

Άλλα σημαντικά θέματα Διακυβέρνησης

Κυβερνοασφάλεια

Πιθανές παραβιάσεις στην ασφάλεια των δικτύων και των πληροφοριακών και λειτουργικών συστημάτων, απειλούν την ακεραιότητα των δεδομένων της εταιρείας, των ευαίσθητων πληροφοριών, καθώς και την εύρυθμη λειτουργία των επιχειρηματικών δραστηριοτήτων. Μια τέτοια πιθανή παραβίαση θα μπορούσε να επηρεάσει αρνητικά τη φήμη της εταιρείας και την ανταγωνιστική της θέση. Επίσης μια πιθανή επιδίκαση αποζημιώσεων, επιβολή προστίμων, ή απώλεια δραστηριοτήτων (περιλαμβανομένου και του κόστους αποκατάστασης), θα μπορούσαν να έχουν σημαντική αρνητική επίδραση στην οικονομική της κατάσταση και τα λειτουργικά αποτελέσματα. Επιπλέον, η διαχείριση των παραβιάσεων κυβερνοασφάλειας, ενδέχεται να απαιτήσει σημαντική επένδυση χρόνου από τη διοίκηση.

Η MYTILINEOS έχει αναπτύξει **Πλαίσιο Ασφάλειας Πληροφοριών** και έχει δεσμευτεί στην εφαρμογή ενός **ολιστικού Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών**, μέσω του οποίου επιτυγχάνεται η αποτελεσματική και αποδοτική προστασία των πληροφοριακών συστημάτων και των δεδομένων της Εταιρείας.

Το Πλαίσιο Ασφάλειας Πληροφοριών θέτει ένα συνεχή κύκλο βελτίωσης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, προδιγράφοντας δραστηριότητες για την αξιολόγηση των κινδύνων, την ανάπτυξη και την εφαρμογή πολιτικών ασφαλείας πληροφοριών, προτύπων, διαδικασιών και οδηγιών για τον μετριασμό των κινδύνων και για την παρακολούθηση της αποτελεσματικότητας και της αποδοτικότητάς τους.

Η MYTILINEOS ανά τακτά διαστήματα συνεργάζεται με **ανεξάρτητους οργανισμούς** και συμβούλους, οι οποίοι αξιολογούν την επάρκεια και την αποτελεσματικότητα του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και επαληθεύουν ότι ένας πληροφοριακός πόρος, ή ένα σύστημα διαχείρισης, πληροί τις απαραίτητες απαιτήσεις που προσδιορίζονται από τις αντίστοιχες πολιτικές και τις βέλτιστες πρακτικές για την προστασία των πληροφοριακών συστημάτων και των δεδομένων τους.

Επίσης, έχει αναπτυχθεί ένα τακτικό και δομημένο πρόγραμμα ευαισθητοποίησης και εκπαίδευσης σε θέματα ασφαλείας πληροφοριών, το οποίο εφαρμόζεται σε όλη την MYTILINEOS σε συνεχή βάση. Ο στόχος του προγράμματος είναι να διασφαλίσει ότι όλοι οι εργαζόμενοι, οι εργολάβοι και τα σχετικά τρίτα μέρη με πρόσβαση σε πληροφορίες και πληροφοριακά συστήματα, κατανοούν την ανάγκη για την ασφάλεια πληροφοριών, αποδέχονται τις ευθύνες που τους έχουν ανατεθεί βάσει του Πλαισίου Ασφάλειας Πληροφοριών και εκτελούν τα καθήκοντά τους επιδεικνύοντας ένα υψηλό επίπεδο επαγγελματικής δεοντολογίας. Το εν λόγω πρόγραμμα αξιολογείται και αναθεωρείται εφόσον θεωρηθεί σκόπιμο, σε τακτά χρονικά διαστήματα μέσω εξετάσεων, καθώς και ασκήσεων που προσομοιάζουν πραγματικές επιθέσεις κυβερνοασφάλειας.

