

Ερωταπαντήσεις βάσει της απόφασης 32/2021, με την οποία εκδίδονται Κατευθυντήριες Γραμμές σχετικά με την εφαρμογή των κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της τηλεργασίας

airetos.gr

1. Τι εννοούμε με τον όρο τηλεργασία;

Η τηλεργασία συνιστά μορφή οργάνωσης ή/και εκτέλεσης εργασίας στο πλαίσιο σύμβασης ή σχέσης εργασίας ή υπηρεσιακής σχέσης με το Δημόσιο, με τη χρήση ΤΠΕ, που παρέχεται εκτός των εγκαταστάσεων του οργανισμού ή της επιχείρησης.

2. Προβλέπεται νομοθετικά η τηλεργασία;

Η τηλεργασία έχει ρυθμιστεί νομοθετικά με τον ν.4807/2021 (ΦΕΚ Α'96) για τους απασχολούμενους του δημοσίου τομέα και με την διάταξη του άρθρου 67 του ν.4808/2021 (ΦΕΚ Α'101) για τους απασχολούμενους του ιδιωτικού τομέα. Και στις δυο περιπτώσεις προβλέπεται η έκδοση προεδρικού διατάγματος για την ειδικότερη ρύθμιση θεμάτων προστασίας δεδομένων προσωπικού χαρακτήρα, μετά από γνώμη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔ).

3. Είναι υποχρεωτική η παροχή τηλεργασίας;

Η παροχή τηλεργασίας είναι καταρχήν προαιρετική. Προβλέπεται, όμως, κατ'εξάιρεση, τόσο για τους απασχολούμενους του δημοσίου τομέα όσο και για τους εργαζόμενους του ιδιωτικού τομέα, η υποχρεωτική παροχή τηλεργασίας μετά από πρόταση του φορέα ή του εργοδότη, αντίστοιχα, κυρίως για λόγους προστασίας της δημόσιας υγείας.

4. Δικαιούται ο εργαζόμενος να παρέχει τηλεργασία;

Ο απασχολούμενος του δημοσίου τομέα δικαιούται να υποβάλει αίτημα στον Προϊστάμενο της Διεύθυνσης του φορέα όπου υπηρετεί, βάσει των χρονικών ορίων και του καθορισμού των θέσεων τηλεργασίας που προβλέπονται στον ν. 4807/2021 ή να υποβάλει αίτημα, σε περίπτωση κινδύνου υγείας καθώς και όταν αντιμετωπίζει μόνιμα ή πρόσκαιρα προβλήματα υγείας, και εφόσον η φύση των καθηκόντων του καθιστά εφικτή την εκτέλεσή τους μέσω τηλεργασίας.

Για τους εργαζόμενους του ιδιωτικού τομέα η τηλεργασία συμφωνείται καταρχήν με τον εργοδότη, κατά την πρόσληψη ή την τροποποίηση της σύμβασης εργασίας. Μπορεί δε να παρασχεθεί κατ' εξαίρεση μετά από αίτηση του εργαζομένου, σε περίπτωση τεκμηριωμένου κινδύνου της υγείας του, ο οποίος μπορεί να αποφευχθεί μέσω τηλεργασίας .

5. Για ποιο λόγο η ΑΠΔ εκδίδει κατευθυντήριες γραμμές για το ζήτημα της τηλεργασίας;

Η παροχή εργασίας εξ αποστάσεως βασίζεται στην χρήση ΤΠΕ και ως αυτοματοποιημένη επεξεργασία εμπίπτει κατεξοχήν στο πεδίο εφαρμογής των κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα. Περαιτέρω, η τηλεργασία συνεπάγεται εκ των πραγμάτων μεγαλύτερη επέμβαση την ιδιωτικότητα των εργαζόμενων και στην προστασία των δεδομένων προσωπικού τους χαρακτήρα, καθιστώντας επιτακτική την ανάγκη στην Αρχή, βάσει των αρμοδιοτήτων της από τον ΓΚΠΔ και τον ν. 4624/2019, να επιβάλει την εφαρμογή των κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα και να προωθήσει την ευαισθητοποίηση του κοινού και των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία σχετικά με την κατανόηση των κινδύνων, των κανόνων, των εγγυήσεων και των δικαιωμάτων και σχετικά με τις υποχρεώσεις τους δυνάμει του ΓΚΠΔ, αντίστοιχα, κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

