνωστοποίηση της παραβίασης των προσωπικών δεδομένων στην Εποπτεύουσα Αρχή αποτελεί υποχρέωση της Εταιρείας. Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν όλες οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά, χωρίς αδικαιολόγητη καθυστέρηση. Η γνωστοποίηση περιλαμβάνει κατ' ελάχιστο τις προβλεπόμενες στον ΓΚΠΔ πληροφορίες:

Η γνωστοποίηση της παραβίασης των προσωπικών δεδομένων στην Εποπτεύουσα Αρχή πραγματοποιείται από τον Υπεύθυνο Προστασίας Δεδομένων, μέσω της χρησιμοποίησης της πρότυπης φόρμας γνωστοποίησης της Εποπτεύουσας Αρχής.
Παραδείγματα πιθανών περιστατικών παραβίασης και αξιολόγηση ανάγκης γνωστοποίησης στην Εποπτεύουσα Αρχή:

- ►Ένα περιστατικό παραβίασης κατά το οποίο μεγάλος αριθμός προσωπικών δεδομένων κοινολογήθηκε σε μη εξουσιοδοτημένα τρίτα μέρη, αποτελεί παραβίαση προσωπικών δεδομένων

και θα πρέπει να γνωστοποιηθεί στην Εποπτεύουσα Αρχή.

►Η προσωρινή απώλεια της διαθεσιμότητας η οποία δεν επιτρέπει στην Εταιρεία να στείλει ενημερωτικά δελτία (newsletters) δεν αποτελεί παραβίαση προσωπικών δεδομένων και δε θα πρέπει να γνωστοποιηθεί στην Εποπτεύουσα Αρχή.

6.2.2 Ανακοίνωση στα υποκείμενα των δεδομένων.

Στις περιπτώσεις κατά τις οποίες η παραβίαση των προσωπικών δεδομένων ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η Εταιρεία ανακοινώνει αμελλητί την παραβίαση των προσωπικών δεδομένων στα υποκείμενα των δεδομένων.

Η ανακοίνωση της παραβίασης των προσωπικών δεδομένων προς τα υποκείμενα των δεδομένων περιλαμβάνει κατ' ελάχιστο τις προβλεπόμενες στον ΓΚΠΔ πληροφορίες.

Στις περιπτώσεις κατά τις οποίες η Εταιρεία κρίνει ότι απαιτείται η ανακοίνωση της παραβίασης των προσωπικών δεδομένων προς τα υποκείμενα των δεδομένων, η ανακοίνωση πραγματοποιείται από τον Υπεύθυνο Προστασίας Δεδομένων. Επιπλέον, ακόμα και αν η Εταιρεία κρίνει ότι η παραβίαση των προσωπικών δεδομένων δεν είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, η Εποπτεύουσα Αρχή, αφού ενημερωθεί, μπορεί να έχει διαφορετική άποψη και να ζητήσει από την Εταιρεία να ενημερώσει τα υποκείμενα των δεδομένων.

Τα μέσα επικοινωνίας που χρησιμοποιούνται για την ανακοίνωση της παραβίασης των προσωπικών δεδομένων προς τα υποκείμενα των δεδομένων, εξαρτώνται από διάφορους παράγοντες όπως, την κατηγορία των επηρεαζόμενων υποκειμένων των δεδομένων, τον αριθμό / όγκο των επηρεαζόμενων υποκειμένων των δεδομένων και τη σοβαρότητα της παραβίασης. Ενδεικτικά και όχι περιοριστικά μπορούν να χρησιμοποιηθούν μηνύματα ηλεκτρονικού ταχυδρομείου, SMS, ταχυδρομική επικοινωνία, κλπ. Τα άμεσα μηνύματα προτιμώνται εκτός εάν συνεπάγονται δυσανάλογη προσπάθεια, οπότε χρησιμοποιούνται άλλες μέθοδοι επικοινωνίας, όπως δημόσια ανακοίνωση, προκειμένου τα υποκείμενα των δεδομένων να ενημερωθούν με εξίσου αποτελεσματικό τρόπο.

Παραδείγματα πιθανών περιστατικών παραβίασης και αξιολόγηση ανάγκης ανακοίνωσης στα υποκείμενα των δεδομένων:

►Η αποκάλυψη του ονόματος ενός υποκειμένου των δεδομένων υπό κανονικές συνθήκες είναι απίθανο να προκαλέσει υψηλό κίνδυνο και ως εκ τούτου δεν απαιτείται σχετική ανακοίνωση. Ωστόσο, εάν το όνομα σε συνδυασμό με τη διεύθυνση ενός θετού γονέα αποκαλυφθούν σε ένα φυσικό γονέα, οι συνέπειες θα μπορούσαν να είναι πολύ σοβαρές τόσο για το θετό γονέα όσο και για το παιδί και ως εκ τούτου απαιτείται σχετική ανακοίνωση.

►Παραβιάσεις οι οποίες περιλαμβάνουν έγγραφα ταυτότητας ή οικονομικά στοιχεία, όπως στοιχεία πιστωτικής κάρτας, μπορούν να προκαλέσουν υψηλό κίνδυνο στα υποκείμενα των δεδομένων. Ως εκ τούτου, απαιτείται σχετική ανακοίνωση (βλ. περαιτέρω εδάφιο 5 κατωτέρω).

6.3 Διαδικασία διαχείρισης περιστατικών παραβίασης προσωπικών δεδομένων

Οι παραβιάσεις προσωπικών δεδομένων μπορεί να προκληθούν από διάφορους παράγοντες, να προέρχονται από διαφορετικές πηγές, να επηρεάσουν διαφορετικές κατηγορίες προσωπικών δεδομένων και να προκαλέσουν μια σειρά πραγματικών ή πιθανών κινδύνων τόσο για την Εταιρεία όσο και για τα υποκείμενα των δεδομένων. Ως εκ τούτου, δεν υπάρχει ένας μοναδικός τρόπος διαχείρισης και ανταπόκρισης για τις παραβιάσεις προσωπικών δεδομένων.
Κάθε περιστατικό παραβίασης εξετάζεται και αντιμετωπίζεται κατά περίπτωση, ακολουθώντας τα παρακάτω εννιά βασικά βήματα:

Βήμα 1ο : Εντοπισμός περιστατικού παραβίασης και εσωτερική επικοινωνία. Ένα περιστατικό παραβίασης μπορεί να εντοπιστεί με διάφορους τρόπους, όπως:

- ►Εντοπισμός εσωτερικά μέσω μηχανισμών/δικλείδων ασφαλείας (controls) οι οποίες εφαρμόζονται από την Εταιρεία.
- ►Τυχαίος εντοπισμός από εργαζόμενο της Εταιρείας.
- ►Εντοπισμός από συνεργαζόμενο τρίτο μέρος το οποίο εμπλέκεται στην επεξεργασία των προσωπικών δεδομένων.
- ►Εντοπισμός έπειτα από σχετική επικοινωνία των υποκειμένων των δεδομένων με την Εταιρεία.
- ►Εντοπισμός έπειτα από σχετική ανακοίνωση σε μέσα μαζικής ενημέρωσης.

Κάθε περιστατικό παραβίασης επικοινωνείται άμεσα και χωρίς αδικαιολόγητη καθυστέρηση στον Υπεύθυνο Προστασίας Δεδομένων. Σε περίπτωση που η επεξεργασία πραγματοποιείται από τρίτο μέρος (εκτελών την επεξεργασία), η επικοινωνία του περιστατικού παραβίασης πραγματοποιείται άμεσα από τον εκτελούντα την επεξεργασία και σε κάθε περίπτωση εντός του διαστήματος όπως αυτό ορίζεται στη σχετική σύμβαση.

Βήμα 2ο : Αξιολόγηση περιστατικού παραβίασης
Έπειτα από τον εντοπισμό, ο Υπεύθυνος Προστασίας Δεδομένων προχωράει στην αξιολόγηση του περιστατικού προκειμένου να καθορίσει αρχικά το κατά πόσο αποτελεί παραβίαση προσωπικών δεδομένων και εν συνεχεία τη σχετική έκταση της παραβίασης.
Κατά το στάδιο αυτό ο Υπεύθυνος Προστασίας Δεδομένων συγκεντρώνει, σε συνεργασία με τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner) όλη την απαραίτητη πληροφορία, εξετάζοντας τα ακόλουθα αρχικά ερωτήματα:

- ►Περιλαμβάνει η παραβίαση προσωπικά δεδομένα;
- ►Ποιες κατηγορίες προσωπικών δεδομένων περιλαμβάνει η παραβίαση;
- ►Ποια είναι η έκταση της παραβίασης;
- ►Ποιος είναι ο κατά προσέγγιση αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων;
- ►Ποιες είναι οι ενδεχόμενες συνέπειες και ο βαθμός του κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων από την παραβίαση;
- ►Ποια ήταν η αιτία και η φύση του συμβάντος / της παραβίασης;

Σε περίπτωση όπου επιβεβαιωθεί η παραβίαση των προσωπικών δεδομένων, ο Υπεύθυνος Προστασίας Δεδομένων χρησιμοποιεί την παραπάνω πληροφορία που συγκεντρώθηκε προκειμένου να αξιολογήσει το περιστατικό παραβίασης και να καθορίσει:

- ►Τα απαραίτητα τεχνικά και οργανωτικά μέτρα προκειμένου αρχικά να περιοριστεί και εν

συνεχεία να αντιμετωπιστεί το περιστατικό της παραβίασης,

►το κατά πόσο απαιτείται η γνωστοποίηση της παραβίασης των προσωπικών δεδομένων στην Εποπτεύουσα Αρχή,

►το κατά πόσο απαιτείται η ανακοίνωση της παραβίασης των προσωπικών δεδομένων προς τα υποκείμενα των δεδομένων,

►το κατά πόσο απαιτείται η εμπλοκή της Διοίκησης, επιπλέον διευθύνσεων / τμημάτων της Εταιρείας καθώς και εξωτερικών εμπειρογνωμόνων (subject matter experts).

