
# ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

## (PERSONAL DATA PROTECTION POLICY)

**ΜΑΙΟΣ 2018**

# Έλεγχος Εντύπου

## ΙΣΤΟΡΙΚΟ ΕΚΔΟΣΕΩΝ

| Εκδοχή | Συγγραφέας | Ημερομηνία Έκδοσης | Σχόλια |
|---|---|---|---|
| V.1 | Έλενα Χριστοφή | 2018 | |
| | | | |
| | | | |
| | | | |

### ΑΝΑΘΕΩΡΗΤΕΣ ΕΝΤΥΠΩΝ

| Όνομα | Θέση | Ημερομηνία Υπογραφής |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

## ΕΓΚΡΙΣΗ ΕΓΓΡΑΦΟΥ

| Όνομα | Θέση | Ημερομηνία Υπογραφής |
|---|---|---|
| | BOD | |
| | | |
| | | |
| | | |

**Περιεχόμενα**

## 1. Εισαγωγή

Η Υδρόγειος Ασφαλιστική Εταιρεία (Κύπρου) Λτδ λόγω των επιχειρηματικών δραστηριοτήτων της, είναι απαραίτητο να συλλέγει, επεξεργάζεται, αποθηκεύει, διαβιβάζει και διαγράφει προσωπικά δεδομένα σε ποικιλία μορφών - γραπτή, προφορική ή ηλεκτρονική.

Η συλλογή και επεξεργασία μπορεί να αφορά πελάτες, ασφαλιστικούς διαμεσολαβητές, συνεργάτες, προμηθευτές, επιχειρηματικές επαφές, υπαλλήλους της Εταιρείας και άλλα άτομα που η Εταιρεία έχει σχέση με ή μπορεί να χρειαστεί να επικοινωνήσει προς επίτευξη των σκοπών της.

Αυτή η πολιτική περιγράφει τον τρόπο συλλογής, επεξεργασίας, διαβίβασης, αποθήκευσης και διαγραφής αυτών των προσωπικών δεδομένων ώστε να πληρούνται οι κανόνες προστασίας προσωπικών δεδομένων της εταιρείας και να υπάρχει συμμόρφωση με τον Κανονισμό (ΕΕ) αρ. 2016/679 και οδηγίες της Επιτρόπου Προστασίας Προσωπικών Δεδομένων.

## 2. Ορισμοί – Γλωσσάριο Βασικών Όρων

***Δεδομένα Προσωπικού Χαρακτήρα (personal data),*** *κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου κατά τρόπο που καθίσταται δυνατή η εξακρίβωση της ταυτότητας του. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορεί να προσδιορισθεί η ταυτότητα του φυσικού προσώπου στο οποίο αναφέρονται. Εάν τα δεδομένα που αναφέρονται στο πρόσωπο αυτό υφίστανται επεξεργασία, το πρόσωπο καλείται:*

***Υποκείμενο των Δεδομένων*** *νοείται το φυσικό εκείνο πρόσωπο, τα προσωπικά δεδομένα του οποίου συλλέγονται και υφίστανται επεξεργασία.*

***Υπεύθυνος Επεξεργασίας και Εκτελών την Επεξεργασία,*** *νοείται μόνο η Υδρόγειος Ασφαλιστική Εταιρεία (Κύπρου) Λτδ εκ Μεδούσης 2, Ydrogios House, 6059 Λάρνακα, τηλ. 24200826, τηλεομοιότυπο:24828290, email: DPO@ydrogios.com.cy*

***Υπεύθυνος Επεξεργασίας*** *είναι το πρόσωπο που διορίζει η εταιρεία το οποίο μόνο του ή από κοινού με άλλα πρόσωπα καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.*

***Επεξεργασία Προσωπικών Δεδομένων (personal data process),*** *κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα φυσικού προσώπου ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή, ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η αποκάλυψη, με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση, ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.*

***Ευαίσθητα Δεδομένα (sensitive data),*** *είναι τα δεδομένα που αφορούν την φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, τα γενετικά δεδομένα, τα βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, την υγεία, την σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό, τις ποινικές διώξεις ή καταδίκες, καθώς και τη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.*

***Αποδέκτης (receiver),*** *το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία αποκαλύπτονται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες.· Η επεξεργασία των δεδομένων αυτών από τις εν λόγω*

*δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας.*

***Συγκατάθεση του υποκειμένου των δεδομένων (consent),*** *κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.*

***Τρίτος (third party),*** *οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.*

***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.*

***Κατάρτιση Προφίλ (profiling),*** *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.*

***Ψευδωνυμοποίηση,*** *η επεξεργασία δεδομένων προσωπικού χαρακτήρα 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 ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ψευδωνυμοποίηση επιτυχαίνεται μέσω κρυπτογράφησης και χρήση σχετικού κλειδιού κρυπτογράφησης. Όποιος δεν κατέχει το κλειδί αποκρυπτογράφησης, μπορεί να προσδιορίσει την ταυτότητα των ψευδωνυμοποιημένων δεδομένων με δυσκολία. Ο σύνδεσμος με την ταυτότητα εξακολουθεί να υπάρχει με τη μορφή ψευδωνύμου συν το κλειδί αποκρυπτογράφησης. Η εξακρίβωση της ταυτότητας είναι εύκολα δυνατή για όσους έχουν δικαίωμα χρήσης του κλειδιού αποκρυπτογράφησης.*

***Ανωνυμοποιημένα Δεδομένα,*** *τα δεδομένα ανωνυμοποιούνται όταν από σύνολο προσωπικών δεδομένων διαγράφονται όλα τα αναγνωριστικά της ταυτότητας του προσώπου στοιχεία . Στις πληροφορίες δεν πρέπει να απομένει κανένα στοιχείο το οποίο θα μπορούσε να συμβάλει στην εξακρίβωση της ταυτότητας του προσώπου στο οποίο αναφέρονται. Όταν τα δεδομένα ανωνυμοποιούνται επιτυχώς, παύουν να είναι προσωπικά δεδομένα.*

***Αυθεντικοποίηση*** *είναι η διαδικασία με την οποία το πρόσωπο αποδεικνύει ότι είναι ο κάτοχος συγκεκριμένης ταυτότητας και/ή είναι εξουσιοδοτημένο να προβαίνει σε συγκεκριμένες ενέργειες, π.χ. να εισέρχεται σε ελεγχόμενη περιοχή και/ή να έχει πρόσβαση σε συγκεκριμένα αρχεία.*

***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.*

***Εποπτική Αρχή:*** *Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Ιάσονος 1, 1082 Λευκωσία, τηλ. +357 22818456.*

## 3. Περιγραφή & Σκοπός Πολιτικής

Η προστασία των προσωπικών δεδομένων, και ιδιαιτέρως η ασφαλής διαχείριση των προσωπικών δεδομένων των πελατών, ασφαλιστικών διαμεσολαβητών, συνεργατών, προμηθευτών, που προκύπτουν από επιχειρηματικές επαφές, υπαλλήλων της Εταιρείας και άλλων ατόμων που η Εταιρεία έχει σχέση αποτελεί πρωταρχικό μέλημα της Υδρογείου Ασφαλιστικής. Το παρόν εγχειρίδιο αποτελεί διακήρυξη άρχων και αξιών όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, λειτουργεί συμπληρωματικά προς την ισχύουσα νομοθεσία και είναι δεσμευτικό για όλα τα μελή της Εταιρείας, όπου και αν αυτά δραστηριοποιούνται.