6. Ποια τα βασικά χαρακτηριστικά της τηλεργασίας που μπορεί να θέσουν σε κίνδυνο την προστασία των προσωπικών δεδομένων και την ιδιωτικότητα του εργαζόμενου;

Η τηλεργασία και η «κινητή τεχνολογία» καθιστά δυσδιάκριτα τα όρια μεταξύ σπιτιού και εργασίας. Οι νέες μορφές εργασίας απαιτούν συχνά μεγαλύτερη συμμετοχή και αυτενέργεια των εργαζομένων αλλά συνεπάγονται και μεγαλύτερη διείσδυση στον ιδιωτικό χώρο και χρόνο, αμφισβητώντας εκ των πραγμάτων την προστασία της ιδιωτικότητας, των προσωπικών δεδομένων και του δικαιώματος στον ιδιωτικό βίο και διαμορφώνοντας παράλληλα μια κουλτούρα «διαρκούς παρουσίας και μόνιμης

επιφυλακής των εργαζομένων», η οποία έχει αρνητικό αντίκτυπο στην ισορροπία μεταξύ της επαγγελματικής και της προσωπικής τους ζωής.

7. Τι είναι το δικαίωμα στην αποσύνδεση;

Σύμφωνα με τις αρχές της νομιμότητας και του περιορισμού του σκοπού του άρθρου, ο απασχολούμενος εξ αποστάσεως έχει το δικαίωμα μετά το πέρας του χρόνου κατά τον οποίο έχει υποχρέωση παροχής εργασίας (συμπεριλαμβανομένων των περιόδων που βρίσκονται σε οποιασδήποτε μορφής άδεια), να αποσυνδέεται χωρίς επιπτώσεις σε βάρος του από τα ψηφιακά μέσα (λογισμικά, ψηφιακή πλατφόρμα, κοινωνικά δίκτυα, ασύρματες συνδέσεις, ηλεκτρονικά μηνύματα, internet/intranet) που χρησιμοποιούνται για την οργάνωση της απασχόλησης.

Το δικαίωμα στην αποσύνδεση προβλέπεται ρητά στις διατάξεις των άρθρων 18 του ν.4807/2021 και 67 παρ. 10 του ν.4808/2021, για τους απασχολούμενους του δημοσίου και του ιδιωτικού τομέα, αντίστοιχα.

8. Είναι νόμιμος ο έλεγχος της τήρησης του χρόνου τηλεργασίας από τον εργοδότη;

Για τους απασχολούμενους του δημοσίου τομέα προβλέπεται η δυνατότητα λειτουργίας συστήματος παρακολούθησης του χρόνου εργασίας και ορίζεται ότι οποιοδήποτε είδος συστήματος παρακολούθησης του χρόνου εργασίας πρέπει να επιβάλλεται από τις λειτουργικές ανάγκες του φορέα.(άρθρο 5 στοιχ. δ' ν.4807/2021).

Ως προς τον ιδιωτικό τομέα, αναμένεται η έκδοση Προεδρικού Διατάγματος σύμφωνα με το άρθρο 67 παρ. 12 ν. 4808/21 με το οποίο θα ρυθμίζονται οι λεπτομέρειες ελέγχου τήρησης του ωραρίου εργασίας και εν γένει της εργατικής νομοθεσίας κατά την τηλεργασία, με διασφάλιση του επιχειρηματικού απορρήτου και των προσωπικών δεδομένων των εργαζομένων.