Η αξιολόγηση του περιστατικού παραβίασης ολοκληρώνεται το αργότερο εντός 24 ωρών από τη λήψη της σχετικής ενημέρωσης και σε καμιά περίπτωση δεν ξεπερνά τις 48 ώρες από τη στιγμή του εντοπισμού της παραβίασης.

Βήμα 3ο : Περιορισμός περιστατικού παραβίασης

Έπειτα από την αξιολόγηση του περιστατικού παραβίασης, ο Υπεύθυνος Προστασίας Δεδομένων προχωράει στην παροχή συστάσεων και υποστήριξης προς τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner), προκειμένου να εφαρμοστούν τα απαραίτητα μέτρα για τον περιορισμό της παραβίασης.

Τα εν λόγω μέτρα εφαρμόζονται κατά περίπτωση, ανάλογα με τα ιδιαίτερα χαρακτηριστικά του εκάστοτε περιστατικού παραβίασης, και μπορεί να περιλαμβάνουν ενδεικτικά και όχι περιοριστικά:

►Απενεργοποίηση συστήματος,

►αποσύνδεση συστήματος από το δίκτυο,

►συνέχιση των εργασιών και παρακολούθηση δραστηριότητας,

►παύση εξερχόμενης επικοινωνίας από το «μολυσμένο» (infected) μηχάνημα,

►αποκλεισμό εισερχόμενης κίνησης,

►μετάβαση σε δευτερεύον κέντρο δεδομένων (secondary data center).

Τα μέτρα για τον περιορισμό της παραβίασης εφαρμόζονται υπό τη γενικότερη επίβλεψη και καθοδήγηση του Υπευθύνου Προστασίας Δεδομένων και μόνο κατόπιν χορήγησης σχετικής του έγκρισης.

Βήμα 4ο : Διαμόρφωση πλάνου επίλυσης περιστατικού παραβίασης

Έπειτα από τον αρχικό περιορισμό του περιστατικού παραβίασης, ο Υπεύθυνος Προστασίας Δεδομένων προχωράει στη διαμόρφωση του πλάνου επίλυσης του περιστατικού παραβίασης, σε συνεργασία με τον αντίστοιχο Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner). Το πλάνο επίλυσης περιλαμβάνει τις ενέργειες που πρέπει να πραγματοποιηθούν και εγκρίνεται από τον Υπεύθυνο Προστασίας Δεδομένων.

Βήμα 5ο : Γνωστοποίηση περιστατικού παραβίασης στην Εποπτεύουσα Αρχή

Παράλληλα με τον περιορισμό και τη διαμόρφωση του πλάνου επίλυσης του περιστατικού παραβίασης, και εφόσον κατόπιν της σχετικής αξιολόγησης κριθεί ότι απαιτείται η γνωστοποίηση της παραβίασης των προσωπικών δεδομένων, η Εταιρεία προχωρά στην παροχή όλων των απαραίτητων πληροφοριών προς την Εποπτεύουσα Αρχή, μέσω της φόρμας γνωστοποίησης περιστατικών παραβίασης που αναφέρεται υπό 6.4.

Η γνωστοποίηση της παραβίασης των προσωπικών δεδομένων στην Εποπτεύουσα Αρχή πραγματοποιείται από τον Υπεύθυνο Προστασίας Δεδομένων, το αργότερο εντός 72 ωρών από τη στιγμή

που έχει λάβει γνώση της παραβίασης των προσωπικών δεδομένων. Σε περίπτωση όπου η γνωστοποίηση δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.
Η γνωστοποίηση πραγματοποιείται μέσω της συμπλήρωσης και αποστολής της πρότυπης φόρμας γνωστοποίησης της Εποπτεύουσας Αρχής, με τη χρήση των σχετικών προδιαμορφωμένων εντύπων.

Βήμα 6ο : Ανακοίνωση περιστατικού παραβίασης στα υποκείμενα των δεδομένων
Παράλληλα με τον περιορισμό και τη διαμόρφωση του πλάνου επίλυσης του περιστατικού παραβίασης και εφόσον κατόπιν της σχετικής αξιολόγησης κριθεί ότι απαιτείται η ανακοίνωση της παραβίασης των προσωπικών δεδομένων, η Εταιρεία προχωρά στην παροχή όλων των απαραίτητων πληροφοριών προς τα υποκείμενα των δεδομένων.
Η ανακοίνωση πραγματοποιείται από τον Υπεύθυνο Προστασίας Δεδομένων.

Βήμα 7ο : Καταγραφή περιστατικού παραβίασης

- Έπειτα από την ολοκλήρωση των παραπάνω ενεργειών, ο Υπεύθυνος Προστασίας Δεδομένων καταγράφει τις λεπτομέρειες για κάθε περιστατικό παραβίασης προσωπικών δεδομένων ξεχωριστά, σε σχετικό αρχείο καταγραφής περιστατικών παραβίασης.
- Το αρχείο καταγραφής περιστατικών παραβίασης περιλαμβάνει πληροφορίες όπως:
- Ημερομηνία και ώρα έναρξης / λήξης της παραβίασης,
- ημερομηνία και ώρα κατά την οποία εντοπίστηκε η παραβίαση,
- περιγραφή της παραβίασης και της έκτασής της,
- κατηγορίες προσωπικών δεδομένων που περιλαμβάνονταν στην παραβίαση,
- αριθμό εμπλεκόμενων υποκειμένων των δεδομένων,
- ενδεχόμενες συνέπειες και βαθμό κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων από την παραβίαση,
- ποια ήταν η αιτία και η φύση του συμβάντος / της παραβίασης,
- μέτρα / ενέργειες οι οποίες λήφθηκαν για τον περιορισμό και την επίλυση της παραβίασης,
- αξιολόγηση του κατά πόσο ήταν απαραίτητη και πραγματοποιήθηκε η γνωστοποίηση της παραβίασης στην Εποπτεύουσα Αρχή καθώς και η ανακοίνωση της παραβίασης στα υποκείμενα των δεδομένων,
- Κατάσταση (status) του πλάνου επίλυσης της παραβίασης.
  Η καταγραφή των περιστατικών παραβίασης επιτρέπει στην Εταιρεία να είναι σε θέση να απαντά έγκαιρα και αποτελεσματικά σε ερωτήσεις των υποκειμένων των δεδομένων, της Εποπτεύουσας Αρχής καθώς και της κοινής γνώμης, εφόσον αυτό χρειαστεί.

Βήμα 8ο : Παρακολούθηση πλάνου επίλυσης περιστατικού παραβίασης
Το πλάνο επίλυσης του περιστατικού παραβίασης ενδέχεται να περιλαμβάνει βραχυπρόθεσμες και μακροπρόθεσμες ενέργειες οι οποίες απαιτούνται προκειμένου να εξασφαλιστεί η πλήρης επίλυση, να επιτευχθεί η πλήρης ανάκαμψη και να μειωθεί η πιθανότητα νέας εμφάνισης ίδιου τύπου περιστατικού παραβίασης στο μέλλον.
Η παρακολούθηση της αποτελεσματικής εκτέλεσης και ολοκλήρωσης του πλάνου επίλυσης του περιστατικού παραβίασης πραγματοποιείται σε τακτά προκαθορισμένα διαστήματα από τον Υπεύθυνο Προστασίας Δεδομένων.

Βήμα 9ο : Ολοκλήρωση πλάνου επίλυσης περιστατικού παραβίασης (κλείσιμο περιστατικού)
Το πλάνο επίλυσης του περιστατικού παραβίασης θεωρείται ολοκληρωμένο μόνο μετά την ολοκλήρωση όλων των απαραίτητων ενεργειών. Η πιστοποίηση της επιτυχούς ολοκλήρωσης του πλάνου επίλυσης πραγματοποιείται από τον Υπεύθυνο Προστασίας Δεδομένων. Έπειτα από την επιτυχή ολοκλήρωση, ο Υπεύθυνος Προστασίας Δεδομένων επικαιροποιεί την κατάσταση (status) του πλάνου επίλυσης της παραβίασης στο αρχείο καταγραφής περιστατικών παραβίασης.