Σκοπός του είναι να θέσει συγκεκριμένες παραμέτρους και να καθορίσει τους ρόλους και τις ευθύνες για να διασφαλίσει ότι τόσο η Εταιρεία όσο και οι εξουσιοδοτημένοι υπάλληλοί της ή/και εξουσιοδοτημένοι εξωτερικοί συνεργάτες, φυσικά ή νομικά πρόσωπα συμμορφώνονται με τον ισχύοντα Νόμο, Κανονισμό (ΕΕ) και οδηγίες της Εποπτικής Αρχής. Επιπλέον, το παρόν Εγχειρίδιο στοχεύει στην επίτευξη συμμόρφωσης με τις εσωτερικές πολιτικές και κανονισμούς της Εταιρείας.

Η αποτυχία προστασίας προσωπικών δεδομένων μπορεί να δημιουργήσει πολύ σοβαρά προβλήματα στην Εταιρεία όπως μέτρα επιβολής και κυρώσεις από την εποπτική αρχή, όπως πρόστιμα τα οποία μπορεί να φθάνουν στο 4% του ετήσιου τζίρου της εταιρείας, ποινικές ευθύνες καθώς επίσης ζημία στην καλή φήμη της Εταιρείας. Επιπλέον, η απώλεια τυχαία ή παράνομη ή η τυχαία ή μη αποκάλυψη προσωπικών δεδομένων μπορεί να θέσει τους πελάτες και συνεργάτες σε κίνδυνο και να υπονομεύσει την εμπιστοσύνη των πελατών και της αγοράς έναντι της εταιρείας.

## 4. Στόχοι

Η Πολιτική Προστασίας Προσωπικών Δεδομένων καθορίζει τις αρχές, τους αναγκαίους ελέγχους, τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας που διασφαλίζουν την εμπιστευτικότητα για την προστασία των προσωπικών δεδομένων φυσικών προσώπων που έχει συλλέξει η Εταιρεία για σκοπούς και μόνο της επιχειρηματικής της δραστηριότητας. Η εστίαση των ελέγχων είναι στο "τι" απαιτείται για τη συμμόρφωση με τις πρόνοιες του Νόμου και Ευρωπαϊκού Κανονισμού για την ασφαλή συλλογή, επεξεργασία και διαχείριση των προσωπικών δεδομένων, επιτρέποντας μεγαλύτερη ευελιξία στα τμήματα της Εταιρείας να προσδιορίσουν ποιος είναι ο καλύτερος τρόπος συμμόρφωσης μέσα από τις δικές τους διαδικασίες και διεργασίες ακολουθώντας την παρούσα πολιτική.

## 5. Πεδίο Εφαρμογής

Η Πολιτική απευθύνεται στο σύνολο του προσωπικού της Εταιρείας, τους ασφαλιστικούς διαμεσολαβητές και συνεργάτες της Εταιρείας, που μπορεί να έχουν πρόσβαση σε προσωπικά δεδομένα φυσικών προσώπων που συλλέγει, επεξεργάζεται και διαχειρίζεται η Εταιρεία.

Η πολιτική προστασίας των δεδομένων διασφαλίζει ότι η Υδρόγειος:

- Συμμορφώνεται με την ισχύουσα νομοθεσία περί προστασίας προσωπικών δεδομένων φυσικών προσώπων.
- Προστατεύει τα δικαιώματα του προσωπικού, των πελατών, ασφαλιστικών διαμεσολαβητών και των συνεργατών.
- Καθορίζονται οι υποχρεώσεις όλου του προσωπικού της Εταιρείας, ασφαλιστικών διαμεσολαβητών και συνεργατών ως προς την ασφαλή διαχείριση των προσωπικών δεδομένων ανάλογα με την πρόσβαση που έχει ο καθένας.
- Εφαρμόζει όλα τα απαραίτητα και κατάλληλα τεχνικά και οργανωτικά μέτρα που διασφαλίζουν την ασφάλεια διαχείρισης των προσωπικών δεδομένων, επανεξετάζοντας ανά τακτά χρονικά διαστήματα και αναβαθμίζοντας τα σύμφωνα με τις τεχνολογικές εξελίξεις ή άλλες εκ του νόμου απαιτήσεις.

### 5.1 Νόμος Περί Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα. Ο περί Προστασίας των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα Νόμος και Ευρωπαϊκός Κανονισμός παρέχει δικαιώματα στα φυσικά πρόσωπα (τα υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους συλλέγουν, επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα φυσικών προσώπων (τους υπεύθυνους επεξεργασίας και εκτελών την επεξεργασία).

Όλα τα φυσικά ή νομικά πρόσωπα που συλλέγουν, επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα πρέπει να συμμορφώνονται, ενσωματώνοντας τις απαιτήσεις του νόμου στις συνήθεις επιχειρηματικές τους δραστηριότητες.

Η πράξη προστασίας των δεδομένων στηρίζεται σε 6 σημαντικά σημεία τα οποία έχουν ως ακολούθως:

1. Να συλλέγονται για συγκεκριμένο και νόμιμο σκοπό, με την συγκατάθεση του υποκειμένου των δεδομένων.

2. Να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο **ασύμβατο** με το σκοπό που συλλέγησαν, π.χ. **ελάχιστη πρόσβαση**.

3. Να συλλέγονται **μόνο** όσα εξ' αυτών είναι απαραίτητα.

4. Να είναι ακριβή και να επικαιροποιούνται.

5. Να τηρούνται **μόνο** για όσο χρονικό διάστημα απαιτείται για το σκοπό που συλλέγησαν και σε κάθε περίπτωση για την ελάχιστη περίοδο που απαιτείται από τον νόμο ή από οποιοδήποτε ρυθμιστικό φορολογικό ή άλλο φορέα που έχει δικαιοδοσία πάνω στην Εταιρεία, και

6. Η επεξεργασία τους να γίνεται με τρόπο ώστε να διασφαλίζεται η ασφάλεια τους από τυχόν παραβίαση.

## 6. Έγκριση και Επικαιροποίηση της Πολιτικής

### 6.1 Γενικά

Ο καθορισμός της Πολιτικής Προστασίας των προσωπικών δεδομένων ανήκει στον Υπεύθυνο Προστασίας προσωπικών δεδομένων ο οποίος είναι υπεύθυνος για τη διασφάλιση της, την επικαιροποίηση, την κατάλληλη διανομή της στο προσωπικό, ασφαλιστικούς διαμεσολαβητές και συνεργάτες καθώς και στην παροχή σεμιναρίων κατάρτισης τους για το περιεχόμενό της.

