Πολιτική Προστασίας Αρχείων Εταιρίας Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα και Πληροφοριών της MetLife Alico

<u>Προστασία Αρχείων Εταιρίας και Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα και Πληροφοριών</u>

Η τεχνολογία έχει αυξήσει σημαντικά τη μεταφορά και ανταλλαγή προσωπικών πληροφοριών.

Οι πελάτες μας, μας εμπιστεύονται αρκετές προσωπικές τους πληροφορίες και περιμένουν από εμάς να διαχειριζόμαστε τις προσωπικές τους πληροφορίες με τη μέγιστη προσοχή έτσι ώστε, να τις διατηρούμε ασφαλείς, προστατευμένες και εμπιστευτικές.

Αν κάνουμε κακή διαχείριση αυτών των σημαντικών «Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα», (ΑΔΠΧ) κινδυνεύουμε να χάσουμε την εμπιστοσύνη τους και την προτίμησή των πελατών μας στην Εταιρία. Γι' αυτό και η νομοθεσία μας επιβάλει να έχουμε τη ρητή συγκατάθεση του υποκείμενου των δεδομένων που συλλέγουμε και επεξεργαζόμαστε.

Στο πλαίσιο των καθημερινών δραστηριοτήτων της, η Εταιρεία συλλέγει, διατηρεί, διανέμει και, τελικά, καταστρέφει πληροφορίες για άτομα.

Ως «Αναγνωρίσιμο Δεδομένο Προσωπικού Χαρακτήρα», εννοούμε κάθε ατομική πληροφορία ή στοιχείο που ανήκει και που προσδιορίζει ένα άτομο, έναν μεριδιούχο ή έναν υπάλληλο της Εταιρίας και που ενδεικτικά και όχι περιοριστικά μπορεί να είναι:

- Αριθμός Διαβατηρίου
- Αριθμός Δελτίου Ταυτότητας
- Αριθμός Φορολογικής Ταυτότητας
- Φορολογική δήλωση, όπου εμφανίζονται εισοδήματα πελατών
- Φυλετική ή Εθνική Προέλευση
- Θρησκευτικές ή Πολιτικές Πεποιθήσεις
- Ποινικό Μητρώο
- Αριθμός Τραπεζικού Λογαριασμού
- Διεύθυνση Κατοικίας
- Διεύθυνση Εργασίας
- Αριθμός Τηλεφώνου

Στις μορφές Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα συμπεριλαμβάνονται επίσης:

- Ηλεκτρονικά Δεδομένα (Ηλεκτρονικό Ταχυδρομείο, Διαδίκτυο)
- Γραπτές πληροφορίες (σε χαρτί)
- Προφορικές Πληροφορίες

Τα ΑΔΠΧ, δεν επιτρέπεται να χρησιμοποιούνται για σκοπούς πέραν εκείνων για τους οποίους αυστηρά συλλέγονται. Τα ΑΔΠΧ που αφορούν τους πελάτες της Εταιρίας ενδέχεται να χρησιμοποιούνται από κοινού από υπαλλήλους και συνεργάτες της

εταιρείας καθώς και από τρίτους, όταν αυτό είναι αναγκαίο για την παροχή τυπικών υπηρεσιών προς τους πελάτες και εφόσον η κοινή χρήση των πληροφοριών δεν συνιστά παραβίαση της τοπικής νομοθεσίας. Όμως, τα ΑΔΠΧ των πελατών, δεν είναι οι μοναδικές πληροφορίες που πρέπει να προστατεύουμε.

Τα Προσωπικά Δεδομένα των Υπαλλήλων, υπόκεινται στους ίδιους ή παρόμοιους κανόνες Προστασίας Δεδομένων/Ιδιωτικού Απορρήτου. Συνεπώς, η Εταιρία πρέπει να συμμορφώνεται με τις απαιτήσεις Προστασίας Δεδομένων/Ιδιωτικού Απορρήτου και να αποδεικνύει ότι έχει θεσπίσει πολιτικές για τη διαφύλαξη της ασφάλειας της εμπιστευτικότητας και του ιδιωτικού απορρήτου όλων των ΑΔΠΧ.