6.4 Φόρμα γνωστοποίησης περιστατικών παραβίασης στην Εποπτεύουσα Αρχή

Για τη γνωστοποίηση περιστατικού παραβίασης στην Εποπτεύουσα Αρχή, ο Υπεύθυνος Προστασίας Δεδομένων συμπληρώνει ειδική φόρμα, με βάση τις προδιαγραφές της ΑΠΔΠΧ και την υποβάλει ηλεκτρονικά, μέσω της αποστολής της στην ηλεκτρονική διεύθυνση: databreach@dpa.gr
Η φόρμα μπορεί να υποβληθεί με άλλο τρόπο (π.χ. με φυσική υποβολή) μόνο σε εξαιρετική περίπτωση και σε αυτήν την περίπτωση θα πρέπει να τεκμηριώνεται επαρκώς ο λόγος που δεν προτιμήθηκε η ηλεκτρονική υποβολή.

6.5 Χρήση συστήματος μαγνητοσκόπησης

Στα πλαίσια της παρούσας πολιτικής γίνεται ειδική αναφορά στη συλλογή, επεξεργασία και αποθήκευση δεδομένων με τη χρήση συστήματος μαγνητοσκόπησης, ήτοι ενός συστήματος μόνιμα εγκατεστημένου στο χώρο που λειτουργεί συνεχώς ή τακτικά η Εταιρεία και έχει τη δυνατότητα λήψης και μετάδοσης σήματος εικόνας ή και ήχου από το χώρο αυτό προς περιορισμένο, συγκεκριμένο αριθμό οθονών προβολής ή μηχανημάτων καταγραφής.
Η Εταιρεία λαμβάνει όλα τα απαραίτητα μέτρα προκειμένου να εξασφαλίσει ότι η συλλογή, επεξεργασία και αποθήκευση δεδομένων με τη χρήση συστήματος μαγνητοσκόπησης πληροί όλες τις απαιτούμενες εκ του νόμου προϋποθέσεις ώστε να είναι νόμιμη, να περιορίζεται αποκλειστικά στους σκοπούς της επεξεργασίας, να μην οδηγεί σε παραβίαση της προστασίας των υποκειμένων και να τηρείται μόνο για όσο χρόνο κρίνεται απαραίτητη.

6.5.1 Σκοπός της επεξεργασίας

Η επεξεργασία δεδομένων που συλλέγονται με τη χρήση συστήματος μαγνητοσκόπησης αποσκοπεί στην προστασία προσώπων και αγαθών, που με τη σειρά της εκπορεύεται από την υποχρέωση της Εταιρείας και, ταυτόχρονα, το έννομο συμφέρον αυτής να προστατεύσει το χώρο των εγκαταστάσεών της από παράνομες και κακόβουλες πράξεις και να λάβει μέτρα για την ασφάλεια της ζωής, της σωματικής ακεραιότητας, της υγείας και της περιουσίας της ιδίας και παντός προσώπου που εργάζεται ή παρευρίσκεται στους χώρους αυτούς.
Η εν λόγω επεξεργασία επιδιώκει να προασπίσει έννομα συμφέροντα της Εταιρείας και, εκ του λόγου τούτου, θεωρείται ότι δεν απαιτείται προηγούμενη συγκατάθεση από τα υποκείμενα της επεξεργασίας. Περαιτέρω, με τη λήψη όλων των απαιτούμενων μέτρων η Εταιρεία διασφαλίζει ότι έναντι των έννομων συμφερόντων της δε θίγονται και δεν υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων, έτσι ώστε η προστασία τους να απαιτεί την προηγούμενη συγκατάθεση των υποκειμένων.

6.5.2 Αρχές επεξεργασίας δεδομένων

Όπως εκτενώς διαλαμβάνεται στο κεφάλαιο ΙΙ της παρούσας, η επεξεργασία δεδομένων που συλλέγονται με χρήση συστήματος μαγνητοσκόπησης διέπεται από τις αρχές επεξεργασίας δεδομένων και, επιπλέον, εφαρμόζονται τα εξής:

- Το σύστημα μαγνητοσκόπησης χρησιμοποιείται στο έκταση και στο μέτρο που παραμένει πρόσφορο και αναγκαίο για την επίτευξη του επιδιωκόμενου σκοπού, ο οποίος δε μπορεί να επιτευχθεί με ηπιότερα μέσα.
- Ο τρόπος λήψης των δεδομένων με τη χρήση καμερών είναι τέτοιος ώστε η συλλογή δεδομένων να περιορίζεται στα απολύτως απαραίτητα για την εκπλήρωση του σκοπού της επεξεργασίας και να μη θίγονται θεμελιώδη δικαιώματα των ανθρώπων που βρίσκονται στο χώρο που επιτηρείται.
- Η επιτήρηση της περιμέτρου του κτιρίου της Εταιρείας δεν πραγματοποιείται με λήψη εικόνας από παράπλευρες οδούς και πεζοδρόμια, ούτε από εισόδους ή εσωτερικό γειτονικών κατοικιών, κτιρίων ή άλλων χώρων.
- Δεν υφίστανται και δεν επιτρέπεται να τοποθετηθούν στο μέλλον κάμερες σε σημεία του κτιρίου από τα οποία η συλλογή δεδομένων δεν εξυπηρετεί τους σκοπούς της επεξεργασίας ή/και ενδέχεται να παραβιάσει την προστασία των δεδομένων των υποκειμένων (π.χ. τουαλέτες).
- Η χρήση κάμερας με δυνατότητα στρέψης ή/και εστίασης επιτρέπεται μόνο εξαιρετικά και για το σκοπό της νυκτερινής ασφάλειας και της δυνατότητας παρέμβασης σε πραγματικό χρόνο.
- Τα δεδομένα που συλλέγονται από το σύστημα μαγνητοσκόπησης δε μπορούν, σε καμία περίπτωση, να χρησιμοποιηθούν ως κριτήρια για την αξιολόγηση της συμπεριφοράς και αποδοτικότητας των εργαζομένων, όταν μαγνητοσκοπούνται εσωτερικοί χώροι της εταιρείας.
- Η διαβίβαση των δεδομένων που συλλέγονται από το σύστημα μαγνητοσκόπησης επιτρέπεται μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων, με εξαίρεση τη διαβίβαση αυτών σε αστυνομικές, δικαστικές και εισαγγελικές αρχές που ζητούν νομίμως τα δεδομένα κατά την άσκηση των καθηκόντων τους, ή τις περιπτώσεις οικειοθελούς διαβίβασης των δεδομένων αυτών από την Εταιρεία προς τις ως άνω αρχές στις περιπτώσεις που ενδέχεται να αποτελούν αποδεικτικά στοιχεία αξιόποινων πράξεων.
- Η Εταιρεία ενημερώνει τα πρόσωπα που πρόκειται να εισέλθουν σε χώρους που μαγνητοσκοπούνται για το γεγονός αυτό με ευδιάκριτες πινακίδες.
- Το υποκείμενο των δεδομένων έχει πάντοτε τη δυνατότητα πρόσβασης στα δεδομένα αυτής της μορφής που το αφορούν, τίθεται στη διάθεσή του οποτεδήποτε το ζητήσει αναλυτική ενημέρωση σχετικά με το σκοπό της συλλογής και επεξεργασίας των δεδομένων, το σύστημα που χρησιμοποιείται, τους χώρους που επιτηρούνται, την εμβέλεια των καμερών, το χρόνο τήρησης των δεδομένων, τους χειριστές του συστήματος και τους νόμιμους αποδέκτες.

7. Καταστροφή δεδομένων

Η Εταιρεία αναγνωρίζει τη σπουδαιότητα της ορθής και ασφαλούς καταστροφής των προσωπικών δεδομένων έπειτα από την εκπλήρωση του σκοπού της επεξεργασίας και εφόσον δεν υφίσταται νόμιμη υποχρέωση τήρησής τους και για το σκοπό αυτό, διαθέτει και εφαρμόζει συγκεκριμένες ρυθμίσεις και διαδικασίες τόσο ως προς την τήρηση, όσο και ως προς την καταστροφή δεδομένων στα πλαίσια της παρούσας πολιτικής.

Σκοπός των ρυθμίσεων αυτών είναι ο καθορισμός των απαιτούμενων σχετικά με τη διάρκεια τήρησης των δεδομένων καθώς και με την καταστροφή τους (διαγραφή/ανωνυμοποίησηη) έπειτα από την εκπλήρωση του σκοπού της επεξεργασίας και εφόσον δεν υφίσταται νόμιμη υποχρέωση τήρησής τους.

7.1 Τήρηση Δεδομένων

7.1.1 Βασικές αρχές τήρησης.

Η Εταιρεία εφαρμόζει τις κάτωθι αρχές όσον αφορά την τήρηση των δεδομένων:

►Τα δεδομένα τηρούνται μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας.