Είναι ευθύνη όλου του προσωπικού, ασφαλιστικών διαμεσολαβητών και συνεργατών να είναι εξοικειωμένοι με το περιεχόμενο της παρούσας πολιτικής και να ασκούν ορθή κρίση ώστε να ενεργούν εντός του πλαισίου αυτής της πολιτικής στην καθημερινή τους εργασία.

Σε κάθε περίπτωση το προσωπικό, ασφαλιστικοί διαμεσολαβητές και συνεργάτες εάν διαπιστώσουν ασάφεια και/ή ελλείψεις στην παρούσα πολιτική οφείλουν να ενημερώσουν άμεσα τον υπεύθυνο προστασίας προσωπικών δεδομένων και να ζητήσουν γραπτώς την καθοδήγηση του.

Οποιεσδήποτε παραβιάσεις της πολιτικής, είτε σκόπιμες είτε όχι, θεωρούνται σοβαρό ζήτημα για την Εταιρεία και θα πρέπει να αποκαλύπτονται άμεσα, να ενημερώνεται ο υπεύθυνος προστασίας προσωπικών δεδομένων και η Επιτροπή Προστασίας προσωπικών δεδομένων και να παραπέμπεται το θέμα για χειρισμό στο Διοικητικό Συμβούλιο της Εταιρείας («ΔΣ»).

### 6.2 Έγκριση της Πολιτικής

Το Διοικητικό Συμβούλιο (Δ.Σ.) είναι το αρμόδιο όργανο για την έγκριση της Πολιτικής Προστασίας Προσωπικών Δεδομένων που εφαρμόζει η Εταιρεία.

Η ισχύς της αρχίζει από την ημέρα που αυτή θα εγκριθεί με απόφαση του Διοικητικού Συμβουλίου και μέχρι την μεταγενέστερη επικαιροποίηση της.

Η επικαιροποίηση της παρούσας πολιτικής καθώς και η καθημερινή παρακολούθηση συμμόρφωσης με τις διαδικασίες έγκειται στον Υπεύθυνο Προστασίας προσωπικών δεδομένων.

### 6.3 Συνεχής Επικαιροποίηση

Η παρούσα πολιτική θα πρέπει να επικαιροποιείται τουλάχιστον σε ετήσια βάση ή όποτε κρίνεται απαραίτητο από τον υπεύθυνο προστασίας προσωπικών δεδομένων και να τίθεται προς έγκριση από το Διοικητικό Συμβούλιο της Εταιρείας σύμφωνα με τις επιχειρησιακές ανάγκες, τηρώντας εσωτερικές κατευθυντήριες γραμμές για συνεχή επαλήθευση της επιχειρησιακής τεκμηρίωσης, ώστε να διασφαλίζεται ότι οι πολιτικές και οι διαδικασίες αντανακλούν τις πλέον πρόσφατες κανονιστικές απαιτήσεις και επιχειρηματικές αλλαγές ή διαδικασίες.

Η Επιτροπή Προσωπικών Δεδομένων σε συνεργασία με τον Υπεύθυνο Προστασίας προσωπικών δεδομένων είναι υπεύθυνοι να επανεξετάζουν και να προ-εγκρίνουν τις αλλαγές στη Πολιτική σε ετήσια βάση και να τις προωθούν στο ΔΣ για τελική έγκριση.

### 6.4 Ευθύνες

Όλοι οι εργοδοτούμενοι της Εταιρείας, ασφαλιστικοί διαμεσολαβητές και συνεργάτες έχουν ευθύνη για την ασφαλή συλλογή, επεξεργασία και διαχείριση των προσωπικών δεδομένων των πελατών.

Κάθε τμήμα της Εταιρείας που χειρίζεται προσωπικά δεδομένα πελατών/συνεργατών πρέπει να διασφαλίζει ότι η συλλογή, επεξεργασία και διαχείριση γίνεται σύμφωνα με τον νόμο πρωταρχικά και σύμφωνα με την παρούσα συμπληρωματική και βοηθητική πολιτική της Εταιρείας.

### 6.5 Ειδικές Ευθύνες

- **Διοικητικό Συμβούλιο**

Το Διοικητικό Συμβούλιο είναι υπεύθυνο για τη διασφάλιση ότι η Εταιρεία εφαρμόζει εκείνα τα κατάλληλα οργανωτικά και τεχνικά μέτρα ούτως ώστε να συμμορφώνεται με τις υποχρεώσεις της που απορρέουν από τον νόμο.

- **Υπεύθυνος Προστασίας Δεδομένων**

- Ενημερώνει την Επιτροπή Προστασίας Προσωπικών Δεδομένων και το ΔΣ σχετικά με τις ευθύνες, τους κινδύνους και τα θέματα προστασίας προσωπικών δεδομένων.
- Επανεξετάζει κατά τακτά χρονικά διαστήματα όλες τις διαδικασίες, τεχνικά και οργανωτικά μέτρα προστασίας των προσωπικών δεδομένων που εφαρμόζει η Εταιρεία.
- Οργανώνει εκπαιδεύσεις αναφορικά για την προστασία των προσωπικών δεδομένων για όλο το προσωπικό της Εταιρείας και για τα άτομα τα οποία καλύπτονται από αυτήν την πολιτική.
- Χειρίζεται / Αντιμετωπίζει τυχόν ερωτήματα όσο αναφορά την προστασία προσωπικών δεδομένων τόσο από το προσωπικό της Εταιρείας όσο και από εξωτερικούς φορείς και δίνει απαντήσεις.
- Ασχολείται με αιτήματα από άτομα τα οποία θέλουν να ενημερωθούν για τα προσωπικά δεδομένα τα οποία διατηρεί η Εταιρεία για αυτούς ( subject access requests).

- Είναι υπεύθυνος για τον έλεγχο και την έγκριση οποιωνδήποτε συμβάσεων ή συμφωνιών με συνεργάτες και/ή άλλους τρίτους που ενδέχεται λόγω της συνεργασίας να τους αποκαλύπτονται νόμιμα και κάτω από συγκεκριμένες διαδικασίες προσωπικά δεδομένα πελατών.
- Αναλύει και ελέγχει τις δραστηριότητες των τμημάτων της εταιρείας και κατά πόσο οι επεξεργασίες είναι σύμφωνες με τον Νόμο και Κανονισμό και ενημερώνει την διεύθυνση. Συμβουλεύει την διεύθυνση στην σύνταξη πολιτικών ασφαλείας και προστασίας προσωπικών δεδομένων.

