ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα 15/4/2020
Αριθ. Πρωτ.: 2684

ΔΕΛΤΙΟ ΤΥΠΟΥ

Κατευθυντήριες Γραμμές της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τη λήψη μέτρων ασφάλειας στο πλαίσιο τηλεργασίας

Λόγω του ότι πολλοί οργανισμοί και επιχειρήσεις προτρέπουν ή/και υποχρεώνουν το προσωπικό τους σε τηλεργασία λόγω των μέτρων περιορισμού που έχουν επιβληθεί για την αποτροπή εξάπλωσης της COVID-19, η Αρχή Προστασίας Δεδομένων, με στόχο την ευαισθητοποίηση των υπευθύνων επεξεργασίας, των εκτελούντων την επεξεργασία, των εργαζομένων και γενικότερα του κοινού αναφορικά με τους κινδύνους που αφορούν την προστασία των προσωπικών δεδομένων αλλά, ταυτόχρονα, και τις σχετικές υποχρεώσεις που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων και τον νόμο 4624/2019, εξέδωσε **Κατευθυντήριες Γραμμές για τη λήψη μέτρων ασφαλείας στο πλαίσιο τηλεργασίας**. Τα μέτρα αυτά αφορούν κυρίως την πρόσβαση στο δίκτυο, τη χρήση εφαρμογών ηλεκτρονικού ταχυδρομείου/ανταλλαγής μηνυμάτων, τη χρήση τερματικής συσκευής/αποθηκευτικών μέσων και τον τρόπο πραγματοποίησης τηλεδιασκέψεων.

Τμήμα Επικοινωνίας

Κατευθυντήριες Γραμμές της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τη λήψη μέτρων ασφάλειας στο πλαίσιο τηλεργασίας

Λόγω των μέτρων περιορισμού που έχουν επιβληθεί για την αποτροπή εξάπλωσης της COVID-19, πολλοί οργανισμοί και επιχειρήσεις προτρέπουν ή/και υποχρεώνουν το προσωπικό τους σε τηλεργασία, αξιοποιώντας σχετικές δυνατότητες της τεχνολογίας. Ως τηλεργασία θεωρείται η εργασία από απόσταση (δηλαδή χωρίς φυσική παρουσία στον χώρο της εργασίας) με χρήση των απαραίτητων τεχνολογιών πληροφορικής και επικοινωνιών.

Η Αρχή, με στόχο την ευαισθητοποίηση των υπευθύνων επεξεργασίας, των εκτελούντων την επεξεργασία, των εργαζομένων και γενικότερα του κοινού αναφορικά με τους κινδύνους που αφορούν την προστασία των προσωπικών δεδομένων αλλά, ταυτόχρονα, και τις σχετικές υποχρεώσεις που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων και τον νόμο 4624/2019, παραθέτει τις ακόλουθες Κατευθυντήριες Γραμμές.

1. Ο οργανισμός/επιχείρηση (εφεξής, φορέας) οφείλει να ορίσει και να υποστηρίξει συγκεκριμένες διαδικασίες για την τηλεργασία. Οι διαδικασίες αυτές πρέπει να λαμβάνουν υπόψη, για την κάθε περίπτωση, τη φύση και τη σοβαρότητα των κινδύνων ως προς την προστασία προσωπικών δεδομένων, οι οποίοι απορρέουν από την εξ αποστάσεως εργασία.
2. Ο φορέας οφείλει να ενημερώνει επαρκώς, να εκπαιδεύει και να συνδράμει τους εργαζομένους του στην εφαρμογή των διαδικασιών αυτών, λαμβάνοντας υπόψη ότι πολλοί χρήστες δεν είναι εξοικειωμένοι με τις τεχνολογίες που υποστηρίζουν την τηλεργασία και τους σχετικούς κινδύνους. Για τον σκοπό αυτό, είναι πολύτιμη η συμβολή του Υπεύθυνου Προστασίας Δεδομένων (DPO) όπου έχει ορισθεί.
3. Επισημαίνεται ιδιαίτερα ότι οι υποχρεώσεις των φορέων αναφορικά με την προστασία των προσωπικών δεδομένων των εργαζομένων τους αποκτούν ιδιάζουσα βαρύτητα στην περίπτωση της τηλεργασίας. Και τούτο, διότι ο εργαζόμενος, λόγω του γεγονότος ότι βρίσκεται στο σπίτι του, έχει μεγαλύτερη προσδοκία για την προστασία της ιδιωτικής του ζωής.