Με βάση τις αρχές προστασίας των προσωπικών δεδομένων κατ' άρθρο 5 παρ. 1 ΓΚΠΔ θα ήταν καταρχήν θεμιτό εκ μέρους του υπευθύνου επεξεργασίας να ζητά πρόσθετη επιβεβαίωση (αυθεντικοποίηση) από τον χρήστη ΤΠΕ (Η/Υ, λογισμικών επικοινωνίας – ηλεκτρονικής αλληλογραφίας) – απασχολούμενο ότι αυτός πράγματι παρέχει τη συμφωνηθείσα εργασία και να τηρεί τη σχετική πληροφορία.

9. Συνιστά η τηλεργασία λόγο άρσης της υποχρέωσης του υπευθύνου επεξεργασίας για τη συμμόρφωσή του προς τους κανόνες προστασίας δεδομένων προσωπικού χαρακτήρα;

Η υποχρέωση ικανοποίησης των δικαιωμάτων που ασκούνται από τα υποκείμενα των δεδομένων, διατηρείται ακέραιη κατά την εκτέλεση της εργασίας από απόσταση. Από καμία διάταξη του ΓΚΠΔ και της εθνικής νομοθεσίας δεν προβλέπεται η πρόσκαιρη αναστολή των σχετικών προθεσμιών και υποχρεώσεων ικανοποίησης των δικαιωμάτων των υποκειμένων των δεδομένων. Επιπλέον, συνιστά υποχρέωση του υπευθύνου επεξεργασίας να τεκμηριώνει τους λόγους καθυστέρησης ή μη ικανοποίησης των ασκηθέντων δικαιωμάτων. Τυχόν δε επίκληση σχετικών καθυστερήσεων τόσο έναντι των υποκειμένων των δεδομένων, όσο και έναντι της Αρχής κατά την άσκηση των ελεγκτικών των αρμοδιοτήτων θα πρέπει να είναι ιδιαίτερως τεκμηριωμένη και μη προσχηματική δοθέντος ότι τα απαιτούμενα τεχνικά και οργανωτικά μέτρα θα πρέπει να έχουν ήδη ληφθεί και να εφαρμόζονται προ της έναρξης της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

10. Ποιες οι γενικές υποχρεώσεις για την ασφάλεια κατά την επεξεργασία προσωπικών δεδομένων μέσω τηλεργασίας;

Ο υπεύθυνος επεξεργασίας έχει διαρκή υποχρέωση λήψης τεχνικών μέτρων ασφάλειας και σχετικής ενημέρωσης των απασχολούμενων, αξιοποιώντας τις υπηρεσίες του Υπευθύνου Προστασίας Δεδομένων της επιχείρησης ή του οργανισμού (άρθρο 39 παρ. 1 στοιχ. α' ΓΚΠΔ). Επίσης ευθύνεται για την ασφαλή επεξεργασία των προσωπικών δεδομένων στο πλαίσιο της λειτουργίας της επιχείρησης που λαμβάνει χώρα μέσω των συστημάτων υλικού και λογισμικού της εταιρίας, δικτύων VPN κ.λπ. των οποίων κάνουν χρήση οι εργαζόμενοι, συμπεριλαμβανομένων των αποθηκευμένων σε τερματικές συσκευές, διακομιστές κ.λπ., είτε ανήκουν στην επιχείρηση, είτε στους ίδιους τους υπαλλήλους.

Η Αρχή, στις **Κατευθυντήριες Γραμμές 2/2020** έχει συστήσει τεχνικά μέτρα που θα πρέπει να περιλαμβάνουν οι διαδικασίες που εφαρμόζει ο υπεύθυνος επεξεργασίας για τη τηλεργασία.