Η Εταιρία απαιτεί όπως όλοι οι υπάλληλοι, οι συνεργάτες, οι συνεργαζόμενοι στα Κέντρα Πώλησης και οι παροχείς υπηρεσιών, να προστατεύουν την εμπιστευτικότητα των πληροφοριών των πελατών, σε οποιοδήποτε σημείο είναι αρχειοθετημένα, αποθηκευμένα τα έγγραφα ή οι πληροφορίες.

Εντός της Εταιρίας, οι πληροφορίες των πελατών πρέπει να παρέχονται αποκλειστικά βάσει της ανάγκης για γνώση και μόνο για την εξυπηρέτηση των δραστηριοτήτων της Εταιρίας. Συνεπώς, αρχεία τα οποία περιέχουν εμπιστευτικές πληροφορίες των πελατών μας δεν πρέπει να διαχειρίζονται και διανέμονται «ελεύθερα» ή να τηρούνται με τρόπο που δεν είναι σύμφωνος με την παρούσα διαδικασία.

Πρέπει πάντα να αναρωτιέστε και να προβληματίζεστε, για ποιόν λόγο και γιατί κάποιος τρίτος (συνάδελφος ή συνεργάτης ή επισκέπτης) επιθυμεί να μάθει κάποια πληροφορία η οποία είναι εμπιστευτική ή δεν χρειάζεται να την γνωρίζει.

Όλοι οι υπάλληλοι πρέπει να φροντίζουν την ασφάλεια των πληροφοριών που διαχειρίζονται και να λαμβάνουν μέτρα για να διαφυλάττουν τα ΑΔΠΧ στο πλαίσιο των εργασιακών καθηκόντων τους.

Σε περίπτωση που απολεσθούν ή κλαπούν ΑΔΠΧ, οι ακόλουθες συνέπειες μπορεί να προκύψουν:

- Κλοπή Ταυτότητας, με ενδεχομένως σημαντικό κόστος και ταλαιπωρία για το άτομο ή την Εταιρία.

- Βλάβη της Φήμης της Εταιρίας. Μπορεί να υπάρξουν επιπτώσεις στις επιχειρησιακές πρακτικές της Εταιρίας και πιθανό να υποβληθεί αγωγή εναντίον της Εταιρίας ή/και κάποιου υπαλλήλου.

- Μπορεί να υπάρξουν αρνητικές συνέπειες όσον αφορά στην εμπιστοσύνη των πελατών στην ικανότητα της Εταιρίας να προστατεύει πληροφορίες, κάτι που τελικά οδηγεί στην απώλεια πελατών για την Εταιρία.

Για αυτό το λόγο, η Εταιρεία θεσπίζει πολιτικές και διαδικασίες για την προστασία όλων των πληροφοριών που συγκεντρώνει σχετικά με οποιοδήποτε άτομο και βασίζεται στη δική σας γνώση όσον αφορά στο πώς να προστατεύετε τις πληροφορίες που έχει στην κατοχή της η Εταιρία και στο τι πρέπει να κάνετε σε περίπτωση πιθανής παραβίασης των δεδομένων.

Σημειώνεται ότι «ΑΠΑΓΟΡΕΥΕΤΑΙ» σε όλους τους υπαλλήλους και στους Άμεσους ή Έμμεσους συνεργάτες της Εταιρίας, να μεταφέρουν εκτός Εταιρίας, με οποιονδήποτε τρόπο (φωτοτυπία, αποστολή σε προσωπική ή άλλη ηλεκτρονική διεύθυνση) οποιοδήποτε έγγραφο ή στοιχείο ή δεδομένο της Εταιρίας και της Μητρικής Εταιρίας, χωρίς αιτιολογημένο επαγγελματικό λόγο. Σε περίπτωση που διαπιστωθεί παράβαση σχετικά με όσα αναφέρονται στην ανωτέρω πρόταση, η Εταιρία θα εξετάσει την περίπτωση και ενδεχομένως να προβεί στις απαραίτητες ενέργειες και να λάβει πειθαρχικά μέτρα τα οποία είναι πιθανό να συμπεριλαμβάνουν την καταγγελία της σύμβασης εργασίας.

Πρακτικές Προστασίας Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα Πελατών της Εταιρίας

- Τα δεδομένα και οι πληροφορίες πρέπει να γνωστοποιούνται με βάση την ανάγκη γνώσης αποκλειστικά και μόνο για τις δραστηριότητες και τις ανάγκες της Εταιρίας.