❖ **Τμήμα Πληροφορικής**

- Εξασφαλίζει ότι όλα τα λογισμικά συστήματα, οι υπηρεσίες και ο εξοπλισμός που χρησιμοποιούνται για την συλλογή, αποθήκευση και επεξεργασία δεδομένων προσωπικού χαρακτήρα πληρούν τα αποδεκτά πρότυπα ασφαλείας.
- Επαναξιολογεί κατά τακτά χρονικά διαστήματα όλα τα συστήματα ασφαλείας τα οποία χρησιμοποιεί για την προστασία των προσωπικών δεδομένων και εισηγείται προς τον Υπεύθυνο Προστασίας Προσωπικών δεδομένων και την Επιτροπή Προστασίας Προσωπικών δεδομένων την βελτίωση τους, την αντικατάσταση τους από πιο σύγχρονα και εξελιγμένα συστήματα.
- Εκτελεί τακτικούς ελέγχους και σαρώσεις για να διασφαλίσει ότι το λογισμικό ασφαλείας λειτουργεί σωστά και είναι αξιόπιστο.
- Αξιολογεί από άποψη ασφαλείας οποιεσδήποτε παροχές υπηρεσιών από τρίτα μέρη που η Εταιρεία σκέπτεται να χρησιμοποιήσει για να αποθηκεύσει ή να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα. Για παράδειγμα, υπηρεσίες cloud computing.
- Ενημερώνει άμεσα γραπτώς τον Υπεύθυνο Προστασίας Προσωπικών δεδομένων και την Επιτροπή Προστασίας Προσωπικών δεδομένων για τυχόν κινδύνους που εντοπίζει για την ασφάλεια των προσωπικών δεδομένων και εισηγείται τρόπους αντιμετώπισης τους.
- Ενημερώνει άμεσα γραπτώς τον Υπεύθυνο Προστασίας Προσωπικών δεδομένων και την Επιτροπή Προστασίας Προσωπικών δεδομένων για τυχόν διαρροή σκόπιμη ή μη και/ή κλοπή προσωπικών δεδομένων από τα λογισμικά συστήματα.

❖ **Επιτροπή Προσωπικών Δεδομένων**

- Συνεδριάζει ανά εξάμηνο και ενημερώνεται από τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων ο οποίος παρουσιάζεται ενώπιον της σχετικά με τα προβλήματα, ευθύνες, τους κινδύνους και τα θέματα προστασίας προσωπικών δεδομένων που απασχολούν την Εταιρεία.
- Παρέχει κάθε αναγκαία υποστηρικτική συνδρομή στον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων ούτως ώστε να εκτελεί τα ανατεθειμένα σε αυτόν καθήκοντα με ευχέρεια.
- Επανεξετάζει κατά τακτά χρονικά διαστήματα όλες τις διαδικασίες, τεχνικά και οργανωτικά μέτρα προστασίας των προσωπικών δεδομένων που εφαρμόζει η Εταιρεία σε συνεργασία με τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων και από κοινού λαμβάνουν αποφάσεις για την τυχόν βελτίωση ή αντικατάσταση τους ενημερώνοντας το ΔΣ.

## 7. Διαχείριση Προσωπικών Δεδομένων

### 7.1. Συλλογή Προσωπικών Δεδομένων

Η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα των πελατών, συνεργατών και εργαζομένων πραγματοποιείται με θεμιτά μέσα και με τρόπο ώστε να διασφαλίζεται ο σεβασμός της ιδιωτικής ζωής, της προσωπικότητας και της ανθρώπινης αξιοπρέπειας και, γενικότερα, στο πλαίσιο των πελατειακών, συμβατικών και εργασιακών σχέσεων, και μόνον εφ' όσον είναι αναγκαίο για την εκπλήρωση του επιδιωκόμενου σκοπού.

Τα δεδομένα προσωπικού χαρακτήρα συλλέγονται και υφίστανται επεξεργασία για σαφείς και καθορισμένους σκοπούς (π.χ. αξιολόγηση της πρότασης και/ή πρόσθετης πράξης ασφάλισης, εκτίμηση και αποδοχή ασφαλιστικού κινδύνου, καθορισμός ασφαλίστρου, η εκτέλεση της σύμβασης ασφάλισης, η έκδοση του ασφαλιστηρίου, η διαχείριση του ασφαλιστηρίου, η τυχόν ανανέωση του, η τυχόν διαχείριση απαίτησης που προκύπτει από το ασφαλιστήριο, η οποιαδήποτε οικονομική συναλλαγή, οι από συμβάσεις παροχή υπηρεσιών, από τις εργασιακές συμβάσεις), όπου οι σκοποί της επεξεργασίας είναι εκ των προτέρων γνωστοί και κατανοητοί από τους πελάτες, συνεργάτες και εργαζομένους και εξασφαλίζεται η συγκατάθεση τους.
Τα δεδομένα προσωπικού χαρακτήρα είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά χρειάζονται ενόψει των σκοπών για τον οποίο συντελείται η συλλογή και επεξεργασία.

Όλα τα φυσικά πρόσωπα που αποτελούν το υποκείμενο δεδομένων και των οποίων δεδομένα κατέχονται από την Εταιρεία δικαιούνται υποβάλλοντας γραπτό αίτημα στον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων, να πληροφορούνται και/ή να ζητούν:

- Για το ποια προσωπικά δεδομένα κατέχει η Εταιρεία για αυτούς και για ποιο σκοπό,
- Πώς μπορούν να αποκτήσουν πρόσβαση σε αυτά,
- Ποιοι είναι οι αποδέκτες των προσωπικών τους δεδομένων,
- Διόρθωση των δεδομένων τους εάν τα δεδομένα είναι ανακριβή,
- Διαγραφή των δεδομένων εάν επεξεργάζονται παράνομα και/ή αν ο σκοπός για τον οποίο συνελέγησαν, έπαυσε να υπάρχει,
- Επικαιροποίηση τους
- Ανάκληση της συγκατάθεσης τους για επεξεργασία των προσωπικών τους δεδομένων (νοείται ότι η ανάκληση συγκατάθεσης δεν θίγει την νομιμότητα της επεξεργασίας που βασίστηκε στην συγκατάθεση τους προ της ανάκλησης)
- Την διαγραφή και/ή περιορισμό από τον υπεύθυνο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τους αφορούν εάν δεν είναι πλέον απαραίτητα με σχέση με το σκοπό που συλλέχθηκαν.
- Να εναντιώνονται στην επεξεργασία προσωπικών δεδομένων τους, ιδίως για σκοπούς απευθείας εμπορικής προώθησης, περιλαμβανομένης της κατάρτισης προφίλ εάν σχετίζεται με αυτή της απευθείας εμπορικής προώθησης.
- Την διαβίβαση των δεδομένων προσωπικού χαρακτήρα που τους αφορούν και τα οποία κατέχει η Εταιρεία απευθείας σε άλλο υπεύθυνο επεξεργασίας σε περίπτωση που αυτά είναι τεχνικά εφικτό.

Ο υπεύθυνος προστασίας προσωπικών δεδομένων πρέπει πάντα να επαληθεύει την ταυτότητα των αιτούντων πριν από την παράδοση οποιασδήποτε πληροφορίας.

Σε περίπτωση λήξης της σχέσης με τα ενδιαφερόμενα – εμπλεκόμενα μέρη, τα προσωπικά δεδομένα διατηρούνται από την Εταιρεία σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων για τουλάχιστον δώδεκα (12) έτη και σε κάθε περίπτωση την ελάχιστη περίοδο που απαιτείται από τον νόμο ή από οποιονδήποτε ρυθμιστικό φορέα ή μεγαλύτερο χρόνο εάν απαιτείται από τον νόμο ή φορέα που έχει δικαιοδοσία πάνω σε αυτή.

