

## 1. Σκοπός

Η παρούσα Πολιτική Τηλεργασίας (εφεξής «Πολιτική») καθορίζει το πλαίσιο οργάνωσης, τους κανόνες λειτουργίας και τα τεχνικά και οργανωτικά μέτρα ασφάλειας που εφαρμόζει το Υπουργείο Υποδομών και Μεταφορών (εφεξής «Υπουργείο» ή «Φορέας»), υπό την ιδιότητά του ως υπευθύνου επεξεργασίας, κατά την παροχή εργασίας εξ αποστάσεως από το προσωπικό του.

Σκοπός της Πολιτικής είναι η διασφάλιση της επιχειρησιακής συνέχειας του Υπουργείου, η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των υπηρεσιακών πληροφοριών και υποδομών, καθώς και η προστασία των δεδομένων προσωπικού χαρακτήρα των τηλεργαζομένων, των λοιπών υπαλλήλων και των τρίτων φυσικών προσώπων (πολιτών, συναλλασσομένων) των οποίων τα δεδομένα ενδέχεται να τύχουν επεξεργασίας κατά την άσκηση της τηλεργασίας.

Η Πολιτική συντάχθηκε σε συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 («ΓΚΠΔ»), τον ν. 4624/2019, τον ν. 4807/2021 για την τηλεργασία στον δημόσιο τομέα, το Προεδρικό Διάταγμα 13/2025 και τις Κατευθυντήριες Γραμμές της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

## 2. Πεδίο Εφαρμογής

Η παρούσα Πολιτική εφαρμόζεται σε όλο το προσωπικό του Υπουργείου —μόνιμους υπαλλήλους και υπαλλήλους με σχέση εργασίας ιδιωτικού δικαίου αορίστου ή ορισμένου χρόνου, συμπεριλαμβανομένων των απασχολούμενων με σύμβαση έμμισθης εντολής— το οποίο παρέχει, εν όλω ή εν μέρει, την εργασία του εξ αποστάσεως με χρήση τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ), σύμφωνα με τους όρους του ν. 4807/2021.

Εξαιρούνται από την τηλεργασία οι ασκούντες καθήκοντα προϊσταμένου.

Η Πολιτική εφαρμόζεται τόσο σε κανονικές όσο και σε έκτακτες συνθήκες παροχής τηλεργασίας (π.χ. λόγω κρίσης δημόσιας υγείας ή άλλου έκτακτου γεγονότος) και καλύπτει τη χρήση τόσο υπηρεσιακού εξοπλισμού («Σταθμός Τηλεργασίας») όσο και, κατ' εξαίρεση, προσωπικού εξοπλισμού του τηλεργαζομένου (B.Y.O.D. – «Bring Your Own Device»).

## 3. Νομικό και Κανονιστικό Πλαίσιο

Η παρούσα Πολιτική βασίζεται στο ακόλουθο νομικό και κανονιστικό πλαίσιο:

- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός για την Προστασία Δεδομένων - ΓΚΠΔ).
- Ν. 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679...».
- Ν. 4807/2021 «Θεσμικό πλαίσιο τηλεργασίας, διατάξεις για το ανθρώπινο δυναμικό του δημοσίου τομέα και άλλες επείγουσες ρυθμίσεις».
- Προεδρικό Διάταγμα υπ' αριθμ. 13/2025 «Προστασία δεδομένων προσωπικού χαρακτήρα κατά την τηλεργασία στον δημόσιο τομέα» (ΦΕΚ Α' 19/13.02.2025).
- Ν. 4808/2021 (άρθρο 67, όπως αντικατέστησε το άρθρο 5 του ν. 3846/2010) για την τηλεργασία στον ιδιωτικό τομέα, στο μέτρο που παρέχει ερμηνευτικά κριτήρια εφαρμοστέα κατ' αναλογία.
- Κατευθυντήριες Γραμμές 1/2021 και Απόφαση 32/2021 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) για τη λήψη μέτρων ασφάλειας στο πλαίσιο της τηλεργασίας.

- Η υπ' αριθμ. οικ.Φ.Β2/21011/153/27.03.2020 εγκύκλιος του Υπουργείου Υποδομών και Μεταφορών με βασικά μέτρα ασφάλειας για την παροχή εξ αποστάσεως εργασίας.
- Ν. 3528/2007 (Υπαλληλικός Κώδικας), ιδίως ως προς την υποχρέωση εχεμύθειας (άρθρο 26) και το πειθαρχικό δίκαιο (άρθρα 107 επ.).