Τέλος, για να διασφαλιστεί η επιχειρησιακή συνέχεια και να ελαχιστοποιηθεί ο αντίκτυπος μετά από μια παραβίαση κυβερνοασφάλειας ή φυσική καταστροφή, έχει σχεδιαστεί και εφαρμοστεί **ένα σχέδιο επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών**, το οποίο δοκιμάζεται και ενημερώνεται σε τακτική βάση. Σε τακτά χρονικά διαστήματα, ή εφόσον προκύπτουν θέματα στο ευρύτερο περιβάλλον κυβερνοασφάλειας στο οποίο δραστηριοποιείται η Εταιρεία, πραγματοποιούνται σχετικές παρουσιάσεις σε επίπεδο Ανώτερης Διοίκησης, ή και Επιτροπής Ελέγχου. Η Ανώτερη Διοίκηση είναι υπεύθυνη για τη λήψη κατάλληλων μέτρων που θα εγγυώνται την επιχειρησιακή συνέχεια σύμφωνα με τις επιχειρησιακές ανάγκες.

Απόρρητο Πελατών

Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα και είναι υψίστης σημασίας για την MYTILINEOS. Ως εκ τούτου η συλλογή και επεξεργασία προσωπικών δεδομένων γίνεται μόνον σύμφωνα με το νόμο και όπου αυτό απαιτείται σχετικά με λειτουργία των εργασιακών σχέσεων και την επιχειρηματική δραστηριότητα της Εταιρείας. Η Εταιρεία επιτρέπει την πρόσβαση μόνον εξουσιοδοτημένων προσώπων σε αυτά και λαμβάνει αυξημένα μέτρα ασφάλειας των δεδομένων.

Παρόλο που η MYTILINEOS κατά βάση δεν επεξεργάζεται δεδομένα ειδικών κατηγοριών (ευαίσθητα), η επιχειρηματική κατεύθυνση της Protergia στην λιανική πώληση ηλεκτρικής ενέργειας και φυσικού αερίου καθώς και το μέγεθος της MYTILINEOS σε εργαζόμενους και επιχειρηματικούς εταίρους, προϋποθέτουν επεξεργασίες προσωπικών δεδομένων μεγάλης κλίμακας. Η MYTILINEOS παραμένει υπεύθυνος της επεξεργασίας των δεδομένων με συγκεκριμένες υποχρεώσεις και ευθύνες και σε περιπτώσεις ανάθεσης της επεξεργασίας αυτής σε τρίτους. Επιπλέον, οι συναλλαγές με επιχειρηματικούς εταίρους εκτός Ευρωπαϊκής Ένωσης και κυρίως σε χώρες με λιγότερο αυστηρή νομοθεσία για την προστασία των προσωπικών δεδομένων, δημιουργούν την ανάγκη για τη διαβίβαση προσωπικών δεδομένων των οποίων η προστασία θα πρέπει να διασφαλίζεται.

Η Εταιρεία δύναται να αντιμετωπίσει διάφορους κινδύνους που σχετίζονται με την προστασία των προσωπικών δεδομένων οι οποίοι μπορεί να είναι οικονομικής φύσεως από ενδεχόμενες κυρώσεις Ευρωπαϊκών αρχών προστασίας προσωπικών δεδομένων ή από αξιώσεις υποκειμένων προσωπικών δεδομένων τα οποία έχουν υποστεί βλάβη, αλλά και κινδύνους που σχετίζονται με αρνητική δημοσιότητα και βλάβη στη φήμη σε περίπτωση μη σωστής διαφύλαξης και επεξεργασίας των προσωπικών δεδομένων των πελατών της.

Για το λόγο αυτό η MYTILINEOS έχει προβεί σε μία σειρά από δράσεις για τη διασφάλιση, στο μέτρο του δυνατού, της προστασίας των προσωπικών δεδομένων που διαχειρίζεται. Πιο συγκεκριμένα:

