Εγκύκλιος: 172 / 2021

ERGO Ασφαλιστική
Μονοπρόσωπη Α.Ε.
Λεωφ. Συγγρού 173
171 21 Ν. Σμύρνη
Τηλ. +30 210 3705300
Fax +30 210 3705550
Α.Φ.Μ. 094256484
Δ.Ο.Υ. Φ.Α.Ε. Πειραιά
www.ergohellas.gr

Προς
το Δίκτυο Ανεξάρτητων Συνεργατών

Νέα Σμύρνη, 19 Μαρτίου 2021

Θέμα: Παραβίαση προσωπικών δεδομένων και οδηγίες για την ασφάλεια πληροφοριών

Αγαπητοί Συνεργάτες,

Η Εταιρεία μας στο πλαίσιο της διαδικασίας ενάσκησης των ασφαλιστικών της δραστηριοτήτων είναι υποχρεωμένη να υιοθετεί κατάλληλες διαδικασίες για την προστασία των δεδομένων προσωπικού χαρακτήρα (δεδομένα πελατών, συνεργατών, προμηθευτών, προσωπικού και τρίτων), που να εγγυώνται την ενδεδειγμένη ασφάλειά τους και μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά.

Για την καλύτερη κατανόηση των υποχρεώσεων που προκύπτουν, για όλα τα εμπλεκόμενα μέρη, σας παραθέτουμε στη συνέχεια χρήσιμες πληροφορίες σχετικά με την παραβίαση προσωπικών δεδομένων, καθώς και την ασφαλή διαχείριση εταιρικών πληροφοριών.

Παραβίαση προσωπικών δεδομένων είναι η παραβίαση της ασφάλειας που οδηγεί σε τυχαία και παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Είδη περιστατικών παραβίασης προσωπικών δεδομένων μπορεί να συνιστούν:
- «Παραβίαση απορρήτου», όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αποκάλυψη δεδομένων προσωπικού χαρακτήρα ή μη εξουσιοδοτημένη ή τυχαία πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.
- «Παραβίαση ακεραιότητας», όταν υπάρχει μη εξουσιοδοτημένη ή τυχαία αλλοίωση δεδομένων προσωπικού χαρακτήρα.
- «Παραβίαση διαθεσιμότητας», όταν υπάρχει τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης σε δεδομένα προσωπικού χαρακτήρα ή τυχαία ή μη εξουσιοδοτημένη καταστροφή δεδομένων προσωπικού χαρακτήρα.

Μία παραβίαση μπορεί να αφορά την εμπιστευτικότητα (απόρρητο), την ακεραιότητα και τη διαθεσιμότητα δεδομένων προσωπικού χαρακτήρα ταυτόχρονα, καθώς και οποιονδήποτε συνδυασμό αυτών.

Ενδεικτικά παραδείγματα παραβιάσεων δεδομένων προσωπικού χαρακτήρα:
- ✓ Ένας πελάτης λαμβάνει κατά λάθος έγγραφα που προορίζονται για άλλον πελάτη, π.χ. λόγω ανθρώπινου λάθους στην εμφακέλωση.
- ✓ Αποστολή email που περιλαμβάνει προσωπικά δεδομένα σε λανθασμένο αποδέκτη, π.χ. από ανθρώπινο λάθος λόγω πανομοιότυπων ονομάτων ή ηλεκτρονικών διευθύνσεων.

- ✓ Απώλεια κινητού, χωρίς τη χρήση κωδικού ασφαλείας ή κρυπτογραφημένου μέσου δεδομένων, στο οποίο αποθηκεύονται προσωπικά δεδομένα.
- ✓ Διάρρηξη γραφείων και κλοπή εγγράφων που περιέχουν προσωπικά δεδομένα ή ακόμη και χωρίς κλοπή των εγγράφων, εάν αυτά βρίσκονταν εκτεθειμένα ή μη ασφαλώς αποθηκευμένα.
- ✓ Πληροφορίες σχετικά με τον πελάτη δίνονται σε μη εξουσιοδοτημένο τρίτο μέρος (π.χ. πληροφορίες για συμβόλαιο στον υιό του λήπτη της ασφάλισης/ασφαλισμένου).
- ✓ (Προσωρινή) διακοπή ρεύματος ή επίθεση στα συστήματα της Εταιρείας, που έχει ως αποτέλεσμα τη διακοπή παροχής υπηρεσιών, καθιστώντας τα προσωπικά δεδομένα μη διαθέσιμα.
- ✓ Email για σκοπούς μάρκετινγκ αποστέλλεται μαζικά στους παραλήπτες που αναφέρονται στα πεδία "Προς" ή "Κοινοποίηση", με αποτέλεσμα οι ηλεκτρονικές διευθύνσεις των παραληπτών να είναι ορατές σε όλους τους παραλήπτες.

Εάν διαπιστώσετε την ύπαρξη παραβίασης προσωπικών δεδομένων, πρέπει να ενημερώσετε άμεσα στη διεύθυνση it-security@ergohellas.gr.