►Όπου έχει εφαρμογή νόμιμη ή/και κανονιστική απαίτηση η περίοδος τήρησης των δεδομένων προσδιορίζεται με βάση αυτή.

►Όπου είναι εφικτό, καθορίζεται ποσοτικά η περίοδος τήρησης των δεδομένων (π.χ. είκοσι έτη από την ημερομηνία λύσης της σύμβασης συνεργασίας). Όπου αυτό δεν είναι εφικτό, προσδιορίζονται τα κριτήρια βάσει των οποίων καθορίζεται το εν λόγω διάστημα τήρησης.

►Κατά την περίοδο τήρησης των δεδομένων, εφαρμόζονται τα κατάλληλα μέτρα προστασίας.

7.1.2 Καθορισμός κατάλληλης περιόδου τήρησης.

Τα δεδομένα τηρούνται μόνο για συγκεκριμένες χρονικές περιόδους. Τα δεδομένα δε φυλάσσονται επ' αόριστο στο εσωτερικό της Εταιρείας, αλλά απομακρύνονται (καταστρέφονται/ανωνυμοποιούνταιι) από τα συστήματα και τα φυσικά αρχεία της Εταιρείας όταν εκπληρωθεί ο σκοπός της επεξεργασίας και εφόσον δεν υφίσταται νόμιμη υποχρέωση τήρησής τους.

Ενδεικτικοί παράγοντες που λαμβάνονται υπόψη κατά τον καθορισμό χρονικής περιόδου τήρησης των δεδομένων:

►Η φύση των δεδομένων.

►Ο σκοπός της επεξεργασίας.

►Οι νόμιμες και κανονιστικές απαιτήσεις όπως εκάστοτε ισχύουν στο περιβάλλον στο οποίο δραστηριοποιείται η Εταιρεία.

►Η αξία που έχουν τα δεδομένα για την Εταιρεία.

►Οι κίνδυνοι για την Εταιρεία και τα υποκείμενα που ενδέχεται να απορρέουν από την τήρηση τους.

►Οι ενδεχόμενες υποχρεώσεις της Εταιρείας που ενδέχεται να απορρέουν από την τήρηση τους.

Οι περίοδοι τήρησης των δεδομένων ενδέχεται να διαφέρουν ανάλογα με τον τύπο των δεδομένων, το σκοπό της επεξεργασίας καθώς και άλλους παράγοντες. Στοιχεία σχετικά με την προβλεπόμενη περίοδο τήρησης των δεδομένων περιλαμβάνονται στο «Αρχείο Δραστηριοτήτων Επεξεργασίας Προσωπικών Δεδομένων».

► Εφαρμογή «Πολιτικής Ασφαλείας Δεδομένων

7.1.2.1 Πολιτική ασφαλείας προσωπικών δεδομένων (Security Policy)

Η Πολιτική Ασφαλείας Δεδομένων (ΠΑΔ) καθορίζει τη δέσμευση της Διοίκησης και την προσέγγιση της Εταιρείας σχετικά με την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και την προστασία προσωπικών δεδομένων που τηρεί η Εταιρεία και περιγράφει τα μέτρα προστασίας και τις διαδικασίες που εφαρμόζει για την προστασία και ασφάλεια των δεδομένων που τηρεί και φυλάσσει Η συλλογή και επεξεργασία προσωπικών δεδομένων πραγματοποιείται από την Εταιρεία για τους εξής κυρίως λόγους:

(α) Για την παροχή και στο πλαίσιο της παροχής από την Εταιρεία των υπηρεσιών που δύναται να παρέχει βάσει της άδειας λειτουργίας της και του καταστατικού της.

(β) Για τη συμμόρφωση της Εταιρείας με υποχρεώσεις που υπέχει κατά τη άσκηση των δραστηριοτήτων της έναντι εποπτικών, διοικητικών, φορολογικών, δικαστικών, ελεγκτικών ή άλλων αρμόδιων σχετικά φορέων.

(γ) Για την προστασία των εγκαταστάσεων, των πληροφορικών συστημάτων, των συστημάτων επικοινωνίας και των παντός είδους πληροφοριών που η Εταιρεία συλλέγει και αποθηκεύει για την άσκηση των δραστηριοτήτων της.

(δ) Στα πλαίσια της λειτουργίας της ως ανώνυμη εταιρεία ως προς την πρόσληψη εργαζομένων ή την υποβολή προς αυτήν αιτήσεων πρόσληψης εργαζομένων, καθώς και ως προς τη σύναψη συμβατικών σχέσεων με προμηθευτές και πρόσωπα που παρέχουν προς την Εταιρεία παντός είδους υπηρεσίες.

Ι.Βασικές αρχές ΠΑΔ

Στην ΠΑΔ περιλαμβάνονται:

(α) Οργανωτικά μέτρα ασφαλείας, αναφορικά με τους ρόλους και τις αρμοδιότητες του προσωπικού και των τυχόν εξωτερικών συνεργατών-εκτελούντων την επεξεργασία, την εκπαίδευση του προσωπικού, τη διαχείριση περιστατικών ασφαλείας.

(β) Τεχνικά μέτρα ασφαλείας, αναφορικά με τη διαχείριση των χρηστών του πληροφοριακού συστήματος, την αναγνώριση και αυθεντικοποίηση των χρηστών, την ασφάλεια των επικοινωνιών, τη λειτουργία των αρχείων καταγραφής του πληροφοριακού συστήματος και την εξαγωγή αντιγράφων ασφαλείας.

(γ) Μέτρα φυσικής ασφάλειας.

Με την ΠΑΔ προσδιορίζονται οι ρόλοι κάθε εμπλεκόμενου εντός της Εταιρείας, οι αρμοδιότητες, οι ευθύνες και τα καθήκοντά τους ως προς τις διαδικασίες που αφορούν στην ασφάλεια και περιγράφονται τα μέτρα που προβλέπονται για την κάλυψη των βασικών αρχών και κανόνων ασφαλείας δεδομένων που περιλαμβάνει. Αφορά τόσο αυτοματοποιημένα, όσο και μη αυτοματοποιημένα συστήματα διαχείρισης και επεξεργασίας δεδομένων και υπόκειται σε τακτικές αναθεωρήσεις, λαμβανομένων πάντοτε υπόψη των εκάστοτε αναγκών και τεχνολογικών αλλαγών. Κάθε φυσικό ή νομικό πρόσωπο που συνάπτει συμβατικές σχέσεις με την Εταιρεία ενημερώνεται προσυμβατικά για την υποχρέωση της Εταιρείας να συλλέγει, να επεξεργάζεται και να τηρεί προσωπικά του δεδομένα διαθέτοντας σε κάθε περίπτωση νόμιμη βάση επεξεργασίας και, όπου απαιτείται, τη συναίνεση του υποκειμένου ως προς το ότι δεδομένα που αφορούν το πρόσωπο αυτό, τους αντιπροσώπους ή τους νόμιμους εκπρόσωπούς του και τα οποία ο ίδιος γνωστοποιεί στην Εταιρεία ή η τήρησή τους προβλέπεται από το νόμο, θα τηρούνται από την Εταιρεία σε αρχείο σύμφωνα με τις ισχύουσες διατάξεις και ιδίως τον ΓΚΠΔ όπως κάθε φορά