- Δεν επιτρέπεται να «διανείμετε» τα στοιχεία των πελατών και των Υπαλλήλων.

- Να βεβαιώνεστε ότι έχετε ασφαλίσει ή κλειδώσει τα στοιχεία.

Πρακτικές Προστασίας Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα Υπαλλήλων της Εταιρίας

Η Εταιρία πρέπει να λαμβάνει εγγράφως τη συγκατάθεση των υπαλλήλων όταν γνωστοποιεί ΑΔΠΧ και Πληροφορίες σε οποιοδήποτε άτομο ή οργανισμό ή υπηρεσία, (π.χ. για την επαλήθευση των προηγούμενων αποδοχών και απασχόλησης).

Παραβίαση Ασφαλείας Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα

Ως παραβίαση ασφαλείας ΑΔΠΧ εννοείται η κατοχή και η ενημέρωση μη κρυπτογραφημένων πληροφοριών ενός πελάτη ή υπαλλήλου από μη εξουσιοδοτημένο άτομο.

Απολεσθέντα ή κλεμμένα αρχεία σε έντυπη μορφή ή σε ηλεκτρονική μορφή, που είναι αποθηκευμένα σε σκληρούς δίσκους, φορητούς υπολογιστές ή ταινίες αντιγράφων ασφαλείας, τα οποία περιέχουν αναγνωρίσιμες πληροφορίες θεωρούνται σε κάθε περίπτωση παραβιάσεις ασφαλείας**.**

Συγκεκριμένα παραδείγματα, ενδεικτικά και όχι περιοριστικά είναι τα ακόλουθα:

- Μισθωμένοι υπολογιστές που επιστρέφονται σε προμηθευτές χωρίς να έχει γίνει οριστική διαγραφή όλων των αρχείων από τον σκληρό δίσκο.

- Υπολογιστές που μεταφέρονται ή έντυπα αρχεία που έχουν αποσταλεί για αποθήκευση εκτός των εγκαταστάσεων και χάνονται κατά τη μεταφορά.

- Υπάλληλοι ή συνεργάτες ή εργολήπτες που αποκτούν πρόσβαση σε ηλεκτρονικά ή έντυπα αρχεία χωρίς να υπάρχει επιχειρησιακή ανάγκη ή εξουσιοδότηση για να δουν τα συγκεκριμένα αρχεία.

Η καλόπιστη απόκτηση ΑΔΠΧ ενός πελάτη ή υπαλλήλου από κάποιον ο οποίος ενεργεί εκ μέρους της Εταιρίας δεν συνιστά παραβίαση ασφαλείας, με την προϋπόθεση ότι οι πληροφορίες να μη χρησιμοποιούνται ή διατίθενται σε περαιτέρω γνωστοποίηση χωρίς εξουσιοδότηση και η πρόσβαση σε αυτές τις πληροφορίες να εκτελείται σύμφωνα με τον ισχύοντα νόμο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασίας του Ατόμου) Νόμος του 2001.

Σε περίπτωση που οι πληροφορίες έχουν κρυπτογραφηθεί, παραβίαση ασφαλείας υφίσταται μόνο αν θεωρηθεί ότι η μέθοδος που χρησιμοποιήθηκε για την πρόσβαση σε αυτές συμπεριλάμβανε τη αποκρυπτογράφησή τους.

Ειδοποίηση για Παραβιάσεις Ασφαλείας Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα

Απολεσθέντα ή κλεμμένα αρχεία σε έντυπη μορφή ή σε ηλεκτρονική μορφή, που είναι αποθηκευμένα σε σκληρούς δίσκους, φορητούς υπολογιστές ή ταινίες αντιγραφών ασφαλείας θεωρούνται ως παραβιάσεις ασφαλείας.

Παραδείγματα παραβιάσεων ασφαλείας:

- Απολεσθέντες ή κλαπέντες υπολογιστές σταθεροί ή φορητοί ή SERVERS

- Απολεσθέντα ή κλαπέντα αρχεία σε έντυπη μορφή ή αρχεία υπολογιστών σε σκληρούς δίσκους

- Δεδομένα τα οποία αποστέλλονται εκτός εγκαταστάσεων και χάνονται κατά την μεταφορά

- Απολεσθείσες ή κλαπείσες αναφορές

- FAX που έχουν σταλεί σε λάθος αριθμό και περιέχουν προσωπικά στοιχεία

- Χρήση ΑΔΤ ή άλλου Αριθμού Ταυτότητας χωρίς εξουσιοδότηση

- Αμέλεια υπαλλήλου ή προμηθευτή σε σχέση με τα Προσωπικά Στοιχεία

Διαπίστωση Παραβίασης Ασφαλείας Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα και Πληροφοριών.