Εξάλλου, οι απασχολούμενοι έχουν υποχρέωση τήρησης απορρήτου- εχεμύθειας – πίστης, κατ' εφαρμογή των διατάξεων των άρθρων 371 ΠΚ, 26 του ν. 3528/2007 και 1 του ν. 146/1914, κατά τρόπο που να διασφαλίζεται ότι τρίτοι προς τη σχέση απασχόλησης (π.χ. μέλη οικογένειας) δεν αποκτούν πρόσβαση στα αρχεία του οργανισμού ή της επιχείρησης.

11. Τι σημαίνει ο όρος «B.Y.O.D»;

Το ακρωνύμιο του "B.Y.O.D." (συντομογραφία της αγγλικής έκφρασης "Bring your own device", "Φέρτε τη δική σας συσκευή"), περιγράφει τη χρήση εξοπλισμού προσωπικών συσκευών σε επαγγελματικό πλαίσιο, η οποία εφαρμόζεται ευρέως κατά την παροχή εργασίας εξ αποστάσεως. Η δυνατότητα αυτή προβλέπεται πλέον νομοθετικά (βλ. άρ. 12 παρ. 1 τελ. εδ. και 15 περ. γ' ν. 4807/2021 και αρ. 67 παρ. 4 , 5 εδ. γ' ν. 4808/2021).

12. Ποια τα ζητήματα του «B.Y.O.D» για την ιδιωτικότητα του εργαζόμενου και με ποια μέτρα μπορούν να αντιμετωπιστούν από τον εργοδότη;

Ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει εγκεκριμένη από την ανώτατη διοίκηση του φορέα πολιτική και διαδικασία για τη χρήση ιδιωτικού εξοπλισμού προ της ενάρξεως της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Δεν επιτρέπεται καταρχήν η προσπέλαση εκ μέρους του υπεύθυνου επεξεργασίας, οργανισμού ή επιχείρησης, σε τμήματα της προσωπικής συσκευής, τα οποία τεκμαίρεται ότι χρησιμοποιούνται μόνο για ιδιωτικούς σκοπούς. Επιπλέον, πρέπει να εφαρμόζονται κατάλληλα μέτρα με σκοπό τη διάκριση μεταξύ της ιδιωτικής και επαγγελματικής χρήσης της συσκευής, ιδίως όταν μέσω της παρακολούθησης της θέσης και της κυκλοφορίας των συσκευών αυτών είναι δυνατό να συλλεγούν δεδομένα που σχετίζονται με την ιδιωτική και οικογενειακή ζωή του απασχολούμενου. Ακόμα, ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει μεθόδους με τις οποίες να διαβιβάζονται με ασφάλεια μεταξύ της συσκευής του απασχολούμενου και του δικτύου του προσωπικά δεδομένα που λαμβάνουν επεξεργασία στο πλαίσιο της υπηρεσιακής ή επιχειρηματικής δραστηριότητας.

13. Ποια είναι τα μέτρα ασφάλειας κατά την χρήση B.Y.O.D. στην τηλεργασία:

Ενδεικτικά μέτρα ασφάλειας μπορεί μεταξύ άλλων να αποτελέσουν:

- ✓ ο φυσικός ή λογικός διαχωρισμός των τμημάτων της προσωπικής συσκευής που προορίζεται για χρήση σε επαγγελματικό περιβάλλον
- ✓ ο έλεγχος της απομακρυσμένης πρόσβασης μέσω ισχυρού μηχανισμού ελέγχου ταυτότητας χρήστη
- ✓ ο ορισμός μέτρων κρυπτογράφησης για ροές πληροφοριών (VPN, TLS κ.λπ.)
- ✓ ο ορισμός διαδικασίας για αποκατάσταση σε περίπτωση βλάβης ή απώλειας της προσωπικής συσκευής
- ✓ η απαίτηση τήρησης βασικών μέτρων ασφαλείας, όπως το κλείδωμα του τερματικού με κωδικό πρόσβασης σύμφωνα με τις βέλτιστες πρακτικές και τη χρήση ενός ενημερωμένου αντιϊικού προγράμματος,
- ✓ η ευαισθητοποίηση των χρηστών σχετικά με τους κινδύνους,
- ✓ η προηγούμενη έγκριση του διαχειριστή του δικτύου ή/και του εργοδότη για τη χρήση προσωπικού εξοπλισμού,
- ✓ η ενημέρωση για τις ευθύνες όλων και η αναφορά των προφυλάξεων που πρέπει να λαμβάνονται σε έναν δεσμευτικό χάρτη.