ισχύει, θα αποτελούν αντικείμενο επεξεργασίας από αυτή και ενδέχεται να διαβιβάζονται σε φυσικά πρόσωπα υπαλλήλους και συνεργάτες της Εταιρείας (στο πλαίσιο των αρμοδιοτήτων τους), καθώς και στην Επιτροπή Κεφαλαιαγοράς, άλλες εποπτεύουσες αρχές, σε αρμόδιες δημόσιες υπηρεσίες και δημόσιες αρχές, σε ρυθμιζόμενες αγορές, στις αρμόδιες Δ.Ο.Υ., σε συνεργαζόμενο θεματοφύλακα, καθώς και σε ενδιάμεσους, συνδεδεμένους αντιπροσώπους και λοιπά διαμεσολαβούντα ή άλλως συνεργαζόμενα με την Εταιρεία φυσικά ή νομικά πρόσωπα, στο πλαίσιο της παροχής υπηρεσιών από την Εταιρεία, κατά τα προβλεπόμενα στις εκάστοτε ευρισκόμενες εν ισχύ συμβάσεις μεταξύ φυσικού ή νομικού προσώπου και της Εταιρείας.
Η επεξεργασία, καταχώριση και αποθήκευση σε αρχείο από τους υπαλλήλους των αρμοδίων τμημάτων της Εταιρείας των ατομικών, οικογενειακών, περιουσιακών ή άλλων στοιχείων και προσωπικών δεδομένων προσώπων που συνεργάζονται καθοιονδήποτε τρόπο με την Εταιρεία, καθώς και των στοιχείων που αφορούν τυχόν συναλλαγές που διενεργούνται στο όνομά τους μέσω ή από την Εταιρεία, λαμβάνει χώρα υπό την αδιάκοπη μέριμνα της Εταιρείας για την απόρρητη και ασφαλή επεξεργασία των δεδομένων αυτών σύμφωνα με τις ανάγκες της συμβατικής σχέσης με το εκάστοτε πρόσωπο και τις ισχύουσες διατάξεις. Η επεξεργασία προσωπικών δεδομένων διατηρείται και μετά τη λήξη της συναλλακτικής σχέσης και για όσο χρονικό διάστημα απαιτείται βάσει των ισχυουσών διατάξεων και των σχετικών συμβάσεων.
Όλες οι εντολές που διαβιβάζονται τηλεφωνικά στην Εταιρεία προς κατάρτιση συναλλαγών, ηχογραφούνται και αρχειοθετούνται από την Εταιρεία όπως προβλέπεται κανονιστικά για λόγους προστασίας των συναλλαγών και τίθενται, εφόσον τούτο ζητηθεί, στη διάθεση της Επιτροπής Κεφαλαιαγοράς ή/και άλλων αρμοδίων αρχών, κατά τα οριζόμενα στις ισχύουσες διατάξεις.
Τηρουμένων πάντοτε των προϋποθέσεων και των διατάξεων που ορίζει ο ΓΚΠΔ, όπως ισχύει, η Εταιρεία δύναται να τοποθετήσει και να θέσει σε λειτουργία κλειστό κύκλωμα τηλεόρασης στους χώρους των εγκαταστάσεων που χρησιμοποιεί, προς το σκοπό της επαύξησης των μέτρων προστασίας και ασφάλειας που λαμβάνει για τους εργαζόμενους σε αυτή, για τα περιουσιακά της στοιχεία, για τα πληροφορικά συστήματα που χρησιμοποιεί και για τα προσωπικά δεδομένα, αρχεία και πληροφορίες που συλλέγει και τηρεί σε σχέση με κάθε πρόσωπο με το οποίο συναλλάσσεται καθοιονδήποτε τρόπο.

Η ΠΑΔ είναι ενιαία ώστε να καλύπτει όλα τα πληροφοριακά συστήματα και τις διαδικασίες που άπτονται της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και περιλαμβάνει με σαφήνεια τις ρυθμίσεις που επιτάσσει έτσι ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της. Κατά τη σύνταξή της, λήφθηκε μέριμνα να μη χρησιμοποιούνται κατά το δυνατό εξειδικευμένοι τεχνικοί όροι που ενδεχομένως καθιστούν δύσκολη την εφαρμογή της και να την εξαρτούν από συγκεκριμένες τεχνολογικές επιλογές. Η ΠΑΔ υπόκειται σε τακτικές αναθεωρήσεις ή όταν συμβαίνουν σημαντικές αλλαγές σε κάποιο τουλάχιστον από τα εξής: α) στην οργανωτική δομή της Εταιρείας, β) στα πληροφοριακά συστήματα, γ) στις απαιτήσεις ασφαλείας, δ) στις τεχνολογικές εξελίξεις, ε) στο είδος ή/και στην επεξεργασία των προσωπικών δεδομένων. Η ΠΑΔ μπορεί επίσης να μεταβάλλεται κατόπιν διενέργειας εσωτερικού ή εξωτερικού ελέγχου, ο οποίος καταδεικνύει μη επαρκή ή/και μη αποτελεσματικά μέτρα ως προς την ασφάλεια, ή κατόπιν περιστατικού παραβίασης της ασφάλειας. Η ΠΑΔ καταγράφεται με γενικευμένη μορφή ως οφείλει, υπό την έννοια ότι η εφαρμογή της σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα της Εταιρείας να είναι δυνατή χωρίς να απαιτούνται μεγάλες τροποποιήσεις σε μικρά χρονικά διαστήματα.

Τα αναγραφόμενα στην ΠΑΔ είναι δεσμευτικά για όλο το προσωπικό που χειρίζεται καθ' οιονδήποτε τρόπο προσωπικά δεδομένα και βρίσκεται σε συμφωνία με την κείμενη νομοθεσία.

II. Οργανωτικά μέτρα ασφαλείας

(α) Οργάνωση - Διαχείριση προσωπικού

-Ρόλοι, εξουσιοδοτήσεις: Για κάθε συγκεκριμένη εργασία που επιτελείται εντός της Εταιρείας υφίστανται οργανωτικοί ρόλοι και γίνεται σύνδεση του προσωπικού με τους αντίστοιχους ρόλους. Κάθε εργαζόμενος γνωρίζει με σαφήνεια τους ρόλους που του ανατίθενται διακεκριμένα από τους ρόλους άλλων εργαζομένων. Κάθε εργαζόμενος έχει δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα δεδομένα προσωπικού χαρακτήρα, βάσει των αρμοδιοτήτων και καθηκόντων που του έχουν ανατεθεί και υπαγορεύονται από το ρόλο του

-Αναθεώρηση ρόλων: Οι παρεχόμενες εξουσιοδοτήσεις και δικαιώματα πρόσβασης προς τους εργαζόμενους για την άσκηση των αρμοδιοτήτων τους υπόκεινται σε περιοδική επανεξέταση για όλα τα στάδια της εργασιακής πορείας των υπαλλήλων (πρόσληψη, μετακίνηση, αλλαγή καθηκόντων, αποχώρηση, κλπ).

- Δέσμευση εμπιστευτικότητας: Η Εταιρεία επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Για το σκοπό αυτό, η Εταιρεία λαμβάνει ειδικά μέτρα για τη δέσμευση του προσωπικού που επεξεργάζεται προσωπικά δεδομένα ως προς την εμπιστευτικότητα και τους όρους χρήσης αυτών των πληροφοριών, ιδίως όταν το εν λόγω προσωπικό δε δεσμεύεται ήδη από απόρρητο.

-Ενημέρωση χρηστών συστήματος: Η Εταιρεία ενημερώνει τους χρήστες σε σχέση με την εταιρική πολιτική ασφαλείας δικτύου Η/Υ & πρόσβασης στο διαδίκτυο.

-Αποχώρηση εργαζομένου: Σε περιπτώσεις αποχώρησης εργαζομένου από την Εταιρεία, το Τμήμα Πληροφορικής ενημερώνεται αμελλητί και προβαίνει σε όλες τις δέουσες ενέργειες προκειμένου να διαφυλάξει την ασφάλεια των ηλεκτρονικών συστημάτων και των πληροφοριών που αυτά περιέχουν:

Καταργεί όλους τους λογαριασμούς πρόσβασης, τις εξουσιοδοτήσεις και τους κωδικούς πρόσβασης του αποχωρούντος. Καταργεί τους λογαριασμούς ηλεκτρονικού ταχυδρομείου και δεν επιτρέπει την επαναχρησιμοποίησή τους από άλλους χρήστες.

Μεριμνά για την επιστροφή οποιουδήποτε εξοπλισμού τυχόν είχε παρασχεθεί στον αποχωρούντα υπάλληλο και ανήκει στην Εταιρεία (συμπεριλαμβανομένων υπολογιστών, κλειδιών, ηλεκτρονικών καρτών εισόδου/εξόδου, κλπ).

(β) Διαχείριση πληροφοριακών συστημάτων

Καταγραφή: Υπάρχουν σαφείς διαδικασίες διαχείρισης υλικού και λογισμικού που περιλαμβάνουν την τήρηση επικαιροποιημένου καταλόγου των πληροφοριακών και επικοινωνιακών υποδομών και συστημάτων, του λογισμικού καθώς και των κατηγοριών αρχείων και δεδομένων που χρησιμοποιούνται ή τηρούνται από την Εταιρεία, όπως επίσης και των ατόμων που είναι κάτοχοι ή υπεύθυνοι των αντίστοιχων συστημάτων.

Διαχείριση φυσικού αρχείου: Η πρόσβαση στο φυσικό αρχείο επιτρέπεται αποκλειστικά και μόνο στα πρόσωπα των οποίων οι αρμοδιότητες απαιτούν αυτή τη δυνατότητα.
Διακίνηση πληροφοριακού εξοπλισμού: Σε περίπτωση που εξοπλισμός (π.χ. υπολογιστής ή USB) με προσωπικά δεδομένα μεταφέρεται εκτός των εγκαταστάσεων της Εταιρείας, η ενέργεια αυτή τελεί υπό την έγκριση είτε του Υπευθύνου Προστασίας Δεδομένων είτε του Υπευθύνου του τμήματος Μηχανογράφησης-Πληροφορικής.

(γ) Εκτελούντες την επεξεργασία

-Καταγραφή: Η Εταιρεία τηρεί κατάλογο όλων των εκτελούντων την επεξεργασία που χειρίζονται προσωπικά δεδομένα για λογαριασμό της εντός ή εκτός των εγκαταστάσεων της.