Σε περίπτωση που η Εταιρεία επιθυμεί να αποθηκεύσει τα δεδομένα και μετά την παρέλευση της περιόδου κατά την οποία εξυπηρετούν τον αρχικό τους σκοπό, θα πρέπει να τα ανωνυμοποιήσει ή να τα ψευδωνυμοποιήσει που να μην επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων. Στην επιλογή ψευδωνυμοποίησης, πρέπει να λαμβάνονται ιδιαίτερα μέτρα προστασίας έναντι της χρήσης των κλειδιών αποκρυπτογράφησης από πρόσωπα τα οποία δεν διαθέτουν σχετική άδεια.

### 7.2. Επικαιροποίηση Δεδομένων

Θα πρέπει να εξασφαλίζεται ότι τα προσωπικά δεδομένα που συλλέγονται είναι ακριβή.

Το προσωπικό της Εταιρείας θα πρέπει να χρησιμοποιεί κάθε ευκαιρία που του δίνεται εάν εμπίπτει στην αρμοδιότητα του να επιβεβαιώνει τα συλλεγέντα δεδομένα και αν εντοπίζει λάθη

να προβαίνει σε άμεση διόρθωση και επικαιροποίηση τους ώστε να διασφαλίζεται η ακρίβεια τους. Π.χ. επιβεβαιώνοντας τα στοιχεία του πελάτη, όταν μας καλεί, σε περίπτωση ανανέωσης του συμβολαίου του, τροποποίησης του συμβολαίου του ή σύναψης άλλου συμβολαίου.

Τα προσωπικά δεδομένα θα πρέπει επίσης να διορθώνονται όταν ανακαλύπτονται ανακρίβειες είτε μέσω των ημερήσιων ελέγχων που παρέχει η Διεύθυνση Διαχείρισης Κινδύνων & Αναλογιστικής προς τα επιχειρησιακά τμήματα ή μέσω τηλεφωνικής επικοινωνίας με τους πελάτες και συνεργάτες καθώς επίσης μέσω τις διαδικασίας ανανέωσης συμβολαίων και συμβάσεων με τα ενδιαφερόμενα μέρη.

Επικαιροποίηση προσωπικών δεδομένων γίνεται επίσης και κατόπιν αιτήματος προς την Εταιρεία του πελάτη, συνεργάτη, πάροχου σε περιπτώσεις αλλαγής των στοιχείων του.

### 7.3. Προστασία Προσωπικών Δεδομένων

Λαμβάνουμε τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων πελατών, συνεργατών και των υπαλλήλων της εταιρείας από παραβίαση τους ή από μη εξουσιοδοτημένη πρόσβαση ή χρήση από μη εξουσιοδοτημένα πρόσωπα, είτε εξωτερικά είτε εσωτερικά.

Η πρόσβαση σε προσωπικά δεδομένα γίνεται μόνο μετά από έλεγχο ταυτότητας του χρήστη και αυτό αποτελεί μέρος της διαδικασίας ελέγχου και προστασίας για να μην υπάρξει χρήση από μη εξουσιοδοτημένα πρόσωπα

Η φυσική πρόσβαση στις εγκαταστάσεις του Μηχανογραφικού Κέντρου και του κτηρίου ελέγχεται από εξωτερική και εσωτερική περίμετρο από ολοκληρωμένα συστήματα συναγερμού και 24ωρη παρακολούθηση βίντεο από το κέντρο επιχειρήσεων.

Η λογική πρόσβαση σε προσωπικά δεδομένα περιορίζεται σύμφωνα με την επιχειρησιακή ανάγκη από διαδικασίες έγκρισης πρόσβασης βάση εργασιακών ρόλων, έλεγχο ταυτότητας (authentication), ελαχιστοποίηση και περιορισμένη πρόσβαση σε δεδομένα παραγωγής και άλλα στοιχεία ελέγχου.

Τα δικαιώματα πρόσβασης των χρηστών επιθεωρούνται κάθε έξι (6) μήνες από τον υπεύθυνο του κάθε τμήματος κατόπιν αποστολής της λίστας με τις λεπτομερείς προσβάσεις των χρηστών από το Τμήμα Πληροφορικής.

Για την καταγραφή των δραστηριοτήτων των χρηστών το Τμήμα Πληροφορικής της Εταιρείας μας είναι στην διαδικασία να εφαρμόσει αναλυτική εφαρμογή (DPL – Data Loss Prevention) η οποία θα μπορεί να διασφαλίσει στον μέγιστο βαθμό την ακεραιότητα των δεδομένων αλλά και να τοποθετηθούν περαιτέρω δικλείδες ασφαλείας.

Επιπλέον, όλα τα δεδομένα της Εταιρείας υπόκεινται σε κρυπτογράφηση, συμπεριλαμβανομένων και των εφεδρικών. Για περιπτώσεις απομάκρυνσης πρόσβασης χρηστών στο τεχνολογικό δίκτυο της Εταιρείας, γίνεται με χρήση βιομηχανικών πρωτοκόλλων ασφαλείας (secure transport – VPN) για την προστασία της μεταδιδόμενης πληροφορίας μέσω δημόσιων ή οικιακών δικτύων ενώ παράλληλα είμαστε στην διαδικασία ενεργοποίησης της προστασίας διπλού έλεγχου (Second Factor Authenticator).

### 7.4. Απόρριψη, Διαγραφή, Πάγωμα, Φορητότητα/Διαβίβαση Προσωπικών Δεδομένων & Περιορισμός Επεξεργασίας

Για την ασφαλή απόρριψη των προσωπικών δεδομένων και πληροφοριών που αφορούν πελάτες, συνεργάτες και εργαζόμενους της Εταιρείας σε έντυπη μορφή και άλλες έντυπες μορφές όπως μικροδιαφάνειες (microfilm / microfiche) είναι υπεύθυνο το κάθε πρόσωπο – εργοδοτούμενος που έχει την σχετική πρόσβαση και θα πρέπει να απορρίπτονται στον κλειδωμένο κάδο εμπιστευτικών απορριμμάτων ο οποίος βρίσκεται στον 2$^{ov}$ όροφο του κτιρίου, ή να καταστρέφονται με τη χρήση καταστροφέα τεμαχισμού χαρτιού (shredder).

Για την καταστροφή προσωπικών δεδομένων και πληροφοριών σε ηλεκτρονική μορφή αποθηκευμένα σε φορητό μαγνητικό μέσω π.χ. σκληρός δίσκος, CD, USB, πρέπει να γίνεται ολική διαγραφή του μέσου (format) και όχι απλή διαγραφή (delete) πριν την απόρριψη ή επαναχρησιμοποίηση του και θα πρέπει να ζητείται η βοήθεια του τμήματος Πληροφορικής της εταιρείας.

Σε περίπτωση αποθηκευμένων προσωπικών δεδομένων και πληροφοριών σε φορητό υπολογιστή (π.χ. lap top, tablet) ή τηλεφωνική συσκευή (π.χ. iPhone), πρέπει να γίνεται ολική διαγραφή του μέσου (format) και όχι απλή διαγραφή (delete) πριν την απόρριψη ή επαναχρησιμοποίηση του και θα πρέπει, αν χρειάζεται, να ζητείται η βοήθεια του τμήματος Πληροφορικής της εταιρείας.