14. Ποια είναι τα συνιστώμενα μέτρα για τη διασφάλιση της εμπιστευτικότητας κατά τη διακίνηση προσωπικών δεδομένων μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και εκτυπώσεων;

Πρέπει να αποφεύγεται η προώθηση μηνυμάτων ηλεκτρονικού ταχυδρομείου, τόσο από την επιχείρηση ή τον οργανισμό όσο και από τον εξ αποστάσεως απασχολούμενο στην προσωπική ηλεκτρονική διεύθυνση του τελευταίου, ιδίως όταν δεν πραγματοποιείται κρυπτογράφηση του περιεχόμενου του μηνύματος.

Ακόμα, η εκτύπωση υπηρεσιακών/εταιρικών εγγράφων στην οικία του απασχολούμενου ή σε τόπο/χώρο άλλο πέραν του χώρου εργασίας πρέπει να πραγματοποιείται κατά τρόπο που να διασφαλίζεται ότι δεδομένα προσωπικά χαρακτήρα δεν μπορούν να διαρρεύσουν σε τρίτα μη δικαιούμενα πρόσωπα..

15. Ποια τα συνιστώμενα μέτρα για την αντιμετώπιση επιθέσεων τύπου ransomware;

Αναφορικά με τη διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος επεξεργασίας οφείλει να λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η χρήση κατάλληλων εργαλείων εντοπισμού κακόβουλου λογισμικού, η επαρκής διαχείριση ενημερώσεων λογισμικού στις συσκευές μέσω των οποίων πραγματοποιείται η τηλεργασία, καθώς και η κατάλληλη διαδικασία λήψης αντιγράφων ασφαλείας. Οφείλει επίσης να παρέχει τα μέσα για να εξακριβωθεί εάν τα μηνύματα που λαμβάνονται μέσω ηλεκτρονικού ταχυδρομείου ή με άλλα μέσα επικοινωνίας είναι αυθεντικά και αξιόπιστα. Οι εργαζόμενοι θα πρέπει να εκπαιδευτούν ώστε να αναγνωρίζουν απόπειρες τέτοιων επιθέσεων (π.χ. αναγνώριση των «ύποπτων» μηνυμάτων ηλεκτρονικού ταχυδρομείου), τότε έχει πραγματοποιηθεί μια τέτοια επίθεση και να γνωρίζουν την υποχρέωσή τους να το αναφέρουν αμέσως στον υπεύθυνο ασφαλείας ή και στον υπεύθυνο προστασίας δεδομένων, βάσει μίας σαφώς καταγεγραμμένης διαδικασίας διαχείρισης περιστατικών παραβίασης δεδομένων.

16. Επιτρέπεται η επιτήρηση του εργαζόμενου με την υποχρέωση συνεχούς λειτουργίας της κάμερας του Η/Υ ή την κοινή χρήση της οθόνης ή την εγκατάσταση και λειτουργία λογισμικού καταγραφής πληκτρολόγησης Keylogger ή την υποχρέωση του εργαζομένου να εκτελεί πολύ τακτικές ενέργειες για να αποδείξει την παρουσία του πίσω από την οθόνη του;