-Έγγραφη ανάθεση: Στις περιπτώσεις ανάθεσης της επεξεργασίας δεδομένων σε εκτελούντα, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ότι ο εκτελών την επεξεργασία τη διεξάγει μόνο κατ' εντολή της Εταιρείας, μόνο κατά την έκταση αυτής της εντολής και ότι οι λοιπές υποχρεώσεις ως προς την ασφάλεια βαρύνουν αναλόγως και τον εκτελούντα.

-Μέτρα ασφαλείας που αφορούν τους εκτελούντες: Ο εκτελών την επεξεργασία οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφαλή τήρηση και επεξεργασία των προσωπικών δεδομένων των υποκειμένων που του διαβιβάζονται μέσω της Εταιρείας. Η Εταιρεία επισκοπεί τη συμμόρφωση του εκτελούντος την επεξεργασία με τους όρους και διατάξεις της ΠΑΔ, στο μέτρο που αυτή αφορά τον εκτελούντα, αναφορικά με κανόνες πρόσβασης στα συστήματα, διαχείριση περιστατικών ασφαλείας, μέτρα φυσικής ασφαλείας, κ.λπ.

Δικαιώματα πρόσβασης σε μέλη του προσωπικού του εκτελούντος στα συστήματα της Εταιρείας εκχωρούνται μόνο όταν αυτό είναι απαραίτητο για την υλοποίηση των συμβατικών τους υποχρεώσεων, ωστόσο ακόμα και τότε η Εταιρεία εκχωρεί τις ελάχιστες απαιτούμενες εξουσιοδοτήσεις, οι οποίες καταργούνται με τη λήξη της συμβατικής υποχρέωσης.

-Τόπος επεξεργασίας: Για τη συντήρηση/αναβάθμιση του εξοπλισμού που φέρει προσωπικά δεδομένα εξετάζεται πάντοτε το ενδεχόμενο, εφόσον είναι εφικτό και πρόσφορο, αυτή να πραγματοποιείται στο χώρο των γραφείων της Εταιρείας.

Όταν η επεξεργασία γίνεται εκτός των εγκαταστάσεων της Εταιρείας, αυτή ανατίθεται σε εκτελούντα που δύναται να παρέχει επίπεδο ασφαλείας τουλάχιστον ανάλογο με αυτό που ορίζεται στην παρούσα ΠΑΔ.

-Δέσμευση εμπιστευτικότητας προσωπικού του εκτελούντος: Οι υπάλληλοι του εκτελούντος που επεξεργάζονται, κατά το χρονικό διάστημα της σύμβασης, προσωπικά δεδομένα για λογαριασμό της Εταιρείας πρέπει να δεσμεύονται εγγράφως με κατάλληλη δήλωση εμπιστευτικότητας.

(δ) Εμπιστευτικότητα των πληροφοριών

i. Η Εταιρεία δεν ενοικιάζει, δεν πουλά και δε δημοσιεύει πληροφορίες που συγκεντρώνει στα πλαίσια άσκησης των δραστηριοτήτων της και δίνει αυξημένο βάρος στην προστασία των προσωπικών δεδομένων των συνεργαζόμενων καθοιονδήποτε τρόπο με αυτή.

Εξαιρούνται της ανωτέρω δέσμευσης τήρησης απορρήτου ως προς τις συλλεγόμενες πληροφορίες, οι υποχρεώσεις συμμόρφωσης της Εταιρείας με νομοθετικές ή κανονιστικές υποχρεώσεις της.

Η Εταιρεία ενδέχεται να μεταβιβάσει αυτές τις πληροφορίες σε περίπτωση εταιρικού μετασχηματισμού. Σε αυτήν την περίπτωση, η Εταιρεία θα προβεί σε όλες τις απαραίτητες γνωστοποιήσεις πριν τη μεταβίβαση των πληροφοριών που κατέχει, οι οποίες θα υπόκεινται πλέον σε διαφορετική πολιτική απορρήτου.

ii. Η πρόσβαση στα ηλεκτρονικά αρχεία της Εταιρείας απαγορεύεται ρητώς και εμποδίζεται με κάθε πρόσφορο τρόπο. Εξαίρεση από τον κανόνα αυτόν αποτελεί μόνο η δυνατότητα πρόσβασης, στο βαθμό και στην έκταση που απαιτείται, σε κάθε νομιμοποιούμενο προς τούτο φυσικό πρόσωπο ή εκπρόσωπο νομικού προσώπου για την άσκηση των καθηκόντων του και για την πλήρωση συμβατικών του υποχρεώσεων έναντι της Εταιρείας.

iii. Δημοσιεύσεις σε περιοχές δημόσιας πρόσβασης: Οι περιοχές δημόσιας πρόσβασης είναι όλες οι προσβάσιμες από το κοινό περιοχές της Εταιρείας που μπορούν να ανιχνευθούν από μηχανές αναζήτησης.

Οποτεδήποτε τυχόν διατίθεται η δυνατότητα δημοσίευσης και ανταλλαγής πληροφοριών σε περιοχές δημόσιας πρόσβασης της Εταιρείας, κάθε πρόσωπο που θα αποφασίσει να αποκαλύψει πληροφορίες που ενδέχεται να το ταυτοποιεί προσωπικά θα πρέπει να έχει υπόψη του ότι:

- Αυτές οι πληροφορίες ενδέχεται να παραμείνουν επ' αόριστον στην περιοχή δημόσιας πρόσβασης της Εταιρείας.
- Οι υπόλοιποι χρήστες ενδέχεται να έχουν τη δυνατότητα να δουν δύο ή περισσότερες από τις δημοσιεύσεις του προσώπου αυτού.
- Το πρόσωπο θα φέρει την αποκλειστική ευθύνη για όλες τις πληροφορίες που δημοσιεύει ή αποκαλύπτει στις περιοχές δημόσιας πρόσβασης.

III. Τεχνικά μέτρα ασφαλείας

(α) Τεχνολογική υποδομή.

Οι κύριες λειτουργικές εφαρμογές της Εταιρείας φιλοξενούνται στο τοπικό δίκτυο (Local Area Network -LAN) που έχει αναπτύξει η Εταιρεία

(β) Ημερήσιος έλεγχος πληροφορικών συστημάτων.

Η Εταιρεία προβαίνει σε καθημερινή βάση σε έλεγχο της ασφαλούς και αποτελεσματικής λειτουργίας των πληροφοριακών της συστημάτων, στα πλαίσια του οποίου καταγράφονται και κατηγοριοποιούνται τα γεγονότα που αποτελούν ή θα μπορούσαν να χαρακτηριστούν ως επιβλαβή, κακόβουλα ή επικίνδυνα για τη λειτουργία των πληροφορικών συστημάτων (π.χ. μη εξουσιοδοτημένη δραστηριότητα, κλοπή μηχανογραφικού εξοπλισμού, εσωτερική ή εξωτερική παραβίαση ασφάλειας, μη διαθεσιμότητα ή δυσλειτουργία των ηλεκτρονικών συστημάτων κτλ.) και ενημερώνεται η Διοίκηση της Εταιρείας.

(γ) Ασφάλεια συστημάτων.

Η ασφάλεια των συστημάτων αυτών περιλαμβάνει δύο ενότητες, τη "Φυσική" και τη "Λογική".

i. Φυσική ασφάλεια

Ο Υπεύθυνος του τμήματος Πληροφορικής:

- Έχει την ευθύνη οργάνωσης του χώρου που φιλοξενείται ο μηχανογραφικός εξοπλισμός (computer room) και είναι υπεύθυνος για την ασφάλεια του.
- Ελέγχει τη θερμοκρασία και την υγρασία του computer room και τη σωστή λειτουργία των κλιματιστικών συστημάτων.
- Παρακολουθεί την ορθή λειτουργία των συστημάτων ανίχνευσης καπνού και αυτόματης πυρόσβεσης. Επιβλέπει την εγκατάσταση χειροκίνητων συστημάτων πυρόσβεσης, ελέγχει τις ηλεκτρικές συνδέσεις και εγκαταστάσεις και απομακρύνει από το computer room χαρτί και εύφλεκτα υλικά.
- Εκπαιδεύει το προσωπικό για την αντιμετώπιση καταστάσεων κινδύνου.
- Παρακολουθεί τη συνεχή παροχή ρεύματος μέσω UPS ή γεννήτριας.
- Ελέγχει την εύρυθμη λειτουργία των συσκευών παροχής ρεύματος και πραγματοποιεί συχνές δοκιμές για την εξασφάλιση της αποδοτικότητάς τους.
- Εφαρμόζει τη διαδικασία ελέγχου για την είσοδο του προσωπικού στους χώρους του computer room. Η πρόσβαση επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα και ελέγχεται από σύστημα παρακολούθησης εισόδου/εξόδου που απαιτεί τη χρήση μαγνητικής κάρτας.
- Επιβλέπει την ομαλή λειτουργία των συστημάτων που καταγράφουν, με τη χρήση καμερών και κλειστού κυκλώματος, εικόνες από την παρακολούθηση ζωτικών χώρων των εγκαταστάσεων της Εταιρείας (ταμεία, computer room, είσοδοι γραφείων κ.α.).