Οι διαδικασίες για την τηλεργασία συστήνεται να περιλαμβάνουν μέτρα, όπως τα ακόλουθα:

<u>Πρόσβαση στο δίκτυο</u>

1. Διασφάλιση ότι δεν υπάρχει δυνατότητα μη ασφαλούς απομακρυσμένης πρόσβασης σε πόρους των πληροφοριακών συστημάτων του φορέα, όπως υπολογιστές εσωτερικού δικτύου και εσωτερικά αρχεία. Η ασφαλής σύνδεση μπορεί, ενδεικτικώς, να επιτευχθεί μέσω εικονικού ιδιωτικού δικτύου στο οποίο

πραγματοποιείται κρυπτογράφηση των δεδομένων και αυθεντικοποίηση των χρηστών (π.χ. IPSec VPN).

i. Καθορισμός και περιορισμός των πόρων στους οποίους επιτρέπεται η απομακρυσμένη πρόσβαση στο απολύτως απαραίτητο, ανάλογα με τα καθήκοντα που επιτελεί ο τηλεργαζόμενος.

ii. Σύνδεση σε υπολογιστικά συστήματα του φορέα μέσω υπηρεσίας "απομακρυσμένης επιφάνειας εργασίας" ("Remote Desktop Protocol - RDP"), μόνο εφόσον αυτή γίνεται μέσω ασφαλούς εικονικού ιδιωτικού δικτύου (VPN).

2. Χρήση ασφαλούς πρωτοκόλλου WPA2 με ισχυρό κωδικό, όταν η σύνδεση της συσκευής του τηλεργαζόμενου στο Διαδίκτυο γίνεται μέσω ασύρματου δικτύου (Wi-Fi). Τούτο ισχύει ακόμα και όταν μετά τη σύνδεση στο Διαδίκτυο, γίνεται ασφαλής σύνδεση στο δίκτυο του φορέα π.χ. με χρήση VPN.
3. Αποφυγή αποθήκευσης αρχείων με προσωπικά δεδομένα σε υπηρεσίες διαδικτυακής αποθήκευσης (π.χ. Dropbox, One Drive, google drive), εκτός και αν υπάρχουν τα κατάλληλα εχέγγυα, όπως π.χ. να πρόκειται για υπηρεσία που παρέχεται, με κατάλληλα μέτρα ασφάλειας, από τον φορέα ή τα δεδομένα να αποθηκεύονται αποκλειστικά σε κατάλληλα κρυπτογραφημένη μορφή.

<u>Χρήση εφαρμογών ηλεκτρονικού ταχυδρομείου/ανταλλαγής μηνυμάτων</u>

1. Αποφυγή χρήσης προσωπικού ηλεκτρονικού ταχυδρομείου (π.χ. gmail, yahoo, hotmail) για αποστολή ή λήψη μηνυμάτων για σκοπούς τηλεργασίας, τα οποία σχετίζονται με προσωπικά δεδομένα. Αντ' αυτού, θα πρέπει να χρησιμοποιείται η επαγγελματική ηλεκτρονική διεύθυνση την οποία παρέχει ο φορέας. Εάν αυτό δεν είναι τεχνικά εφικτό (π.χ. μη δυνατότητα πρόσβασης στο εσωτερικό ηλεκτρονικό ταχυδρομείο από εξωτερικό του φορέα δίκτυο), τότε το περιεχόμενο των μηνυμάτων που αφορά προσωπικά δεδομένα πρέπει να κρυπτογραφείται κατάλληλα (π.χ. είτε ολόκληρο το μήνυμα είτε μόνο τα συνημμένα αρχεία).
2. Αποφυγή χρήσης εφαρμογών ανταλλαγής μηνυμάτων (κείμενο ή/και βίντεο) για τους σκοπούς της τηλεργασίας, όταν τα μηνύματα αυτά περιέχουν προσωπικά δεδομένα, των οποίων τυχόν διαρροή θα επέφερε κινδύνους. Αν είναι πραγματικά απαραίτητο, να προτιμώνται υπηρεσίες των οποίων τα χαρακτηριστικά ασφάλειας (κρυπτογράφηση, ρυθμίσεις προστασίας δεδομένων) αξιολογούνται ως ισχυρά.