Η Εταιρεία, μετά από σχετικό αίτημα ολικής ή περιορισμένης διαγραφής ή παγώματος προσωπικών δεδομένων που θα λάβει από ενδιαφερόμενα μέρη, πελάτες, συνεργάτες, προσωπικό θα πρέπει α) να επαληθεύσει την ταυτότητά του αιτητή β) να αξιολογήσει τις επιπτώσεις (νομική, κανονιστική, συμβατική, επιχειρησιακή, λειτουργική) που μπορεί να προκαλέσει η διαγραφή ή/και το πάγωμα των προσωπικών δεδομένων, και μετά να προβεί στις απαραίτητες ενέργειες σύμφωνα με το αίτημα που έλαβε. Επίσης, η ίδια διαδικασία θα ακολουθηθεί σε περίπτωση αντίστοιχου αιτήματος που θα αφορά τον πιθανό περιορισμό επεξεργασίας προσωπικών δεδομένων ή/και την διαβίβασή τους σε άλλο υπεύθυνο επεξεργασίας.

### 7.5. Πρόσβαση σε Προσωπικά Δεδομένα από το Υποκείμενο Δεδομένων

Όπου ζητηθεί πρόσβαση σε προσωπικά δεδομένα από τον ιδιοκτήτη τους – υποκείμενο των δεδομένων και τα οποία διατηρούνται στα τεχνολογικά συστήματα της Εταιρείας, θα πρέπει να ακολουθείται η ακόλουθη διαδικασία για την ικανοποίηση του αιτήματος:

1) Το υποκείμενο, θα πρέπει να αιτείται γραπτώς την πρόσβαση στα δεδομένα του και το έντυπο συνυπογράφεται από τον αιτητή αλλά και από τον υπεύθυνο προσωπικών δεδομένων – DPO.

2) Το αίτημα προωθείται στο τμήμα πληροφορικής και έπειτα εξάγονται τα δεδομένα που αφορούν το υποκείμενο από την βάση δεδομένων της Εταιρείας και του δίνονται υπό μορφή προγράμματος excel. Επιπρόσθετα, αν κάποια δεδομένα που αφορούν το υποκείμενο έχουν να κάνουν με φωτογραφικό υλικό ή άλλα αρχεία εκτός της βάσης δεδομένων τα οποία είναι αποθηκευμένα σε κάποιο φάκελο, αυτά αποθηκεύονται σε φορητό μαγνητικό μέσο το οποίο προσκομίζει ο ίδιος.

3) Το υποκείμενο ταυτόχρονα με την λήψη των προσωπικών δεδομένων του για τα οποία αιτήθηκε, θα πρέπει να υπογράφει σχετικό έντυπο παραλαβής που να αναφέρει συγκεκριμένα τι παραλήφθηκε από αυτό.

### 7.6. Υποχρεώσεις Προσωπικού για την ασφαλή Διαχείριση και Επεξεργασία Προσωπικών Δεδομένων

Καμία προσωπική χρήση και επεξεργασία δεν επιτρέπεται από το προσωπικό σε προσωπικά δεδομένα και πληροφορίες πελατών, συνεργατών και εργαζόμενων της Εταιρείας.

Δεν πρέπει να χρησιμοποιείται το ηλεκτρονικό ταχυδρομείο (email) ή οποιαδήποτε τεχνολογικά συστήματα της Εταιρείας για διαβίβαση προσωπικών δεδομένων και πληροφοριών που αφορούν πελάτες, συνεργάτες και εργαζόμενους της Εταιρείας σε προσωπικό λογαριασμό ηλεκτρονικού ταχυδρομείου (personal email) παρά μόνο σε εξαιρετικές περιπτώσεις μετά από γραπτή έγκριση του Διευθυντή του τμήματος τους και αποκλειστικά και μόνο για τους σκοπούς της εργασίας τους.

Πρέπει να χρησιμοποιείται κρυπτογράφηση για την ηλεκτρονική διαβίβαση αν καταστεί ανάγκη προσωπικών δεδομένων και πληροφοριών που αφορούν πελάτες, συνεργάτες και εργαζόμενους της Εταιρείας.

Σε περίπτωση αποστολής προσωπικών δεδομένων μέσω ταχυδρομείου εκτός Εταιρείας, πρέπει να υπάρχει επιχειρησιακός λόγος για τις πληροφορίες που αποστέλλονται και ο παραλήπτης να έχει νόμιμο δικαίωμα στις πληροφορίες αυτές.

Εάν η ταχυδρομική αποστολή γίνεται σε συνεργάτη, πάλι πρέπει να απευθύνεται ονομαστικά σε πρόσωπο και να υπάρχει συμφωνία εμπιστευτικότητας (non-disclosure agreement). Η συσκευασία σφραγίζεται, δεν πρέπει να είναι διαφανής και να υπάρχει η ένδειξη παραβίασης (tampered evidence). Η αποστολή πρέπει να γίνεται μέσω εγκεκριμένου μεταφορέα ή συστημένο ταχυδρομείο και χρήσης μηχανισμού παρακολούθησης (tracking).

Για τυπωμένη πληροφορία που περιέχει προσωπικά δεδομένα και στέλνεται εντός της Εταιρείας και των υποκαταστημάτων της πρέπει να είναι σε σφραγισμένη συσκευασία και να παραδίδεται ιδιοχείρως έναντι υπογραφής παραλαβής. Για αποστολή μέσω εσωτερικού ταχυδρομείου πρέπει να αναφέρεται το όνομα και διεύθυνση του παραλήπτη και να επιβεβαιώνεται η παραλαβή.

Το προσωπικό θα πρέπει να γνωρίζει και να εφαρμόζει περαιτέρω τα ακόλουθα:

α) να μη συζητά προσωπικά δεδομένα και/ή πληροφορίες αχρείαστα όπου και να βρίσκεται

β) να μη συζητά προσωπικές πληροφορίες σε χώρους όπου μπορεί να το ακούσουν μη εξουσιοδοτημένα τρίτα πρόσωπα και να γίνει διαρροή.

γ) να είναι προσεκτικό όταν απαντά σε ερωτήσεις μέσω τηλεφώνου. Να μην δίνει αμέσως προσωπικές πληροφορίες. Εάν έχει οποιεσδήποτε υποψίες, για την ταυτότητα του προσώπου που το καλεί να ζητήσει τον αριθμό τηλεφώνου του καλούντος και να ελέγξει τον αριθμό (π.χ. με τη χρήση κλήσης τηλεφωνικού κέντρου εταιρείας, τηλεφωνικό κατάλογο ή αρχείο πελατών ή να ζητήσει άλλα στοιχεία επιβεβαίωσης της ταυτότητας του),

δ) να μην αφήνει μηνύματα σε τηλεφωνητή που περιέχουν προσωπικά δεδομένα πελατών, συνεργατών και εργαζομένων της Εταιρείας, και

ε) να χρησιμοποιεί με ασφάλεια τηλεφωνικές διασκέψεις, διαδικτυακές και τηλεδιασκέψεις προστατεύοντας τα διαπιστευτήρια πρόσβασης και επαλήθευσης εξασφαλίζοντας την ένταξη μόνο σε εξουσιοδοτημένους συμμετέχοντες.