ii. Λογική ασφάλεια

- Ο Υπεύθυνος του τμήματος Πληροφορικής είναι υπεύθυνος για την ασφάλεια των συστημάτων (system security) της Εταιρείας σε θέματα πρόσβασης (access) και ασφάλειας δικτύων (network security).
- Ο Υπεύθυνος του τμήματος Πληροφορικής είναι υπεύθυνος των εφαρμογών (application administrator) όσον αφορά τον ορισμό της πρόσβασης των χρηστών σε κάθε εφαρμογή. Οι χρήστες έχουν δικαιώματα πρόσβασης "user access rights" μόνο σε αρχεία και λειτουργίες του συστήματος που χρειάζονται για να επιτελέσουν τα καθήκοντά τους, έτσι ώστε να εξασφαλίζεται ο διαχωρισμός των καθηκόντων.
- Οι σημαντικές εφαρμογές παρέχουν δυνατότητα έκδοσης καταστάσεων με τους χρόνους χρήσης των εφαρμογών από τους χρήστες και τις εργασίες που επιτέλεσαν. Οι καταστάσεις αυτές ελέγχονται περιοδικά. Πιθανές κακόβουλες ή λανθασμένες απόπειρες των χρηστών για τροποποίηση δεδομένων τεκμηριώνονται και αναφέρονται στη Διοίκηση.
- Ο Υπεύθυνος του τμήματος Πληροφορικής είναι υπεύθυνος για την ασφάλεια του δικτύου (System security administrator) και στο πλαίσιο αυτό χορηγεί, κατόπιν εντολών της Διοίκησης, σε ομάδες χρηστών συγκεκριμένα δικαιώματα πρόσβασης στο δίκτυο.

(δ) Πρόσθετες λειτουργίες τμήματος Μηχανογράφησης

1. Το τμήμα Πληροφορικής, υπό την εποπτεία του υπευθύνου αυτού:

- Υποστηρίζει τους χρήστες στις καθημερινές τους εργασίες μέσω των συστημάτων πληροφορικής της Εταιρείας.
- Αναλαμβάνει την εγκατάσταση όλων των σταθμών εργασίας (Η/Υ) του δικτύου και παρέχει

συνεχή υποστήριξη.

- Αντιμετωπίζει τα προβλήματα των χρηστών και φροντίζει για την επίλυσή τους, είτε με ίδια μέσα είτε μέσω της προσφυγής σε εξωτερικούς συνεργάτες.
- Αναφέρει στη Διοίκηση τις εργασίες υποστήριξης που προσφέρει στους χρήστες σε τακτά χρονικά διαστήματα.
- Ελέγχει την αποδοτικότητα του δικτύου, τους χρόνος ανταπόκρισης του συστήματος, τη διαθεσιμότητα της χωρητικότητας των σκληρών δίσκων και προβαίνει σε διορθωτικές ενέργειες όπου και όταν κρίνεται αυτό σκόπιμο.
- Προγραμματίζει τη συντήρηση του μηχανογραφικού εξοπλισμού και κάνει προτάσεις για την βελτίωση της αποδοτικότητας του συστήματος.
- Καταγράφει και τεκμηριώσει τις λειτουργίες διαχείρισης του κεντρικού server και του τοπικού δικτύου.
- Εκπαιδεύει τους χρήστες των συστημάτων.
- Διαπραγματεύεται τους όρους των συμβολαίων που αφορούν την εκπαίδευση με τους προμηθευτές όταν η Εταιρεία πρόκειται να αγοράσει νέες εφαρμογές ή σχεδιάσει να αναβαθμίσει τις υπάρχουσες.
- Παραλαμβάνει το μηχανογραφικό και επικοινωνιακό εξοπλισμό και τον αποθηκεύει μέχρι την τελική του εγκατάσταση.
- Αρχειοθετεί όλα τα εγχειρίδια χρήσης (user manuals) των εφαρμογών και προγραμμάτων και τα δανείζει στους χρήστες όταν αυτό απαιτείται.
- Λαμβάνει κάθε πρόσφορο μέτρο για την προστασία των συστημάτων, servers, λογισμικών και Η/Υ της Εταιρείας από ιούς και από κακόβουλες επιθέσεις με τη χρήση κάθε απαιτούμενου εργαλείου (firewalls, antivirus κ.λπ.), φροντίζοντας ταυτόχρονα για την αναβάθμιση και την άμεση επικαιροποίηση των συστημάτων αυτών.

2. Τήρηση αντιγράφων ασφαλείας: Το τμήμα λαμβάνει κάθε πρόσφορο μέτρο προκειμένου να εξασφαλίσει τη λήψη και διαχείριση αντιγράφων ασφαλείας. Αντίγραφα ασφαλείας τηρούνται και σε διαφορετικό χώρο από τα πρωτογενή δεδομένα, ο οποίος διαθέτει μέτρα ασφαλείας ανάλογα με τα μέτρα που υιοθετούνται για τα πρωτογενή δεδομένα.

3.Αρχεία καταγραφής (log files).

- Τήρηση και έλεγχος αρχείων καταγραφής: Στα κρίσιμα συστήματα, η Εταιρεία τηρεί αρχεία καταγραφής όλων των ενεργειών (log files) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων ασφαλείας διασφαλίζοντας την προστασία και την ακεραιότητα των αρχείων αυτών.

Στα αρχεία αυτά έχει πρόσβαση ο Υπεύθυνος του τμήματος Μηχανογράφησης-Πληροφορικής και όποια άλλα μέλη του προσωπικού είναι επιφορτισμένα με αρμοδιότητες διαχείρισης περιστατικών ασφαλείας κατόπιν εξουσιοδότησης.

Η πρόσβαση στα αρχεία καταγραφής επίσης καταγράφεται και υπόκειται στους ίδιους περιορισμούς με τα υπόλοιπα αρχεία καταγραφής.

4. Διαγραφή αρχείων καταγραφής:

Δεν υφίσταται δυνατότητα διαγραφής των αρχείων καταγραφής του συστήματος από ένα μόνο άτομο. Τέτοια διαγραφή λαμβάνει χώρα με την παρουσία 2 τουλάχιστον ατόμων, τα οποία έχουν διαφορετικούς ρόλους (π.χ. υπεύθυνος ασφαλείας + διοικητικός διευθυντής).

5.Ασφάλεια επικοινωνιών.

-Έλεγχος δικτυακών συσκευών: Εξασφάλιση επαρκούς ελέγχου των συνδεόμενων στο δίκτυο συσκευών (ως προς την πρόσβαση σε αυτές αλλά και τη χρήση τους).

-Απομακρυσμένη πρόσβαση: Το Τμήμα Μηχανογράφησης-Πληροφορικής εφαρμόζει συγκεκριμένες διαδικασίες για τη διαχείριση της απομακρυσμένης πρόσβασης σε συστήματα μέσω ασφαλών καναλιών με δυνατή ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση.

-Κανάλι επικοινωνίας: Η επικοινωνία μεταξύ υπολογιστών/κόμβων γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας

-Πρωτόκολλα δικτύου: Η χρήση ευπαθών ως προς την ασφάλεια πρωτοκόλλων καταρχάς αποφεύγεται και, όταν υπηρεσίες τέτοιων πρωτοκόλλων είναι αναγκαίες, γίνεται χρήση των αντίστοιχων ασφαλών.

-Περιμετρική ασφάλεια: Το Τμήμα ελέγχει τις δικτυακές συνδέσεις του εσωτερικού δικτύου από και προς το διαδίκτυο ή άλλα εξωτερικά δίκτυα , με μέσα όπως το σημείο ελέγχου της περιμέτρου (firewall). Οι συνδέσεις που ενεργοποιούνται μέσω του firewall και οι υπηρεσίες που εξυπηρετούν είναι εγκεκριμένες από την Εταιρεία.

(ε) Ασφάλεια λογισμικού

-Σχεδιασμός εφαρμογών: Ο σχεδιασμός των εφαρμογών που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας (privacy by design). Ως εκ τούτου, οι εφαρμογές ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων (data minimization), καθώς και της ποιότητας των δεδομένων και να περιλαμβάνουν τη δυνατότητα της διαγραφής δεδομένων μετά το χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Επίσης, πρέπει να επιτρέπουν την υλοποίηση όλων των απαιτούμενων τεχνικών μηχανισμών ασφαλείας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

-Ασφαλής ανάπτυξη εφαρμογών: Σε περίπτωση ανάπτυξης εφαρμογών, είτε εσωτερικά στην Εταιρεία είτε από εξωτερικό συνεργάτη, προβλέπεται διαδικασία ασφαλούς υλοποίησης λογισμικού ώστε να εντοπίζονται τυχόν ευπάθειες αυτού ως προς την ασφάλεια προτού το λογισμικό μεταβεί σε λειτουργική φάση. Στις περιπτώσεις όπου η ανάπτυξη των εφαρμογών γίνεται από εξωτερικό συνεργάτη, τηρούνται προδιαγραφές ασφαλείας της εφαρμογής στο έγγραφο

περιγραφής απαιτήσεων λογισμικού, το οποίο εμπεριέχεται στη σύμβαση με τον εκάστοτε ανάδοχο.