Ακολουθούν χρήσιμες συμβουλές και οδηγίες με στόχο την ασφαλή διαχείριση των εταιρικών πληροφοριών και των πληροφοριακών συστημάτων σας, καθώς και της ERGO Ασφαλιστικής Μονοπρόσωπης Α.Ε. («η εταιρεία»):

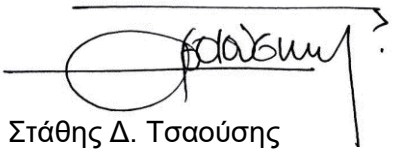
- Οι κωδικοί πρόσβασης (π.χ. passwords για πρόσβαση στον Η/Υ, πρόσβαση στις OnLine πλατφόρμες της εταιρείας) θα πρέπει να απομνημονεύονται και όχι να αποθηκεύονται σε ηλεκτρονικά αρχεία σημειώσεων (π.χ. Notepad, Excel, Word, κ.λπ.). Σε καμία περίπτωση δεν πρέπει οι κωδικοί αυτοί να αποτυπώνονται σε έντυπη μορφή (π.χ. αναγραφή σε post-it κολλημένα σε οθόνες ή κάτω από πληκτρολόγια, σε σημειωματάρια κ.λπ.).
- Θα πρέπει ο μηχανισμός κλειδώματος οθόνης να είναι ενεργοποιημένος (π.χ. η συσκευή να είναι σε κατάσταση αναμονής για πληκτρολόγηση συνθηματικού «screen lock»), ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση στη συσκευή. Στο τέλος του εργασιακού ωραρίου θα πρέπει να απενεργοποιούνται οι Η/Υ των χρηστών.
- Οι εργαζόμενοι δεν πρέπει να απενεργοποιούν ή να παρακάμπτουν τους μηχανισμούς και τους ελέγχους σχετικά με την ασφαλή πλοήγηση στο διαδίκτυο.
- Στις περιπτώσεις κατά τις οποίες παραλαμβάνεται email που περιέχει συνημμένα αρχεία ή συνδέσμους (links), αυτό δεν θα πρέπει να «ανοιχθεί» απευθείας, εάν δεν είναι βέβαιο πρώτα ότι το συγκεκριμένο μήνυμα ηλεκτρονικού ταχυδρομείου προέρχεται από γνωστές ή αξιόπιστες πηγές (π.χ. γνωστός αποστολέας). Υπενθυμίζεται ότι η επικοινωνία σας με την εταιρεία θα γίνεται αποκλειστικά από emails με την κατάληξη @ergohellas.gr. Τέλος, επισημαίνεται ότι η εταιρεία δεν θα σας ζητήσει ποτέ να κοινοποιήσετε τους κωδικούς σας.
- Οι φορητές συσκευές αποθήκευσης όπως CD, DVD, μονάδες USB ή εξωτερικοί σκληροί δίσκοι δεν πρέπει να αφήνονται εκτεθειμένες πάνω στα γραφεία και θα πρέπει να κλειδώνονται σε συρτάρια ή ντουλάπες όταν δεν χρησιμοποιούνται.
- Έγγραφα που περιέχουν προσωπικές και εμπιστευτικές πληροφορίες πρέπει να αποθηκεύονται σε συρτάρια, ντουλάπες ή αρχειοθήκες με ασφαλείς τρόπους (π.χ. κλειδώνοντάς τα σε συρτάρια, ντουλάπια, ειδικά διαμορφωμένα κλειστά δωμάτια).
- Πρέπει να υπάρχει προσωπική παρακολούθηση της διαδικασίας εκτύπωσης από τους εργαζομένους μέχρι αυτή να ολοκληρωθεί, έτσι ώστε να μην παραμένουν έγγραφα με προσωπικά ή εμπιστευτικά δεδομένα στα μηχανήματα εκτύπωσης.
- Όλες οι πληροφορίες σε έντυπη μορφή που είναι εμπιστευτικές ή εμπεριέχουν προσωπικά δεδομένα και δεν χρησιμοποιούνται πλέον για επιχειρηματικούς σκοπούς, θα πρέπει να καταστρέφονται με τρόπους μη ανακτήσιμους, π.χ. σε ειδικούς καταστροφείς εγγράφων.

- Συνιστάται η προσεκτική χρήση εξωτερικών υπηρεσιών επικοινωνίας όταν αυτές αφορούν είδος συνομιλίας (Chat), πλατφόρμες διασκέψεων (teleconference), μέσα κοινωνικής δικτύωσης, υπηρεσίες κοινής χρήσης αρχείων (π.χ. Cloud Storage υπηρεσίες), ιδιωτικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου κ.λπ. Τέλος, δεν θα πρέπει να δημοσιεύονται ευαίσθητες πληροφορίες, όπως για παράδειγμα κωδικοί πρόσβασης, προσωπικά δεδομένα, σε διαδικτυακές πλατφόρμες συνεργατών.

Σε περίπτωση που περιστατικό ασφάλειας επηρεάζει τις προσβάσεις που σας έχουν δοθεί από την ERGO Ασφαλιστική, θα πρέπει να επικοινωνήσετε μέσω email στο it-security@ergohellas.gr ή εναλλακτικά μέσω τηλεφωνικής επικοινωνίας με το Τμήμα Διαχείρισης Συστημάτων, Υποδομών & Δικτύων στον τηλεφωνικό αριθμό 210 9379898.

Εργαζόμαστε τηρώντας τις διαδικασίες που εξασφαλίζουν την ασφαλή άσκηση των δραστηριοτήτων μας

Με φιλικούς χαιρετισμούς,



Στάθης Δ. Τσαούσης
Μέλος του Διοικητικού Συμβουλίου
Διευθυντής Τομέα Πωλήσεων