- έχει προβεί από το 2018 στην πρόσληψη **Υπεύθυνου Προστασίας Δεδομένων** (Data Protection Officer) και γνωστοποίηση αυτού στην αρχή,
- έχει υλοποιήσει **μελέτη απόκλισης** από τον Γενικό Κανονισμό Προστασίας Δεδομένων και έχει προβεί από το 2018 στις κατάλληλες διορθωτικές ενέργειες,
- έχει καταρτίσει **πολιτική προστασίας δεδομένων** για όλους τους εργαζόμενους και όλες τις θυγατρικές καθώς και για τους επιχειρηματικούς εταίρους και την έχει επικοινωνήσει σε όλα τα ενδιαφερόμενα μέρη,
- έχει ολοκληρώσει **μελέτες επιπτώσεων** (Data Privacy Impact Assessments) για τις διαδικασίες επεξεργασίας που απαιτούνται,
- έχει δημιουργήσει και λειτουργεί μηχανισμό **καταγραφής τυχόν παραβιάσεων** προσωπικών δεδομένων και γνωστοποίηση αυτών στην αρμόδια Αρχή Προστασίας Δεδομένων καθώς και στα πληττώμενα υποκείμενα δεδομένων, εάν αυτό απαιτείται, ενώ,
- σε επίπεδο **εκπαίδευσης**, έχει εκπαιδέσει δια ζώσης, αλλά και μέσω περιβάλλοντος υπολογιστή έως το τέλος του 2021 παραπάνω από 850 εργαζόμενους οι οποίοι είτε επεξεργάζονται προσωπικά δεδομένα είτε επιβλέπουν την επεξεργασία τους.

Επιπρόσθετα, οι κίνδυνοι προστασίας προσωπικών δεδομένων περιλαμβάνονται στο Σύστημα Διαχείρισης Κινδύνων της Εταιρείας και

παρακολουθούνται συνεχώς. Το 2021, ολοκληρώθηκαν οι έλεγχοι για την προστασία προσωπικών δεδομένων στους Τομείς Μεταλλουργίας και Ηλεκτρικής Ενέργειας και Φυσικού Αερίου μέσω του εσωτερικού ελέγχου χωρίς σημαντικά ευρήματα. Εντός του 2021, η MYTILINEOS, έχει προβεί σε 10 ενδελεχείς ελέγχους συμμόρφωσης εκτελούντων την επεξεργασία με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (ΓΚΠΔ). **ASI**

Η τήρηση της εφαρμοστέας νομοθεσίας, καθώς και εφαρμογή δικλίδων ελέγχου συμμόρφωσης με τους κανόνες που αφορούσαν στη δραστηριότητα της MYTILINEOS, κατά το 2021, **είχαν σαν αποτέλεσμα την απουσία ουσιαστικών περιστατικών παραβίασης προσωπικών δεδομένων**. Εντός του 2021, στον Τομέα Ηλεκτρικής Ενέργειας και Φυσικού Αερίου υπήρξαν οκτώ (8) περιστατικά αποστολής συμβάσεων/ λογαριασμών σε λανθασμένους παραλήπτες για τα αίτια των οποίων λήφθηκαν πρόσθετα τεχνικά και οργανωτικά μέτρα ώστε αυτά να εκμηδενιστούν. Τα περιστατικά, τα οποία δεν κρίνονται ως ουσιαστικά, αναφέρθηκαν εμπρόθεσμα στην αρμόδια Αρχή και τα υποκείμενα των δεδομένων ενημερώθηκαν άμεσα όπου αυτό απαιτούνταν. Επιπλέον, υπήρξαν 3 επιβεβαιωμένες περιπτώσεις προωθητικών κλήσεων από εξωτερικούς συνεργάτες της MYTILINEOS σε τηλεφωνικούς αριθμούς συνδρομητών οι οποίοι ανήκαν στο άρθρο 11 του νόμου 3471/2006 περί «μη ζητηθείσας επικοινωνίας». Τέλος, διαβιβάστηκαν στην Εταιρεία από την αρμόδια Αρχή τρία υποβληθέντα σε αυτήν παράπονα. **[GRI 418-1]**

Διαχείριση Επιχειρηματικών Κινδύνων

[GRI 102-11] [GRI 102-15]

Οι δραστηριότητες της MYTILINEOS επηρεάζονται από πολλούς κινδύνους, η επέλευση των οποίων ενδέχεται να επηρεάσει συνολικά τις δραστηριότητές της, την επιχειρηματική της δράση, την οικονομική της απόδοση καθώς και την επίτευξη των στρατηγικών στόχων της.