Σε περίπτωση που διαπιστώσετε μια παραβίαση ή μια προσπάθεια παραβίασης ή μια πιθανή παραβίαση ασφαλείας ΑΔΠΧ και πληροφοριών θα πρέπει:

Α. Παραβίαση Ασφαλείας - Συνοπτική Περιγραφή:

Ι. Διαδικασία Ειδοποίησης:

1. Ενημερώστε αμέσως τον Υπεύθυνο Συμμόρφωσης

2. Ο Υπεύθυνος Συμμόρφωσης θα ενεργοποιήσει μια Ομάδα Αντιμετώπισης Περιστατικού

3. Η Ομάδα Αντιμετώπισης Περιστατικού θα διερευνήσει το περιστατικό.

ΙΙ. Ομάδα Αντιμετώπισης Περιστατικού:

Θα συγκληθεί Ομάδα Αντιμετώπισης Περιστατικού στην οποία θα συμμετέχουν τουλάχιστον οι ακόλουθοι:

- Ο Υπεύθυνος Κανονιστικής Συμμόρφωσης
- Εκπρόσωπος του Τμήματος που έγινε η αναφορά παραβίασης ή πιθανής παραβίασης
- Εκπρόσωπος του Τμήματος Μηχανογράφησης (αν χρειάζεται)
- Ένα Διευθυντικό Στέλεχος της Εταιρίας (Λειτουργός Προστασίας Δεδομένων)

ΙΙΙ. Ενέργειες Ομάδας Αντιμετώπισης Περιστατικού

Η Ομάδα Αντιμετώπισης Περιστατικού Παραβίασης Ασφαλείας κατά την διάρκεια της εξέτασης του περιστατικού θα προβεί στις παρακάτω Ενέργειες – Εργασίες:

- Θα συλλέξει πληροφορίες
- Αν πρόκειται για παραβίαση υπολογιστών, θα ακολουθήσει τη διαδικασία σύμφωνα με τον Κανονισμό Αντιμετώπισης Περιστατικών Ασφαλείας Υπολογιστικών Συστημάτων της MetLife Alico
- Θα διεκπεραιώσει τις αναγκαίες διαδικασίες ειδοποίησης, οι οποίες καθορίζονται κατά περίπτωση
- Θα υποβάλει αναφορά περιστατικού στην επικεφαλής Θεμάτων Συμμόρφωσης της MetLife Alico

Β. Παραβίαση Ασφαλείας - Αναλυτική Περιγραφή:

Αμέσως μετά την ενημέρωση για μια παραβίαση ή μια προσπάθεια παραβίασης ή μια πιθανή παραβίαση ΑΔΠΧ και πληροφοριών, ο Υπεύθυνος Κανονιστικής Συμμόρφωσης της Εταιρίας θα ενεργοποιήσει μια Ομάδα Αντιμετώπισης Περιστατικού.

Η Ομάδα Αντιμετώπισης Περιστατικού, είναι μια ομάδα ατόμων που θα επιφορτιστεί με τη διερεύνηση ενός περιστατικού για να καθορίσει την ύπαρξη παραβίασης, πιθανής παραβίασης ή η προσπάθεια παραβίασης και η έκταση της.

Η Ομάδα Αντιμετώπισης Περιστατικού αποτελείται τουλάχιστον από τον Υπεύθυνο Κανονιστικής Συμμόρφωσης, έναν Εκπρόσωπο του Τμήματος που έγινε η αναφορά παραβίασης ή πιθανής παραβίασης, από Εκπρόσωπο του Τμήματος Μηχανογράφησης (αν χρειάζεται) και από ένα Διευθυντικό Στέλεχος της Εταιρίας (Λειτουργός Προστασίας Δεδομένων). Στην Ομάδα Αντιμετώπισης Περιστατικού ενδέχεται να συμπεριληφθεί οποιοσδήποτε κριθεί ότι η συμμετοχή του είναι χρήσιμη ή αναγκαία.