## 4. Ορισμοί

---

- **Τηλεργασία:** η μορφή οργάνωσης και εκτέλεσης εργασίας στο πλαίσιο της οποίας ο υπάλληλος εκτελεί τα καθήκοντά του, εν όλω ή εν μέρει, εκτός των εγκαταστάσεων του Υπουργείου, με τη χρήση τεχνολογιών πληροφορικής και επικοινωνιών.
- **Τηλεργαζόμενος:** ο υπάλληλος του Υπουργείου που παρέχει την εργασία του με καθεστώς τηλεργασίας, κατόπιν έγκρισης σύμφωνα με τις κείμενες διατάξεις.
- **Σταθμός Τηλεργασίας:** ο τηλεπικοινωνιακός εξοπλισμός και η τεχνολογική συσκευή (Η/Υ, περιφερειακά, λογισμικό) που προμηθεύει το Υπουργείο στον τηλεργαζόμενο για την εκτέλεση των καθηκόντων του.
- **B.Y.O.D. (Bring Your Own Device):** η χρήση προσωπικού τεχνολογικού εξοπλισμού του τηλεργαζομένου για την παροχή τηλεργασίας, κατ' εξαίρεση και κατόπιν έγκρισης του Υπουργείου, όταν αυτό δεν είναι σε θέση να παράσχει Σταθμό Τηλεργασίας.
- **Φορέας / Υπεύθυνος Επεξεργασίας:** το Υπουργείο Υποδομών και Μεταφορών, το οποίο καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της τηλεργασίας.
- **Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ):** το φυσικό ή νομικό πρόσωπο που έχει οριστεί από το Υπουργείο σύμφωνα με το άρθρο 37 ΓΚΠΔ και επικουρεί στην εφαρμογή της παρούσας Πολιτικής.

## 5. Γενικές Αρχές Επεξεργασίας

---

Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της τηλεργασίας διέπεται από τις ακόλουθες αρχές του άρθρου 5 ΓΚΠΔ:

- Νομιμότητα, αντικειμενικότητα και διαφάνεια: ο τηλεργαζόμενος ενημερώνεται με σαφή και κατανοητό τρόπο για τους σκοπούς, τη νομική βάση και τους κινδύνους της επεξεργασίας.
- Περιορισμός του σκοπού: τα δεδομένα συλλέγονται αποκλειστικά για τους σκοπούς οργάνωσης και εκτέλεσης της τηλεργασίας.
- Ελαχιστοποίηση δεδομένων: υποβάλλονται σε επεξεργασία μόνο τα δεδομένα που είναι απολύτως αναγκαία.
- Ακρίβεια και περιορισμός περιόδου αποθήκευσης, όπως εξειδικεύεται στην Ενότητα 15 της παρούσας.
- Ακεραιότητα και εμπιστευτικότητα: εφαρμόζονται τα τεχνικά και οργανωτικά μέτρα που περιγράφονται στην Ενότητα 9.
- Λογοδοσία: το Υπουργείο τεκμηριώνει και είναι σε θέση να αποδείξει τη συμμόρφωσή του με τις ανωτέρω αρχές.

## 6. Έγκριση και Οργάνωση της Τηλεργασίας

---

Η παροχή τηλεργασίας εγκρίνεται από τον αρμόδιο Προϊστάμενο Διεύθυνσης, σύμφωνα με το άρθρο 14 του ν. 4807/2021, κατόπιν αιτήματος του υπαλλήλου.

Η τηλεργασία μπορεί να παρέχεται από την οικία του τηλεργαζομένου ή από άλλο χώρο εντός της Ελληνικής Επικράτειας ή εντός των συνόρων κρατών μελών του Συμβουλίου της Ευρώπης, υπό την προϋπόθεση ότι ο χώρος πληροί τις ελάχιστες προϋποθέσεις εργονομίας, υγιεινής και ασφάλειας και καθιστά εφικτή την απρόσκοπτη εκτέλεση των καθηκόντων.

Πριν από την έναρξη κάθε προγράμματος τηλεργασίας, το Υπουργείο διενεργεί εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (άρθρο 35 ΓΚΠΔ), σύμφωνα με το άρθρο 3 παρ. 3 του ΠΔ 13/2025, εφόσον δεν έχει ήδη διενεργηθεί αντίστοιχη εκτίμηση για τη συγκεκριμένη επεξεργασία.