<u>Χρήση τερματικής συσκευής\αποθηκευτικών μέσων</u>

1. Εγκατάσταση και τακτική ενημέρωση αντιϊκού προγράμματος και “αναχώματος ασφαλείας” (firewall) στη συσκευή (π.χ. υπολογιστής, laptop κτλ.) μέσω της οποίας πραγματοποιείται η τηλεργασία.
2. Εγκατάσταση των πλέον πρόσφατων ενημερώσεων του λογισμικού εφαρμογών και λειτουργικού συστήματος της συσκευής των εργαζομένων.
3. Χρήση προγραμμάτων πλοήγησης στο Διαδίκτυο (π.χ. Firefox, Chrome κτλ.) με τις πλέον πρόσφατες, κάθε φορά, εκδόσεις τους. Μη τήρηση ιστορικού (ανώνυμη περιήγηση) ή διαγραφή από το ιστορικό των συνδέσμων εκείνων που σχετίζονται με την τηλεργασία, κατά το τέλος της εργασίας.
4. Διαχωρισμός των αρχείων που περιέχουν προσωπικά δεδομένα, τα οποία σχετίζονται με την εργασία από προσωπικά αρχεία τα οποία τηρεί ο εργαζόμενος στη συσκευή (π.χ. σε σαφώς διακριτούς φακέλους, με κατάλληλη προσδιοριστική ονομασία). Χρήση «εικονικού μηχανήματος» (virtual machine) αποκλειστικά για την παροχή τηλεργασίας, όταν αυτό είναι εφικτό.
5. Υποστήριξη από τον φορέα διαδικασιών κατάλληλης κρυπτογράφησης αρχείων που περιέχουν προσωπικά δεδομένα, ιδίως όταν τηρούνται σε φορητό/αποσπώμενο μέσο αποθήκευσης (π.χ. usb stick). Ανά περίπτωση, θα πρέπει να εξετάζεται και το ενδεχόμενο κρυπτογράφησης των αρχείων και στην κυρίως συσκευή από την οποία πραγματοποιείται η τηλεργασία (Η/Υ, laptop κτλ.), ιδίως για δεδομένα υψηλού κινδύνου.
6. Υποστήριξη, από τον φορέα, διαδικασιών λήψης αντιγράφων ασφαλείας για αρχεία με προσωπικά δεδομένα, τα οποία υφίστανται επεξεργασία στο πλαίσιο δραστηριοτήτων τηλεργασίας. Για τα αντίγραφα ασφαλείας πρέπει να τηρούνται μέτρα ανάλογα με όσα περιγράφονται στο σημείο 5.
7. «Κλείδωμα» της συσκευής από την οποία γίνεται η τηλεργασία (π.χ. προφύλαξη οθόνης, με κωδικό απενεργοποίησης) εφόσον μένει, για κάποιο λόγο, χωρίς επιτήρηση.

<u>Πραγματοποίηση τηλεδιασκέψεων</u>

1. Στην περίπτωση τηλεδιασκέψεων, θα πρέπει να αξιοποιούνται πλατφόρμες που υποστηρίζουν υπηρεσίες ασφαλείας (κρυπτογράφηση). Για παράδειγμα, θα πρέπει να αποφεύγεται λογισμικό τηλεδιάσκεψης το οποίο δεν εξασφαλίζει κρυπτογράφηση από άκρη σε άκρη (end-to-end encryption).
2. Σε περίπτωση προγραμματισμένης τηλεδιάσκεψης, προστασία του συνδέσμου (link) αυτής (π.χ. όχι δημοσιοποίησή του σε κοινωνικό δίκτυο).
3. Προσεκτική μελέτη των όρων χρήσης και των όρων προστασίας προσωπικών δεδομένων κατά την επιλογή της λύσης τηλεδιάσκεψης.