Η διερεύνηση από την Ομάδα Αντιμετώπισης Περιστατικού συμπεριλαμβάνει τη συλλογή πληροφοριών για την τεκμηρίωση του εντοπισμού της παραβίασης, της πιθανής παραβίασης ή της προσπάθειας παραβίασης.

Όταν συμβαίνει κάποια παραβίαση εξαιτίας παρείσφρησης σε υπολογιστικά συστήματα, η ομάδα αντιμετώπισης περιστατικού ξεκινά τη διαδικασία αντιμετώπισης περιστατικού παραβίασης ασφαλείας υπολογιστικών συστημάτων, σύμφωνα με τον Κανονισμό Αντιμετώπισης Περιστατικών Ασφαλείας Υπολογιστικών Συστημάτων της MetLife Alico (Computer Security Incident Response Standard).

Παραβίαση Ασφαλείας - Απαιτήσεις ειδοποίησης

Αφού καθοριστεί από την Ομάδα Αντιμετώπισης Περιστατικού ότι οι «προστατευμένες πληροφορίες» έχουν παραβιαστεί και ότι απαιτείται ειδοποίηση, η Ομάδα Αντιμετώπισης Περιστατικού προβαίνει στις απαιτούμενες διαδικασίες ειδοποίησης.

Ο υπάλληλος ή ο πελάτης ή οι πελάτες στους οποίους αφορά το περιστατικό, ειδοποιούνται σε εύλογο χρονικό διάστημα.

Αρμόδιες Αρχές (π.χ. Αστυνομία) ενδέχεται να πρέπει να ειδοποιηθούν επίσης, καθώς και συγκεκριμένες κρατικές αρχές ή φορείς αναφοράς πιστωτικών πληροφοριών.

Η Ομάδα Αντιμετώπισης Περιστατικού θα καθορίσει τις ειδοποιήσεις που απαιτούνται κατά περίπτωση και υπεύθυνος για τη διεκπεραίωση όλων των αναγκαίων ειδοποιήσεων είναι ο Υπεύθυνος Κανονιστικής Συμμόρφωσης.

Όλες οι ειδοποιήσεις θα διεκπεραιώνονται με τον πιο αποτελεσματικό τρόπο και χωρίς αδικαιολόγητες καθυστερήσεις.

Σε περίπτωση εμπλοκής Αρμοδίων Αρχών στη διερεύνηση της παραβίασης, η απαιτούμενη ειδοποίηση πιθανό να καθυστερήσει έως ότου η Αρμόδια Αρχή καθορίσει ότι η ειδοποίηση δεν θα παρεμποδίσει ή δεν θα εκθέσει σε κίνδυνο αποτυχίας την έρευνα.

Στην ειδοποίηση θα περιγράφονται η φύση της παραβίασης, οι πληροφορίες που είναι πιθανό να έχουν παραβιαστεί και θα παρέχονται πληροφορίες σχετικά με τα μέτρα εξάλειψης ή περιορισμού του κινδύνου κλοπής ταυτότητας.

Το άτομο ή τα άτομα των οποίων τα στοιχεία έχουν παραβιαστεί θα ειδοποιούνται απευθείας όποτε αυτό κριθεί αναγκαίο με την προϋπόθεση ότι η ειδοποίηση δεν παρεμποδίζει ή δεν θέτει σε κίνδυνο αποτυχίας την έρευνα.

Η ειδοποίηση θα πραγματοποιείται πάντα εγγράφως.

Παραβίαση Ασφαλείας - Αναφορά και στοιχεία αρχειοθέτησης περιστατικού

Ο Υπεύθυνος Κανονιστικής Συμμόρφωσης της Εταιρίας εντός πέντε (5) εργάσιμων ημερών από την στιγμή που θα ειδοποιηθεί αρχικά ή θα λάβει γνώση με οποιονδήποτε τρόπο για την παραβίαση ασφαλείας πρέπει να υποβάλει αναφορά περιστατικού στην Επικεφαλής Θεμάτων Συμμόρφωσης της MetLife Alico.

Η Αρχική Αναφορά Περιστατικού πρέπει να συμπεριλαμβάνει όσο το δυνατό περισσότερες πληροφορίες.

