

Για όλους τους εργαζομένους της VICTORY, ο σεβασμός της ιδιωτικής ζωής και η προστασία των προσωπικών δεδομένων αποτελούν βασικές προτεραιότητες. Για τον λόγο αυτό, η Εταιρεία λαμβάνει όλα τα αναγκαία μέτρα για την αποτροπή περιστατικών κλοπής, απώλειας και διαρροής προσωπικών δεδομένων των πελατών/ασφαλισμένων, εργαζομένων και προμηθευτών της.

## Η Προσέγγιση

Η VICTORY σχεδίασε και εφαρμόζει -από το 2010- ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών. Σκοπός αυτής της πρωτοβουλίας είναι η διασφάλιση και διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των φυσικών και πληροφοριακών δεδομένων της Εταιρείας. Η προστασία τους απαιτεί μία δομημένη, ολοκληρωμένη και αποτελεσματική προσέγγιση. Την προσέγγιση αυτή παρέχει το διεθνές πρότυπο ISO/IEC 27001:2013, στη βάση του οποίου αναπτύχθηκε η πολιτική Ασφάλειας. Αυτή η πολιτική, μέσα από μία σειρά τεχνικών και οργανωτικών μέσων, περιγράφει τις απαιτούμενες ασφαλιστικές δικλίδες που πρέπει να ακολουθούνται από την VICTORY στο σύνολο των λειτουργιών της.

Επιπλέον, η Εταιρεία ανέπτυξε και έθεσε σε εφαρμογή τα κατάλληλα μέτρα, προκειμένου να διασφαλίσει ότι ένα από τα σημαντικότερα αγαθά της Εταιρείας, οι πληροφορίες, είναι επαρκώς προστατευμένες, είτε είναι αποθηκευμένες στα συστήματά της, είτε βρίσκονται υπό επεξεργασία σε αυτά. Η VICTORY διασφαλίζει ένα πολύ υψηλό επίπεδο προστασίας των συστημάτων της και κατ' επέκταση και των δεδομένων που διαχειρίζεται, μέσα από μία σειρά τεχνικών -και μη- μέτρων (ενδεικτικά αναφέρονται ορισμένα από αυτά: Vulnerability Assessment, Penetration Testing, Business Impact Analysis, Risk Assessment, Data Classification Policy, Access Control Policy, RBAC, Data Leakage Prevention κ.ά.).

Εναρμονιζόμενη με τις απαιτήσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η Εταιρεία έχει λάβει από την Αρχή τις απαραίτητες άδειες για τη συλλογή, διατήρηση και επεξεργασία αρχείων με προσωπικά και ευαίσθητα δεδομένα πελατών, προμηθευτών και εργαζομένων. Τα δεδομένα των πελατών της, στα οποία έχουν πρόσβαση συγκεκριμένοι εργαζόμενοι λόγω θέσης ή/και δραστηριότητας, είναι απόρρητα και εμπιστευτικά και δεν γνωστοποιούνται σε τρίτους.

Η VICTORY, από το 2016, προχώρησε στη δημιουργία και στελέχωση ομάδας διαχείρισης έργου, η οποία ανέλυσε σε βάθος τα άρθρα και τις έννοιες του κανονισμού. Η ανάλυση θεωρείται ως ένα από τα πρώτα βασικά βήματα για τη συμμόρφωση. Η νέα τάξη πραγμάτων που φέρνει ο ευρωπαϊκός κανονισμός General Data Protection Regulation (GDPR), πρωτίστως κατανοήθηκε και εμπεδώθηκε από τη Διοίκηση, που υποστήριξε την εκπαίδευση μέσω προγράμματος ενημέρωσης (awareness program) επαναληπτικού χαρακτήρα, για την εξοικείωση όλου του ανθρωπίνου δυναμικού του Οργανισμού και την ομαλή προσαρμογή του στο κανονιστικό πλαίσιο. Η διεξαγωγή του DPIA (Data Privacy Impact Assessment) από την VICTORY ανέδειξε από τις αρχές του 2017 τις ελλείψεις και τις ευπάθειες που υπήρχαν στην Εταιρεία και βάσει αυτών, σχεδιάστηκε το πλάνο υλοποίησης.

Ακόμη, η VICTORY δημιούργησε οργανική θέση Data Protection Officer (DPO) και προχώρησε σε ανάθεση καθηκόντων καθώς και στη δημιουργία διατμηματικής ομάδας (DPO Hub), που απαρτίζεται από στελέχη ποικίλων δεξιοτήτων, στην οποία προεδρεύει ο DPO. Σκοπός της σύστασης της ομάδας αποτελεί η κάλυψη όλου του εύρους των απαιτήσεων του Κανονισμού καθώς και η συνεχής συνεργασία για την αντιμετώπιση σχετικών θεμάτων που ενδέχεται να ανακύπτουν. Επίσης, πραγματοποιήθηκαν βασικές ενέργειες προσανατολισμένες στη συμμόρφωση, όπως:

- η εκπόνηση διαδικασιών και δράσεων,
- η σύνταξη πολιτικής για την Προστασία Προσωπικών Δεδομένων,
- η ικανοποίηση των δικαιωμάτων (πρόσβασης, διόρθωσης, διαγραφής, περιορισμού της επεξεργασίας, φορητότητας και εναντίωσης) του υποκειμένου των δεδομένων (πελάτη),
- η δημιουργία συγκατάθεσης (ηλεκτρονική και έγγραφη) η οποία πρέπει να είναι σαφώς διακριτή, κατανοητή, εύκολα προσβάσιμη, σαφής και απλή.

Παράλληλα, διαμορφώθηκε πλαίσιο, ώστε να πληρούνται οι “by default και by design” προδιαγραφές στα συστήματα και τις διαδικασίες, η διαβάθμιση και κατηγοριοποίηση των δεδομένων σύμφωνα με τον νέο κανονισμό, η χαρτογράφηση, καταγραφή και ο έλεγχος της ροής της επεξεργασίας των δεδομένων, η διεξαγωγή Clean Desk Assessment και η πολιτική Διατήρησης Δεδομένων (Archiving and Retention Policy).