## 7. Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα

---

Κατά την τηλεργασία ενδέχεται να τύχουν επεξεργασίας οι ακόλουθες κατηγορίες δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 4 του ΠΔ 13/2025:

- Δεδομένα ταυτότητας (ονοματεπώνυμο, όνομα χρήστη).
- Δεδομένα επικοινωνίας (διεύθυνση ηλεκτρονικού ταχυδρομείου).
- Τεχνικά δεδομένα (διεύθυνση πρωτοκόλλου διαδικτύου - IP).
- Δεδομένα ήχου ή/και εικόνας, σε περίπτωση διενέργειας τηλεδιασκέψεων, σύμφωνα με τους όρους της Ενότητας 11.
- Οποιοδήποτε άλλο δεδομένο σχετίζεται με την άσκηση των καθηκόντων του Φορέα και είναι απαραίτητο για τον σκοπό αυτό, τηρουμένης της αρχής της ελαχιστοποίησης.

Τα ανωτέρω δεδομένα αφορούν τους τηλεργαζόμενους, λοιπούς εργαζόμενους του Υπουργείου, καθώς και τυχόν τρίτα φυσικά πρόσωπα (π.χ. συμμετέχοντες σε τηλεδιάσκεψη, πολίτες που συναλλάσσονται με την Υπηρεσία).

## 8. Υποχρεώσεις του Υπουργείου ως Υπευθύνου Επεξεργασίας

---

### 8.1 Παροχή Εξοπλισμού

Η Υπηρεσία Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων (Δ9) του Υπουργείου προμηθεύει τον τηλεργαζόμενο με τον απαραίτητο και κατάλληλο Σταθμό Τηλεργασίας για την αποτελεσματική εκτέλεση των καθηκόντων του. Ο Σταθμός Τηλεργασίας χρησιμοποιείται αποκλειστικά για την άσκηση των υπηρεσιακών καθηκόντων.

### 8.2 Ασφαλής Απομακρυσμένη Πρόσβαση

Το Υπουργείο διασφαλίζει τη δυνατότητα ασφαλούς απομακρυσμένης πρόσβασης στους πόρους των πληροφοριακών του συστημάτων. Η πρόσβαση σε εσωτερικές εφαρμογές, ψηφιακά αρχεία και ηλεκτρονικές βάσεις δεδομένων που φιλοξενούνται στο εσωτερικό δίκτυο πραγματοποιείται αποκλειστικά μέσω εικονικού ιδιωτικού δικτύου (VPN) ή αντίστοιχης τεχνολογίας με κρυπτογραφημένη και προστατευμένη δρομολόγηση δεδομένων.

### 8.3 Ενημέρωση και Εκπαίδευση

Το Υπουργείο, με τη συνδρομή του Υπευθύνου Προστασίας Δεδομένων, ενημερώνει επαρκώς, εκπαιδεύει και επικουρεί τους τηλεργαζόμενους σχετικά με την ασφαλή διαμόρφωση και χρήση του εξοπλισμού τους, τη χρήση ισχυρών κωδικών πρόσβασης, την ασφαλή χρήση ηλεκτρονικού ταχυδρομείου και εξωτερικών μέσων αποθήκευσης, καθώς και την ασφαλή πλοήγηση στο διαδίκτυο.

### 8.4 Εκτίμηση Αντικτύπου και Τεκμηρίωση

Το Υπουργείο τηρεί πολιτικές ασφάλειας και διαδικασίες ανταπόκρισης σε συμβάντα ασφάλειας, και μεριμνά για την περιοδική αναθεώρησή τους.

Οι Υπηρεσίες τηρούν επικαιροποιημένο αρχείο δραστηριοτήτων επεξεργασίας (άρθρο 30 ΓΚΠΔ) και διενεργούν Μελέτη Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων (άρθρο 35 ΓΚΠΔ).

## 9. Τεχνικά και Οργανωτικά Μέτρα Ασφάλειας

---

Τα ακόλουθα μέτρα είναι υποχρεωτικά για κάθε τηλεργαζόμενο, ανεξαρτήτως αν χρησιμοποιεί υπηρεσιακό ή, κατ' εξαίρεση, προσωπικό εξοπλισμό.