-Προστασία αρχείων λειτουργικών συστημάτων: Τα λειτουργικά αρχεία των συστημάτων (system files), τα δεδομένα ελέγχου συστημάτων (system test data), καθώς και ο πηγαίος κώδικας (source code) των προγραμμάτων λογισμικού ελέγχονται και προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

(στ) Διαχείριση αλλαγών

Μεταβολές στα πληροφοριακά συστήματα πραγματοποιούνται ακολουθώντας πάντοτε τη μεθοδολογία καθορισμού των ρόλων και των προσώπων που έχουν δικαίωμα έγκρισης των αλλαγών, καταγραφής των αιτημάτων αλλαγής, προσδιορισμού των κριτηρίων αποδοχής των αλλαγών και χρονοδιαγράμματος υλοποίησης.
Περιβάλλον δοκιμών: Οι ενημερώσεις λογισμικού, είτε σε επίπεδο επιμέρους εφαρμογών είτε σε επίπεδο λειτουργικού συστήματος, δοκιμάζονται σε δοκιμαστικό περιβάλλον πριν τεθούν σε κανονική παραγωγή. Το δοκιμαστικό περιβάλλον είναι απομονωμένο από το παραγωγικό σύστημα και επικαιροποιημένο.

IV. Μέτρα φυσικής ασφάλειας

Σχέδιο ανάκαμψης από καταστροφές.
Η Εταιρεία έχει εξασφαλίσει τη λειτουργία εφεδρικού συστήματος πληροφορικής, όπου τηρείται το σύνολο των αρχείων των πελατών και μπορεί να λειτουργήσει ανά πάσα στιγμή εφεδρικά σε περίπτωση που το βασικό σύστημα πληροφοριών της Εταιρείας για οποιοδήποτε λόγο δε μπορεί να συνεχίσει τη λειτουργία του για διάστημα μεγαλύτερο μίας εβδομάδας. Ένα τέτοιο ενδεχόμενο μπορεί να λάβει χώρα σε περίπτωση που το βασικό σύστημα αναστείλει τη λειτουργία του εξαιτίας εσωτερικής ή εξωτερικής παραβίασης των συστημάτων ηλεκτρονικής ασφαλείας (π.χ. παραβίαση των κωδικών πρόσβασης, επίθεση από ηλεκτρονικούς ιούς κτλ.). Επίσης, το εφεδρικό σύστημα μπορεί να ενεργοποιηθεί σε περίπτωση που το βασικό σύστημα, λόγω υλικής καταστροφής από οποιαδήποτε αιτία (πυρκαγιά, σεισμός κτλ.), δεν μπορεί να υποστηρίξει τις συναλλακτικές δραστηριότητες της εταιρείας.

7.1.3 Ενέργειες κατά τη λήξη της περιόδου τήρησης

Τα δεδομένα μετά το πέρας της περιόδου τήρησής τους καταστρέφονται (διαγράφονται/ ανωνυμοποιούνται) εκτός εάν συντρέχει ιδιαίτερος λόγος για την περαιτέρω τήρησή τους. Η καταστροφή των δεδομένων πραγματοποιείται μόνο κατόπιν χορήγησης σχετικής έγκρισης από τον Υπεύθυνο Προστασίας Δεδομένων, σύμφωνα με τα όσα ορίζονται στις παρακάτω ενότητες της παρούσας πολιτικής. Επιπλέον, σε περίπτωση που το υποκείμενο των δεδομένων ζητήσει από την Εταιρεία τη διαγραφή των δεδομένων του, τότε τα δεδομένα αυτά θα πρέπει να διαγραφούν μόνο κατόπιν έγκρισης από τον Υπεύθυνο Προστασίας Δεδομένων και εν συνεχεία το υποκείμενο να ενημερωθεί σχετικά. Σε περίπτωση που τα δεδομένα πρέπει να τηρούνται λόγω νομικής νόμιμης ή κανονιστικής υποχρέωσης, το υποκείμενο των δεδομένων θα πρέπει να ενημερωθεί σχετικά με την αδυναμία διαγραφής και τους σχετικούς λόγους που επιβάλλουν την τήρηση των δεδομένων.

7.2 Καταστροφή δεδομένων

Η καταστροφή δεδομένων πραγματοποιείται από την Εταιρεία πάντοτε αμέσως μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας και κατά τρόπο ασφαλή, ήτοι κατά τρόπο που εξασφαλίζει την πλήρη και μόνιμη καταστροφή των δεδομένων αυτών, έτσι ώστε να καθίσταται αδύνατη η περαιτέρω, μετά την καταστροφή, μη νόμιμη και αθέμιτη επεξεργασία τους, όπως είναι η κάθε μορφής διάθεσή τους σε τρίτους, καθώς και κάθε δυνατότητα αναγνώρισης των υποκειμένων των δεδομένων.

Σε κάθε ασφαλή τρόπο καταστροφής δεδομένων η καταστροφή είναι μη αναστρέψιμη, δηλαδή δεν είναι δυνατή η ανάκτηση των δεδομένων μετά την καταστροφή με τεχνικά ή άλλα μέσα.

Τα προς καταστροφή δεδομένα χωρίζονται στις παρακάτω τρεις (3) κατηγορίες βάσει του τρόπου που τηρούνται και υφίστανται περαιτέρω επεξεργασία. Πιο συγκεκριμένα:

- ►Δεδομένα σε έντυπη μορφή (έγγραφα).
- ►Δεδομένα σε ηλεκτρονική μορφή τα οποία τηρούνται σε οποιοδήποτε μέσο όπως σκληροί δίσκοι υπολογιστών, CD, DVD, USB. Τα δεδομένα αυτά μπορεί να βρίσκονται είτε σε δομημένη μορφή (π.χ. βάση δεδομένων), είτε να αποτελούν σύνολο επιμέρους ηλεκτρονικών αρχείων (π.χ. αρχεία κειμένου, εικόνες, κλπ.).
- ►Δεδομένα σε άλλη μορφή (π.χ. δεδομένα που τηρούνται σε βιντεοκασέτες, κλπ.).

Στις περιπτώσεις κατά τις οποίες η Εταιρεία λάβει οποιοδήποτε αίτημα νομικής φύσης σχετικά με τη λήψη αρχείων ή πληροφοριών καθώς και στις περιπτώσεις κατά τις οποίες η Εταιρεία ή οποιοσδήποτε εργαζόμενός της αποτελέσει αντικείμενο ελέγχου ή έρευνας, η καταστροφή δεδομένων αναστέλλεται μέχρι να καταστεί δυνατό να προσδιοριστεί η απαίτηση για την παροχή των σχετικών αρχείων και πληροφοριών.

<u>Σύνταξη πρωτόκολλου καταστροφής δεδομένων.</u>

Σε κάθε περίπτωση καταστροφής δεδομένων συντάσσεται πρωτόκολλο καταστροφής, το οποίο περιλαμβάνει στοιχεία όπως η ημερομηνία καταστροφής των δεδομένων, περιγραφή των δεδομένων που καταστράφηκαν, τη μέθοδο καταστροφής καθώς και τα στοιχεία του Υπευθύνου Δραστηριότητας Επεξεργασίας (Owner) ή του εκτελούντος στην περίπτωση που η καταστροφή ανατίθεται σε τρίτη Εταιρεία.

Το πρωτόκολλο καταστροφής συμπληρώνεται από τον Υπεύθυνο Δραστηριότητας Επεξεργασίας (Owner), ή από τον εκτελούντα στην περίπτωση που η καταστροφή ανατίθεται σε τρίτη Εταιρεία και κοινοποιείται στον Υπεύθυνο Προστασίας Δεδομένων.

8. Θέματα εφαρμογής Πολιτικής

8.1 Ορισμός Υπεύθυνου Προστασίας Προσωπικών Δεδομένων

Ο Υπεύθυνος Προστασίας Δεδομένων ορίζεται με απόφαση του ΔΣ της Εταιρείας. Τα καθήκοντά του προσδιορίζονται στα πλαίσια της παρούσας. Απευθύνεται άμεσα προς το ΔΣ και, εκ του λόγου τούτου, οργανωτικά τοποθετείται σε επίπεδο αντίστοιχο των λοιπών εσωτερικών ελεγκτικών μονάδων της Εταιρείας.

8.2 Επικαιροποίηση Πολιτικής

Η Εταιρεία ελέγχει, επανεξετάζει και επικαιροποιεί σε τακτά χρονικά διαστήματα και, σε κάθε περίπτωση, όποτε τούτο κρίνεται αναγκαίο, την παρούσα Πολιτική, λαμβάνοντας υπόψη το εκάστοτε ισχύον νομοθετικό και κανονιστικό πλαίσιο.