Όπως έχει διαπιστώσει η Αρχή με σειρά αποφάσεων της που αφορούν ζητήματα ελέγχου των επικοινωνιών των εργαζομένων από εργοδότη (βλ. ΑΠΔ 34/2018, 26/2019 και 43/2019), «μια συστηματική, διαρκής και γενικευμένη συλλογή δεδομένων προσωπικού χαρακτήρα που οδηγεί στην κατάρτιση και συνεχή ανανέωση προφίλ ...δύσκολα θα μπορούσε να χαρακτηριστεί ως σύμφωνη με την αρχή της αναλογικότητας» (ΑΠΔ 5/2020). Με βάση την αρχή της λογοδοσίας κατ' αρ. 5 παρ. 2 ΓΚΠΔ εναπόκειται στον υπεύθυνο επεξεργασίας, μετά από εσωτερική τεκμηρίωση και αξιολόγηση, να κρίνει σχετικά, αφού λάβει υπόψη και τη σχετική νομολογία της Αρχής.

17. Υποχρεούται ο εργαζόμενος στο πλαίσιο τηλεδιάσκεψης να έχει ανοικτή την κάμερα ή αρκεί η συμμετοχή μέσω του μικροφώνου;

Κατά την πραγματοποίηση τηλεδιασκέψεων, ο υπεύθυνος επεξεργασίας θα πρέπει κατ' αρχήν να μην προβαίνει σε χρήση συστημάτων λήψης και εγγραφής κινούμενων εικόνων του τηλεργαζόμενου (κάμερα), ούτε να υποχρεώνει τους τηλεργαζόμενους να ενεργοποιούν την σχετική ρύθμιση, εκτός αν πληρούνται οι προϋποθέσεις του δεύτερου εδαφίου της παρ. 6 του άρθρου 6 του ν. 4807/2021 και έχει προηγουμένως προβεί σε τεκμηρίωση και αξιολόγηση της αναγκαιότητας και προσφορότητας (εκφάνσεις της αρχής της αναλογικότητάς) της εν λόγω επεξεργασίας.

Αντίστοιχα, ο απασχολούμενος εξ αποστάσεως, δικαιούται, κατ' εφαρμογή της αρχής της ελαχιστοποίησης των δεδομένων, να ενεργοποιεί τη δυνατότητα της χρησιμοποιούμενης πλατφόρμας, για συμμετοχή του σ' αυτή μόνο μέσω μικροφώνου, και όχι συνεχώς κατά τη διάρκεια πραγματοποίησής της μέσω κάμερας, ιδίως όταν συντρέχουν λόγοι που το επιβάλλουν (π.χ. προστασία της ανηλικότητας). Επιπλέον, ο απασχολούμενος εξ αποστάσεως συστήνεται να επιλέγει δυνατότητες της χρησιμοποιούμενης πλατφόρμας που επιτρέπουν την απόκρυψη φόντου (background) με θόλωση ή με προσθήκη εικόνας (virtual background) προκειμένου να αποφευχθεί ο κίνδυνος αποκάλυψης προσωπικών πληροφοριών που μπορεί να προκύψουν από την θέαση.

18. Επιτρέπεται η καταγραφή της τηλεδιάσκεψης από τον εργοδότη;

Αναφορικά με την καταγραφή των τηλεδιασκέψεων που πραγματοποιούνται για τους σκοπούς των υποχρεώσεων του εργαζομένου όπως προκύπτουν από τη σύμβαση τηλεργασίας ή τον νόμο, ο υπεύθυνος επεξεργασίας (εργοδότης) οφείλει, κατ' εφαρμογή των αρχών της αναλογικότητας και της ελαχιστοποίησης, να μην προβαίνει σε αυτήν, εκτός αν δύναται να αποδείξει ότι μία τέτοια επεξεργασία είναι απολύτως αναγκαία και πρόσφορη αλλά και ασφαλής σε σχέση με τον επιδιωκόμενο σκοπό.