### 9.1 Ασφάλεια Οικιακού Δικτύου

- Αλλαγή του προεπιλεγμένου (default) κωδικού διαχείρισης του δρομολογητή (router) και, όπου είναι εφικτό, του ονόματος χρήστη διαχειριστή.
- Αλλαγή του προεπιλεγμένου κωδικού πρόσβασης και ονόματος (SSID) του ασύρματου οικιακού δικτύου.
- Χρήση ενημερωμένου πρωτοκόλλου κρυπτογράφησης ασύρματης σύνδεσης με ισχυρό κωδικό πρόσβασης.
- Έλεγχος και αναγνώριση των συσκευών που συνδέονται στο οικιακό δίκτυο, ώστε να αποφεύγεται μη εξουσιοδοτημένη πρόσβαση.
- Αποφυγή σύνδεσης του Σταθμού Τηλεργασίας σε δημόσια ασύρματα δίκτυα (public Wi-Fi).

### 9.2 Κωδικοί Πρόσβασης και Ταυτοποίηση

- Χρήση ισχυρών και μοναδικών κωδικών πρόσβασης, μήκους τουλάχιστον 12 χαρακτήρων, με συνδυασμό πεζών/κεφαλαίων, αριθμών και ειδικών χαρακτήρων.
- Χρήση διαφορετικού κωδικού πρόσβασης για κάθε λογαριασμό και συσκευή, ώστε τυχόν παραβίαση ενός κωδικού να μην θέτει σε κίνδυνο το σύνολο των λογαριασμών.
- Ενεργοποίηση, όπου είναι τεχνικά εφικτό, ελέγχου ταυτότητας δύο παραγόντων (2FA) για την πρόσβαση σε υπηρεσιακούς λογαριασμούς και εφαρμογές.
- Χρήση εγκεκριμένου λογισμικού διαχείρισης κωδικών πρόσβασης (password manager), κατόπιν σχετικής υπόδειξης της Υπηρεσίας Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων (Δ9).

### 9.3 Ενημερώσεις Λογισμικού και Προστασία από Κακόβουλο Λογισμικό

- Ενεργοποίηση αυτόματων ενημερώσεων (automatic updates) για το λειτουργικό σύστημα και τις εφαρμογές του Σταθμού Τηλεργασίας.
- Εγκατάσταση και τακτική ενημέρωση λογισμικού προστασίας από ιούς (antivirus) και τείχους προστασίας (firewall) στον Σταθμό Τηλεργασίας.
- Απαγόρευση εγκατάστασης μη αδειοδοτημένου («πειρατικού») λογισμικού, καθώς και εγκατάστασης εφαρμογών από μη αξιόπιστες πηγές.
- Άμεση αναφορά στην Υπηρεσία Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων (Δ9) κάθε ένδειξης πιθανής μόλυνσης του Σταθμού Τηλεργασίας με κακόβουλο λογισμικό (π.χ. ασυνήθιστη συμπεριφορά συστήματος, αναδυόμενα παράθυρα, άγνωστες εφαρμογές).

### 9.4 Προστασία από Επιθέσεις Κοινωνικής Μηχανικής (Phishing)

- Ιδιαίτερη προσοχή σε μηνύματα ηλεκτρονικού ταχυδρομείου που δημιουργούν αίσθημα επείγοντος, ζητούν παράκαμψη διαδικασιών ασφαλείας ή προέρχονται από φαινομενικά γνωστούς αποστολείς με ασυνήθιστο περιεχόμενο.
- Έλεγχος της πραγματικής διεύθυνσης του αποστολέα πριν από οποιαδήποτε ενέργεια, και αποφυγή ανοίγματος συνημμένων αρχείων ή συνδέσμων από άγνωστη ή ύποπτη πηγή.
- Άμεση αναφορά ύποπτων μηνυμάτων στην αρμόδια υπηρεσία ασφάλειας/πληροφορικής, χωρίς απάντηση σε αυτά.

## 9.5 Αντίγραφα Ασφαλείας

Το Υπουργείο μεριμνά για την τακτική λήψη αντιγράφων ασφαλείας (backup) των υπηρεσιακών δεδομένων που τηρούνται σε κεντρικά συστήματα. Ο τηλεργαζόμενος δεν αποθηκεύει μόνιμα υπηρεσιακά δεδομένα αποκλειστικά σε τοπικό αποθηκευτικό μέσο του Σταθμού Τηλεργασίας, χωρίς αυτά να είναι διαθέσιμα και σε υπηρεσιακό περιβάλλον.