Μετά την ολοκλήρωση της διερεύνησης ο Υπεύθυνος Κανονιστικής Συμμόρφωσης ή τα μέλη της Ομάδας Αντιμετώπισης Περιστατικού θα υποβάλλουν στην Επικεφαλής Θεμάτων Συμμόρφωσης της MetLife Alico μια «Τελική Αναφορά Περιστατικού».

Η Τελική Αναφορά Περιστατικού πρέπει να περιγράφει αναλυτικά τη φύση και την αιτία του περιστατικού, τον τρόπο ειδοποίησης που χρησιμοποιήθηκε και σε ποιον στάλθηκε, η διαδικασία αντιμετώπισης και ποια μέτρα ελήφθησαν προκειμένου για αποτραπεί η εμφάνιση παρόμοιου περιστατικού στο μέλλον.

Οι Αναφορές και οι πληροφορίες που έχουν συγκεντρωθεί για όλες τις παραβιάσεις ή τις πιθανές παραβιάσεις πρέπει να αποθηκεύονται με ασφάλεια. Αυτά τα στοιχεία πρέπει να διατηρούνται για περίοδο τουλάχιστον πέντε ετών, εκτός εάν εκκρεμεί δικαστική υπόθεση.

Συμβουλές Πρόληψης Παραβίασης Ασφαλείας

Είναι πάρα πολύ σημαντικό να τηρούνται αυστηρά πρότυπα ασφαλείας στον χώρο εργασίας σας.

Κατά την διαχείριση Αρχείων και εγγράφων της εταιρίας θα πρέπει να δώσετε ιδιαίτερη προσοχή στα «Αναγνωρίσιμα Δεδομένα Προσωπικού Χαρακτήρα» των πελατών και των υπαλλήλων της Εταιρίας.

Η Εταιρία απαιτεί τη λήψη των ακόλουθων προφυλάξεων για την αποφυγή πιθανών παραβιάσεων ασφαλείας:

- Τα έγγραφα και οι αναφορές που είναι τυπωμένες πρέπει να προστατεύονται δεόντως. Για παράδειγμα, τα γραφεία και τα ερμάρια αρχειοθέτησης πρέπει να ασφαλίζονται και να κλειδώνονται.

- Είναι ευθύνη όλων μας να εξασφαλίζουμε την ασφάλεια των Αναγνωρίσιμων Προσωπικών Δεδομένων και Πληροφοριών των πελατών, των υπαλλήλων, των συνεργατών και των προμηθευτών. Οι υπάλληλοι που διαχειρίζονται

προσωπικά αναγνωρίσιμες πληροφορίες πρέπει να είναι κατάλληλα εκπαιδευμένοι στη διαχείριση αυτών των πληροφοριών.

- Κρυπτογραφείτε όλες τις ηλεκτρονικά μεταφερόμενες πληροφορίες που αφορούν προσωπικά δεδομένα, τους φορητούς υπολογιστές και άλλες ηλεκτρονικές συσκευές. Υπάρχουν διαθέσιμες διάφορες λύσεις κρυπτογράφησης και πρέπει να χρησιμοποιείται κάποια από αυτές. (Επικοινωνήστε με το Τμήμα Μηχανογράφησης για βοήθεια, αν απαιτείται).

- Οι σκληροί δίσκοι φορητών υπολογιστών και άλλων φορητών συσκευών που περιέχουν Αναγνωρίσιμα Δεδομένα Προσωπικού Χαρακτήρα πρέπει να είναι κρυπτογραφημένοι σύμφωνα με τα εταιρικά πρότυπα.

- Σε φορητές συσκευές ή σε συσκευές που βρίσκονται εκτός Εταιρίας, συμπεριλαμβανομένων των επιτραπέζιων υπολογιστών, των φορητών υπολογιστών ή συσκευών, πρέπει να αποθηκεύονται μόνο Αναγνωρίσιμα Δεδομένα Προσωπικού Χαρακτήρα που είναι απολύτως αναγκαία για τους άμεσους σκοπούς διεκπεραίωσης των επαγγελματικών δραστηριοτήτων.
  Όλες οι άλλες πληροφορίες οι οποίες είναι αναγκαίες πρέπει να αποθηκεύονται στα συστήματα και δίκτυα της Εταιρίας, όπου τηρούνται τα κατάλληλα επίπεδα ασφαλείας.