Σε περίπτωση καταγραφής τηλεδιάσκεψης με τρίτο πρόσωπο/μέρος (πέραν του απασχολούμενου) που πραγματοποιείται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής, απαιτείται η μετά από προηγούμενη ενημέρωση για τους σκοπούς της

καταγραφής προηγούμενη συγκατάθεση των μερών της επικοινωνίας (άρθρο 4 παρ. 3 ν.3471/2006).

19. Επιτρέπεται η χρήση πλατφόρμας τηλεδιάσκεψης ή εργαλείων κατά την τηλεργασία μέσω των οποίων λαμβάνει χώρα διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες;

Σε περίπτωση που κατά την τηλεργασία ή /και την τηλεδιάσκεψη λαμβάνει χώρα διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, ο υπεύθυνος επεξεργασίας χρησιμοποιεί εργαλεία και πλατφόρμες που συμμορφώνονται με τις ρυθμίσεις του Κεφαλαίου V του ΓΚΠΔ για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή, μετά την κατάργηση με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης Schrems II της Ασπίδας Προστασίας ΕΕ-ΗΠΑ για τις διατλαντικές διαβιβάσεις δεδομένων («Privacy Shield»), χρησιμοποιεί για τη διαβίβαση τυποποιημένες συμβατικές ρήτρες (Standard Contractual Clauses) που έχουν εγκριθεί από την Ευρωπαϊκή Επιτροπή και παραμένουν σε ισχύ.

20. Ποια μέτρα συμμόρφωσης προς τις απαιτήσεις του ΓΚΠΔ, της νομοθεσίας για την προστασία των προσωπικών δεδομένων και της τηλεργασίας συστήνεται στον εργοδότη να λαμβάνει στο πλαίσιο της αρχής της λογοδοσίας;

Με την επιφύλαξη των ελάχιστων τεχνικών και οργανωτικών μέτρων για τη συμμόρφωση προς τις απαιτήσεις προστασίας προσωπικών δεδομένων των τηλεργαζόμενων που πρόκειται να εξειδικευθούν με τα υπό έκδοση Προεδρικά Διατάγματα (βλ. αρ. 19 ν. 4807/2021 και αρ. 67 παρ. 12 ν. 4808/2021) η Αρχή συστήνει προς τους υπευθύνους επεξεργασίας να εξετάσουν κατ' ελάχιστον τη λήψη των κατωτέρω μέτρων:

- Να επικαιροποιούν το αρχείο καταγραφής κατά το άρθρο 30 ΓΚΠΔ.
- Να επικαιροποιούν – τροποποιούν τις συμβάσεις επεξεργασίας δεδομένων με εκτελούντες την επεξεργασία κατ' άρθρο 28 ΓΚΠΔ.
- Να επικαιροποιούν τις πολιτικές και διαδικασίες για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, αλλά και να εξετάζουν το ενδεχόμενο κατάρτισης και εφαρμογής πολιτικής επεξεργασίας προσωπικών δεδομένων

για λόγους που συνδέονται με έκτακτες συνθήκες (π.χ. Covid19) και την αντιμετώπιση σχετικών περιστατικών

- Να διαθέτουν πολιτική και διαδικασίες για την τηλεργασία
- Να διαθέτουν πολιτική και διαδικασίες για την χρήση ιδιωτικού εξοπλισμού σε επαγγελματικό πλαίσιο (B.Y.O.D.)
- Να διενεργούν όπου απαιτείται εκτίμηση αντικτύπου
- Να συμβουλεύονται τους Υπευθύνους Προστασίας Δεδομένων
- Να ενημερώνουν και εκπαιδεύουν το προσωπικό σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα κατά την παροχή τηλεργασίας
- Σε περίπτωση τυχόν επεξεργασίας των εν λόγω δεδομένων των εργαζομένων από τον εργοδότη εκτός της Ε.Ε. (περιλαμβανομένου και του Η.Β. σύντομα) θα πρέπει πλέον να λαμβάνεται υπόψη η απόφαση του ΔΕΕ Schrems II.