## 10. Χρήση Προσωπικού Εξοπλισμού (B.Y.O.D.)

Η χρήση προσωπικού εξοπλισμού για την παροχή τηλεργασίας επιτρέπεται μόνο κατ' εξαίρεση, εφόσον το Υπουργείο δεν έχει τη δυνατότητα να παράσχει Σταθμό Τηλεργασίας, και μόνο κατόπιν έγκρισης σύμφωνα με τα άρθρα 12 και 15 του ν. 4807/2021.

Στην περίπτωση αυτή εφαρμόζονται, κατ' ελάχιστον, τα ακόλουθα μέτρα:

- Λογικός ή φυσικός διαχωρισμός των υπηρεσιακών δεδομένων και εφαρμογών από την προσωπική χρήση της συσκευής.
- Πρόσβαση στο δίκτυο του Υπουργείου αποκλειστικά μέσω VPN ή αντίστοιχης ασφαλούς τεχνολογίας καθ' υπόδειξη της Υπηρεσίας Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων (Δ9).
- Τήρηση των βασικών μέτρων ασφάλειας που περιγράφονται στην Ενότητα 9 (ενημερωμένο λογισμικό, antivirus, ισχυροί κωδικοί).
- Απαγόρευση πρόσβασης στα δεδομένα ειδικών κατηγοριών (άρθρο 9 ΓΚΠΔ) μέσω προσωπικής συσκευής, καθώς και απαγόρευση πρόσβασης του Υπουργείου σε τμήματα της συσκευής που προορίζονται αποκλειστικά για προσωπική χρήση.
- Απαγόρευση εγγραφής ή αποθήκευσης ήχου ή εικόνας τηλεδιασκέψεων σε προσωπική συσκευή.
- Δυνατότητα αποκλεισμού πρόσβασης σε ηλεκτρονικά συστήματα που χαρακτηρίζονται ως κρίσιμα ή ευαίσθητα, όταν χρησιμοποιείται προσωπικός εξοπλισμός.
- Πρόβλεψη διαδικασίας αποκατάστασης σε περίπτωση απώλειας ή βλάβης της προσωπικής συσκευής, συμπεριλαμβανομένης της δυνατότητας απομακρυσμένης διαγραφής των υπηρεσιακών δεδομένων.

*Το Υπουργείο παραμένει υπεύθυνο για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία μέσω προσωπικού εξοπλισμού, ακόμη και όταν δεν έχει φυσικό έλεγχο ή ιδιοκτησία επί της συσκευής.*

## 11. Τηλεδιασκέψεις

Το Υπουργείο χρησιμοποιεί για τις τηλεδιασκέψεις πλατφόρμες που υποστηρίζουν κατάλληλες υπηρεσίες ασφαλείας, όπως κρυπτογράφηση και προστασία του συνδέσμου (hyperlink) της προγραμματισμένης τηλεδιάσκεψης. Ο σύνδεσμος τηλεδιάσκεψης τηρείται εμπιστευτικός και δεν κοινοποιείται σε τρίτους ούτε δημοσιοποιείται.

- Η ενεργοποίηση της κάμερας κατά τη διάρκεια τηλεδιάσκεψης δεν είναι υποχρεωτική, εκτός εάν αυτό επιβάλλεται από συγκεκριμένες λειτουργικές ανάγκες της υπηρεσίας και της φύσης της συνάντησης.
- Απαγορεύεται η χρήση της κάμερας του Σταθμού Τηλεργασίας για τον έλεγχο της απόδοσης του τηλεργαζομένου.
- Όταν η ενεργοποίηση της κάμερας κρίνεται απαραίτητη, συνιστάται η χρήση δυνατοτήτων απόκρυψης φόντου (θόλωση ή εικονικό φόντο), ώστε να αποφεύγεται η αποκάλυψη στοιχείων του ιδιωτικού χώρου.
- Καταγραφή τηλεδιάσκεψης πραγματοποιείται μόνο κατ' εξαίρεση, όταν αυτό απαιτείται για την τήρηση πρακτικών λόγω πιθανής παραγωγής έννομων συνεπειών, ενεργοποιείται αποκλειστικά από ειδικά εξουσιοδοτημένο χρήστη, προϋποθέτει προηγούμενη ενημέρωση όλων των συμμετεχόντων και πραγματοποιείται, κατά κανόνα, σε κρυπτογραφημένη μορφή.