### 7.7. Χρήση Τεχνολογικών Συστημάτων για Προστασία

Η πρόσβαση χρηστών, συμπεριλαμβανομένου και του απαιτούμενου επιπέδου δικαιώματος πρόσβασης, πρέπει να παρέχει στους χρήστες πρόσβαση στα συστήματα πληροφορικής της εταιρείας ανάλογα με τις επιχειρησιακές απαιτήσεις και τις απαιτήσεις του εργασιακού τους ρόλου και όχι πέρα αυτού.

Ο κάθε υπάλληλος είναι υπεύθυνος για την προστασία των κωδικών πρόσβασής του και για τη μυστική διατήρησή τους. Ιδίως θα πρέπει:

α) να δημιουργήσει κωδικούς πρόσβασης που:

• είναι τουλάχιστον δέκα (10) χαρακτήρες σε μήκος,

• περιέχουν χαρακτήρες από τουλάχιστον τρία από τα ακόλουθα:
- Αριθμούς,
- Κεφαλαία γράμματα,
- Πεζά γράμματα, και
- Ειδικούς χαρακτήρες (π.χ. & ^%),

• είναι διαφορετικοί από το μοναδικό σας αναγνωριστικό όνομα χρήστη (user-id),

• είναι εύκολο για σας να το θυμάστε αλλά δύσκολο για κάποιον άλλο να το μαντέψει,

• Διαφέρουν από τα δέκα (10) τελευταία passwords του χρήστη
- δεν περιέχει δυο (2) συνεχόμενους χαρακτήρες από το user-id
-είναι τουλάχιστον έξι (6) χαρακτήρες

β) να μην γράφει ή αποκαλύπτει σε κανέναν τους κωδικούς πρόσβασής του.

Ο κάθε υπάλληλος είναι υπεύθυνος για την ασφαλή διατήρηση των προσωπικών δεδομένων και πληροφοριών που αφορούν πελάτες, συνεργάτες και εργαζόμενους της Εταιρείας κατά τη χρήση φορητών υπολογιστών (laptops), φορητές συσκευές (portable devices) και τα αφαιρούμενα μέσα (removable media) κατά τον χρόνο εκτέλεσης της εργασίας του και ή σε οποιονδήποτε άλλο χρόνο για σκοπούς εκτέλεσης της εργασίας του. Ιδίως θα πρέπει:

α) να χρησιμοποιεί το φορητό υπολογιστή, τις φορητές συσκευές και τα αφαιρούμενα μέσα που του παραχωρεί η εταιρεία με υπευθυνότητα όπου και αν βρίσκεται και μόνο για σκοπούς εκτέλεσης της εργασίας του. Για παράδειγμα, να τοποθετεί την οθόνη του ηλεκτρονικού υπολογιστή του σε τέτοια θέση έτσι ώστε να μην μπορούν να δουν το περιεχόμενο της μη εξουσιοδοτημένα πρόσωπα,

β) να έχει μαζί του και σε ασφαλή θέση ανά πάσα στιγμή το φορητό υπολογιστή του, κινητή συσκευή και αφαιρούμενα μέσα όταν δεν είναι ασφαλώς κλειδωμένα,

γ) να ασφαλίζει το φορητό υπολογιστή του, όταν δεν είναι σε χρήση με καλώδιο ή αλυσίδα με κλειδαριά στο γραφείο του ή σε ένα κλειδωμένο συρτάρι ή ντουλάπι,

δ) να μην αφήνει το φορητό υπολογιστή του, τις κινητές συσκευές χωρίς επίβλεψη σε βεστιάρια, ή άλλους χώρους όπου θα μπορούσε να γίνουν αντικείμενο κλοπής,

ε) να μην αφήνει το φορητό υπολογιστή του, φορητές συσκευές και τα αφαιρούμενα μέσα, μέσα σε αυτοκίνητο κατά τη διάρκεια της νύχτας. Αν πρέπει να αφήσει το φορητό υπολογιστή του σε αυτοκίνητο κατά τη διάρκεια της ημέρας, δεν πρέπει να είναι ορατός, και

στ) να επιστρέφει τα τεχνολογικά περιουσιακά στοιχεία, συμπεριλαμβανομένων φορητών υπολογιστών, φορητών συσκευών, αφαιρούμενα μέσα, στον άμεσο προϊστάμενό του όταν αποχωρήσει από την εταιρεία, ή μετακινηθεί σε άλλο τμήμα εντός της Εταιρείας.

ζ) δεν πρέπει να χρησιμοποιεί προσωπικές ιδιόκτητες συσκευές, όπως φορητούς ηλεκτρονικούς υπολογιστές, φορητές συσκευές (π.χ usb) και/ή άλλα αφαιρούμενα μέσα κατά την εκτέλεση της εργασίας του για σκοπούς αποθήκευσης συλλεγέντων προσωπικών δεδομένων παρά μόνο αυτά που του δίδονται από την εταιρεία.

η) σε περίπτωση δε που του παραχωρηθεί από την εταιρεία φορητός υπολογιστής, φορητή συσκευή και/ή αφαιρούμενο μέσο θα πρέπει να είναι προσεκτικός και να τα προστατεύει από κακόβουλο λογισμικό και ιούς και να αναφέρει κάθε τέτοια περίπτωση στο τμήμα πληροφορικής της εταιρείας. Να χρησιμοποιεί «τοίχους προστασίας» (firewall) για φορητούς υπολογιστές πριν από την χρήση απομακρυσμένης πρόσβασης. Να εφαρμόζει προγράμματα ασφαλείας (patches) σύμφωνα με τον κατασκευαστή του λογισμικού.

### 7.8. Συνεργάτες

Πρέπει να υπογράφεται ταυτόχρονα με την σύμβαση παροχής υπηρεσιών με τους Συνεργάτες, Πάροχους και Προμηθευτές, η υπεύθυνη δήλωση ανάληψης υποχρεώσεων έναντι της εταιρείας για την προστασία των προσωπικών δεδομένων από αυτούς εις τα οποία θα τους δοθεί

πρόσβαση η οποία έχει ετοιμαστεί από την εταιρεία. Τυχόν απόκλιση από το έγγραφο της εταιρείας θα πρέπει να εγκρίνεται από την επιτροπή προστασίας προσωπικών δεδομένων της εταιρείας.

### 7.9. Διαδικασίες στις Περιπτώσεις Απώλειας, διαρροής ή Κλοπής Προσωπικών Δεδομένων

Ο κάθε υπάλληλος θα πρέπει να κατανοήσει και να συμμορφώνεται με τις διαδικασίες σχετικά με την αναφορά συμβάντων απώλειας, διαρροής ή κλοπής προσωπικών δεδομένων. Θα πρέπει:

α) να αναφέρει άμεσα κάθε πραγματικό ή ύποπτο περιστατικό απώλειας, διαρροής ή κλοπής ή προσπάθειας να γίνουν αυτά χωρίς καθυστέρηση στον Διευθυντή ή Προϊστάμενό του και στον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων, και

β) να μη συζητά, χωρίς έγκριση, τις λεπτομέρειες πραγματικών ή ύποπτων περιστατικών προσωπικών δεδομένων με οιονδήποτε άλλο τρίτο πρόσωπο.