- Ποτέ μην αφήνετε φορητούς υπολογιστές χωρίς επίβλεψη:

  Οι φορητοί υπολογιστές που περιέχουν Αναγνωρίσιμα Δεδομένα Προσωπικού Χαρακτήρα δεν πρέπει να αφήνονται χωρίς επίβλεψη και χωρίς τα αναγκαία μέτρα ασφαλείας.

  Κατά τις μετακινήσεις, έχετε τον φορητό υπολογιστή πάντα υπό έλεγχο.

  Όταν βρίσκεστε σε ξενοδοχείο, πρέπει να λαμβάνετε τα κατάλληλα μέτρα προστασίας του φορητού υπολογιστή.

  Όταν βρίσκεστε σε σταθμό εργασίας, οι φορητοί υπολογιστές πρέπει να ασφαλίζονται χρησιμοποιώντας σταθμό σύνδεσης ή με κατάλληλα καλώδια ασφάλισης.

  Κατά τα αεροπορικά ταξίδια, μην παραδίδετε τους φορητούς υπολογιστές με τις αποσκευές.

  Στο εμπόριο διατίθενται τυποποιημένα συστήματα κλειδώματος για υπολογιστές.

- Είναι υποχρέωση όλων μας να είμαστε και εμείς Υπεύθυνοι Θεμάτων Συμμόρφωσης

- Προσέχετε για δραστηριότητες που αφορούν σε διάφορα έργα (π.χ. γενικές εργασίες από εργολάβους, ηλεκτρικές εργασίες, ελαιοχρωματισμοί) τα οποία μπορεί να επηρεάσουν το χώρο εργασίας και την ασφάλεια των εγγράφων ή των υπολογιστών. Σε περίπτωση που έχετε οποιαδήποτε παρατήρηση, αμφιβολία, ερώτηση ή ανησυχία σχετικά με την ασφάλεια των δεδομένων θα πρέπει να επικοινωνήσετε με τον υπεύθυνο του Τμήματός σας ή με τον Υπεύθυνο Συμμόρφωσης.

- Ιστότοποι όπου συλλέγονται προσωπικά αναγνωρίσιμες πληροφορίες καταναλωτών ή υπαλλήλων πρέπει να διαθέτουν τα κατάλληλα μέτρα ασφαλείας στις ιστοσελίδες συλλογής των προσωπικά αναγνωρίσιμων πληροφοριών, σύμφωνα με τα πρότυπα ασφαλείας των πληροφοριών της MetLife Alico.

- Στους ιστότοπους πρέπει να δημοσιεύεται μια πολιτική προστασίας του ιδιωτικού απορρήτου, η οποία θα ενημερώνει τους πελάτες ποιες πληροφορίες συλλέγονται, πώς χρησιμοποιούνται και αν αυτές κοινοποιούνται σε άλλους και σε ποιους. Αν αυτές οι πληροφορίες μεταβιβάζονται πέραν των ορίων δικαιοδοσίας, αυτό πρέπει να αναφέρεται επίσης.

- Μην εγκαθιστάτε μη εγκεκριμένο λογισμικό, ιδιαίτερα, από μηχανές αναζήτησης που μπορούν να εκθέσουν σε κίνδυνο την ασφάλεια των ηλεκτρονικών αρχείων.

- Όλες οι πολιτικές που έχουν σχέση με τη διαχείριση των προσωπικά αναγνωρίσιμων πληροφοριών πελατών και υπαλλήλων πρέπει να εξετάζονται από τον Υπεύθυνο Κανονιστικής Συμμόρφωσης ή τον Υπεύθυνο Ασφαλείας ή τον Νομικό Σύμβουλο της Εταιρίας, για να εξασφαλίζεται ότι αυτές είναι αποτελεσματικές ως προς την προστασία της ασφαλείας των πληροφοριών.

Αν έχετε οποιαδήποτε παρατήρηση, αμφιβολία, ερώτηση ή ανησυχία σχετικά με την ασφάλεια των Αναγνωρίσιμων Δεδομένων Προσωπικού Χαρακτήρα απευθυνθείτε στον Υπεύθυνο Συμμόρφωσης