- Οι συμμετέχοντες ενημερώνονται ότι η χωρίς εξουσιοδότηση καταγραφή, αποθήκευση ή διάδοση δεδομένων ήχου ή εικόνας τηλεδιάσκεψης ενδέχεται να στοιχειοθετεί αξιόποινη πράξη.

## 12. Δικαίωμα Αποσύνδεσης

---

Ο τηλεργαζόμενος έχει δικαίωμα, μετά το πέρας του ωραρίου εργασίας του και κατά τη διάρκεια των νόμιμων αδειών του, να αποσυνδέεται πλήρως από τα ψηφιακά μέσα επικοινωνίας και εργασίας (λογισμικά, πλατφόρμες, ηλεκτρονικό ταχυδρομείο, τηλεφωνικές κλήσεις υπηρεσιακού χαρακτήρα), χωρίς υποχρέωση ανταπόκρισης και χωρίς καμία δυσμενή συνέπεια σε βάρος του, σύμφωνα με το άρθρο 18 του ν. 4807/2021.

Το Υπουργείο δεν αναμένει, ούτε αξιολογεί αρνητικά, τη μη ανταπόκριση του τηλεργαζομένου σε επικοινωνίες εκτός του συμφωνηθέντος ωραρίου εργασίας.

## 13. Διαχείριση Οικιακού Χώρου και Τρίτων Προσώπων

---

- Ο Σταθμός Τηλεργασίας που παρέχεται από το Υπουργείο δεν χρησιμοποιείται από τρίτα πρόσωπα (μέλη οικογένειας, επισκέπτες κ.λπ.).
- Ο τηλεργαζόμενος οφείλει να διασφαλίζει ότι τρίτα πρόσωπα δεν αποκτούν πρόσβαση σε υπηρεσιακά αρχεία, έγγραφα ή συστήματα, στο πλαίσιο της υποχρέωσης εχεμύθειας που τον δεσμεύει.
- Η οθόνη του Σταθμού Τηλεργασίας τοποθετείται σε σημείο που περιορίζει τη θέαση του περιεχομένου της από τρίτους.
- Εφόσον χρησιμοποιείται κοινός Η/Υ με άλλα μέλη του νοικοκυριού, η πρόσβαση αυτών πραγματοποιείται αποκλειστικά μέσω λογαριασμού απλού χρήστη, χωρίς δικαιώματα διαχειριστή.

## 14. Διαχείριση, Εκτύπωση και Καταστροφή Εγγράφων

---

Η εκτύπωση υπηρεσιακών εγγράφων στην οικία του τηλεργαζομένου ή σε άλλο χώρο πραγματοποιείται μόνο εφόσον είναι απολύτως αναγκαία για την εκτέλεση της τηλεργασίας, με ευθύνη του τηλεργαζομένου, ώστε να αποκλείεται η πρόσβαση τρίτων μη δικαιούμενων προσώπων.

Έγγραφα που δεν είναι πλέον απαραίτητα καταστρέφονται με ασφαλή τρόπο (χρήση καταστροφέα εγγράφων ή, ελλείψει αυτού, τεμαχισμό σε μικρά κομμάτια πριν από την απόρριψή τους) και δεν απορρίπτονται ακέραια σε κάδους οικιακών απορριμμάτων.

Κάθε υπηρεσιακή αλληλογραφία διακινείται αποκλειστικά μέσω του επίσημου υπηρεσιακού λογαριασμού ηλεκτρονικού ταχυδρομείου και όχι μέσω προσωπικού λογαριασμού του τηλεργαζομένου. Αποφεύγεται η προώθηση υπηρεσιακών μηνυμάτων σε προσωπική διεύθυνση ηλεκτρονικού ταχυδρομείου.