Παραδείγματα περιστατικών απώλειας ή κλοπής προσωπικών δεδομένων περιλαμβάνουν:

- απώλεια ή κλοπή πληροφοριών και περιουσιακών στοιχείων, όπως φορητές ή αφαιρούμενες συσκευές, αρχεία κλπ,
- μη εξουσιοδοτημένη πρόσβαση εντός ή εκτός της Εταιρείας (π.χ. hacking) ή παραβίαση ιστοσελίδων ή δικτύου με αποτέλεσμα την απώλεια ή αλλοίωση προσωπικών δεδομένων,
- οποιοδήποτε κακόβουλο λογισμικό ή ιούς που έχει κατεβάσει στον υπολογιστή του,
- τυχόν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές κλήσεις που έχετε λάβει από κάποιον που ζητά πληροφορίες σχετικά με προσωπικά δεδομένα,
- υπόνοια ή πραγματική υποκλοπή κωδικού πρόσβασης (password),
- προσωπικά δεδομένα και πληροφορίες που αποστέλλονται εκτός της Εταιρείας και δεν έχουν φθάσει στον προορισμό τους, και
- μη ασφαλή απόρριψη προσωπικών δεδομένων και πληροφοριών.

Σε περίπτωση παραβίασης που θα έχει ως συνέπεια την πιθανή διαγραφή, αλλοίωση ή διαρροή προσωπικών δεδομένων η Εταιρεία σε συνεργασία με τον Υπεύθυνο Προστασίας προσωπικών δεδομένων και το Τμήμα Πληροφορικής θα πρέπει να ενεργοποιήσει την Διαδικασία Διαχείρισης Συμβάντων ή/και την Διαδικασία Διαχείριση Κρίσεων και θα κοινοποιήσει το συμβάν άμεσα και το αργότερο εντός 72 ωρών στην εποπτική αρχή και στα ενδιαφερόμενα μέρη - παθόντες πελάτες, συνεργάτες, πάροχοι, λαμβάνοντας ταυτόχρονα όλα τα απαραίτητα μέτρα για την αποκατάσταση των πιθανών ζημιών που θα έχουν προκληθεί.

Τα μέσα κοινοποίησης μπορεί να περιλαμβάνουν και κατά περίπτωση, έντυπες επιστολές μέσω ταχυδρομείου, μηνύματα μέσω ηλεκτρονικού ταχυδρομείου (email), κοινοποίηση μέσω της εταιρικής ιστοσελίδας (WEB), ανακοίνωση μέσο τύπου και μέσων μαζικής ενημέρωσης.

### 7.10. Κανόνες Κοινής Χρήσης και Διαβίβασης Προσωπικών Δεδομένων εκτός Εταιρείας

Τα δεδομένα προσωπικού χαρακτήρα μπορεί να διαβιβάζονται ή να κοινοποιούνται σε τρίτους μόνο για σκοπούς που σχετίζονται άμεσα με την επιτέλεση του σκοπού για τον οποίο συλλέγησαν ή εφόσον η διαβίβαση προβλέπεται από νόμο και συνάδει με τα οριζόμενα σε αυτόν (π.χ. διαβίβαση σε ασφαλιστικούς οργανισμούς).

Οι κανόνες για την διαβίβαση ή κοινοποίηση δεδομένων προσωπικού χαρακτήρα εφαρμόζονται και εντός της εργασιακής μονάδας/ εντός της εργασίας. Στην περίπτωση αυτή επιτρέπεται μόνο προς πρόσωπα ειδικά προς τούτο εξουσιοδοτημένα από τον Υπεύθυνο Επεξεργασίας (ΥΕ) και μόνο στο πλαίσιο και στο μέτρο που αυτό είναι αναγκαίο για την εκπλήρωση ειδικού καθήκοντος ή ειδικά προσδιορισμένης εργασίας που έχει ανατεθεί στα πρόσωπα αυτά.

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, δηλαδή σε χώρες που δεν ανήκουν στην Ευρωπαϊκή Ένωση, υπόκειται στις ρυθμίσεις του νόμου και Ευρωπαϊκού Κανονισμού (ΕΕ) Περί προστασίας προσωπικών δεδομένων και σε καμία περίπτωση δεν θα διαβιβάζονται χωρίς την γραπτή συγκατάθεση του Υπεύθυνου Προστασίας προσωπικών δεδομένων της εταιρείας. Οι κανόνες και περιορισμοί αυτοί ισχύουν ακόμη και εάν τα δεδομένα προσωπικού χαρακτήρα των εργαζομένων διαβιβάζονται σε μητρικές, θυγατρικές ή συνδεδεμένες επιχειρήσεις, που έχουν την έδρα τους σε τρίτη χώρα.

## 8. Κίνδυνοι που Αντιμετωπίζονται από τη Πολιτική Προστασίας Προσωπικών Δεδομένων

Χωρίς αποτελεσματική προστασία, τα προσωπικά δεδομένα θα μπορούσαν:

• να κλαπούν, ή να αποκαλυφθούν χωρίς έγκριση,

• να μην είναι διαθέσιμα όταν απαιτείται από τις επιχειρησιακές διαδικασίες ή για χρήση,

• να καταστραφούν χωρίς έγκριση, ή να διασφαλιστεί ανεπαρκώς η πλήρης αποκατάστασή τους,

• να αλλάξουν χωρίς έγκριση, εσκεμμένα ή κατά λάθος,

• να γίνει κατάχρηση χρήσης ή για άλλους σκοπούς πέρα για τους σκοπούς για τους οποίους συλλέγησαν από τους υπάλληλους, τους συνεργάτες, ή και από τρίτους και

## 9. Υπεύθυνα Πρόσωπα

Η επιτροπή προστασίας προσωπικών δεδομένων σε συνεργασία με τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων έχει την ευθύνη για την εφαρμογή και τη συνεχή παρακολούθηση συμμόρφωσης με την Πολιτική Προστασίας Προσωπικών Δεδομένων.

Οι Διευθυντές και οι Προϊστάμενοι των Τμημάτων είναι υπεύθυνοι και έχουν την υποχρέωση να υποστηρίζουν και να ελέγχουν την εφαρμογή της παρούσας Πολιτικής από τις διευθύνσεις και τα τμήματά τους, καθώς και να προβαίνουν σε συνεχή παρακολούθηση συμμόρφωσης με την Πολιτική Προστασίας Προσωπικών Δεδομένων εντός της επιχείρησης και την εφαρμογή των ελέγχων για το σκοπό αυτό. Για κάθε διευκρίνιση και/ή αμφιβολία θα πρέπει να απευθύνονται στον Υπεύθυνο Προστασίας προσωπικών δεδομένων γραπτώς.

**10.** Η παρούσα Πολιτική σε καμία περίπτωση δεν υποκαθιστά με οποιονδήποτε τρόπο τον Νόμο και τον Ευρωπαϊκό Κανονισμό.