Η MYTILINEOS, εντός του 2021, βάσει της φύσης και έκτασης των κινδύνων που αντιμετωπίζει σε ένα διαρκώς μεταβαλλόμενο οικονομικό και επιχειρηματικό περιβάλλον, **προχώρησε σε επαναξιολόγηση των κύριων επιχειρηματικών κινδύνων**, τους οποίους ταξινόμησε στις κατωτέρω βασικές κατηγορίες:

- Χρηματοοικονομικοί
- Αγοράς
- Νομικοί, Ρυθμιστικοί & Κανονιστικής Συμμόρφωσης
- Λειτουργικοί
- Στρατηγικοί

Η MYTILINEOS εφαρμόζει ένα **Σύστημα Διαχείρισης Επιχειρηματικών Κινδύνων** για την αναγνώριση, ανάλυση, αξιολόγηση, παρακολούθηση και αναφορά των κινδύνων, με σκοπό να περιορίσει τις πιθανότητες και επιπτώσεις των κινδύνων και να μεγιστοποιήσει το όφελος από τις ευκαιρίες που παρουσιάζονται. Στο πλαίσιο αυτό, έχει υιοθετηθεί μια μεθοδολογία αξιολόγησης κινδύνων (**Enterprise Risk Assessment**), η οποία βασίζεται σε βέλτιστες διεθνείς πρακτικές και είναι προσαρμοσμένη στις ανάγκες της MYTILINEOS, προωθώντας ενιαία κουλτούρα που ενσωματώνει τη διαχείριση κινδύνων στις διαδικασίες και στις δραστηριότητές της.

Η μεθοδολογία (top-down & bottom-up) **ακολουθείται από το σύνολο των Τομέων Επιχειρηματικής Δραστηριότητας** και Κεντρικών Υπηρεσιών και λειτουργιών της MYTILINEOS και περιλαμβάνει:

- Αναγνώριση των βασικών παραγόντων κινδύνου και κατηγοριοποίησή τους
- Εκτίμηση της πιθανότητας επέλευσης των κινδύνων και των επιπτώσεών τους
- Εκτίμηση της επάρκειας των μηχανισμών μετρίασης των κινδύνων
- Εκτίμηση του υπολειπόμενου κινδύνου
- Παρακολούθηση των κινδύνων

Τα αρμόδια στελέχη των Γενικών Διευθύνσεων εμπλέκονται στη συστηματική αναγνώριση και εκτίμηση των κινδύνων που επηρεάζουν τις επιχειρηματικές δραστηριότητες, καθώς και στην εκτίμηση της επάρκειας των μηχανισμών μετρίασης των κινδύνων και επιπλέον εποπτεύουν τη διαμόρφωση και την έγκαιρη υλοποίηση των σχεδίων αντιμετώπισης των κινδύνων. Για το σύνολο των κινδύνων έχουν οριστεί Risk Owners, οι οποίοι είναι υπεύθυνοι για την εφαρμογή της μεθοδολογίας αξιολόγησης των κινδύνων και τον σχεδιασμό αντιμετώπισής τους. Επιπλέον, σε κάθε Γενική Διεύθυνση έχει θεσπιστεί ο ρόλος του Risk Partner, ο οποίος είναι υπεύθυνος για τη διαμόρφωση και ανανέωση του Μητρώου Κινδύνων (Risk Register), καθώς και για τον έλεγχο της προόδου υλοποίησης του εκάστοτε σχεδίου αντιμετώπισης ενός κινδύνου.

Τα αποτελέσματα της αξιολόγησης κινδύνων, κοινοποιούνται, από τη Διεύθυνση Διαχείρισης Επιχειρηματικών Κινδύνων, στην Εκτελεστική Επιτροπή και την Επιτροπή Ελέγχου του Διοικητικού Συμβουλίου της MYTILINEOS.

Στη MYTILINEOS τέλος, διεξάγονται **εσωτερικοί έλεγχοι** προς διασφάλιση της κατάλληλης και αποτελεσματικής εφαρμογής των διαδικασιών διαχείρισης κινδύνων.