## 15. Χρόνος Διατήρησης Δεδομένων

---

- Τα εξωτερικά στοιχεία ηλεκτρονικής επικοινωνίας (ονοματεπώνυμο συμμετέχοντος, ώρα και ημέρα σύνδεσης, διεύθυνση IP) διατηρούνται για διάστημα δώδεκα (12) μηνών, για τον σκοπό της ορθής εφαρμογής της τηλεργασίας και της απόδειξης συμμετοχής σε τηλεδιασκέψεις.
- Δεδομένα που περιλαμβάνονται σε αρχεία τα οποία έχουν μεταφορτωθεί σε προσωπικές συσκευές τηλεργαζομένων διαγράφονται αμέσως μόλις ολοκληρωθεί ο σκοπός της επεξεργασίας τους, με ευθύνη του τηλεργαζομένου, ο οποίος βεβαιώνει εγγράφως τη διαγραφή στο Υπουργείο (Παράρτημα 2).
- Τυχόν μεταδεδομένα τηρούνται για χρονικό διάστημα δύο (2) ετών.

- Κάθε άλλο δεδομένο τηρείται για το χρονικό διάστημα που ορίζουν οι διατάξεις που διέπουν τη λειτουργία του Υπουργείου και η νομοθεσία περί τήρησης αρχείων του δημοσίου τομέα.
- Καταγραφές τηλεδιασκέψεων, όπου κατ' εξαίρεση επιτρέπονται, τηρούνται μόνο για όσο διάστημα υφίσταται σχετική υποχρέωση τήρησης πρακτικών ή έννομο συμφέρον, σύμφωνα με την Ενότητα 11.

## 16. Υποχρεώσεις Τηλεργαζομένου

---

- Τηρεί απαρέγκλιτα την παρούσα Πολιτική και κάθε επιμέρους οδηγία ή διαδικασία ασφάλειας που του κοινοποιεί το Υπουργείο.
- Δεσμεύεται από την υποχρέωση εχεμύθειας του άρθρου 26 του ν. 3528/2007 για κάθε γεγονός ή πληροφορία που περιέχεται σε γνώση του κατά ή επ' ευκαιρία της άσκησης των καθηκόντων του.
- Χρησιμοποιεί τον Σταθμό Τηλεργασίας αποκλειστικά για την άσκηση των υπηρεσιακών του καθηκόντων.
- Ενημερώνει αμελλητί την Υπηρεσία Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων (Δ9) και τη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών για κάθε περιστατικό ή υπόνοια παραβίασης ασφάλειας δεδομένων, απώλειας ή κλοπής εξοπλισμού.
- Διασφαλίζει ότι ο χώρος παροχής της τηλεργασίας πληροί τις ελάχιστες προϋποθέσεις ασφάλειας και εργονομίας.
- Δεν εγκαθιστά μη εξουσιοδοτημένο λογισμικό στον Σταθμό Τηλεργασίας και δεν τροποποιεί τις ρυθμίσεις ασφαλείας που έχουν διαμορφωθεί από την υπηρεσία πληροφορικής.

Η μη τήρηση των ανωτέρω υποχρεώσεων εξετάζεται στο πλαίσιο του πειθαρχικού δικαίου, σύμφωνα με τα άρθρα 107 επ. του ν. 3528/2007.

## 17. Δικαιώματα Υποκειμένων των Δεδομένων

---

Κάθε τηλεργαζόμενος και κάθε φυσικό πρόσωπο του οποίου τα δεδομένα υφίστανται επεξεργασία στο πλαίσιο της τηλεργασίας διατηρεί ακέραια τα δικαιώματα που προβλέπονται στα άρθρα 12 έως 22 του ΓΚΠΔ και στα άρθρα 33 έως 35 του ν. 4624/2019, μεταξύ των οποίων το δικαίωμα πρόσβασης, διόρθωσης, διαγραφής, περιορισμού της επεξεργασίας και εναντίωσης.

Αιτήματα άσκησης δικαιωμάτων απαντώνται από το Υπουργείο χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, εντός μηνός από την παραλαβή τους, με δυνατότητα παράτασης κατά δύο ακόμη μήνες σε περιπτώσεις πολυπλοκότητας, σύμφωνα με το άρθρο 12 ΓΚΠΔ. Σε περίπτωση άρνησης ή μη ανταπόκρισης, το υποκείμενο των δεδομένων δύναται να προσφύγει στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Το Υπουργείο ενημερώνει τηλεργαζόμενους και τρίτους για τη δυνατότητα άσκησης των ανωτέρω δικαιωμάτων με κάθε πρόσφορο μέσο, ιδίως με ανάρτηση σχετικών πληροφοριών στην ιστοσελίδα του.

## 18. Διαχείριση Περιστατικών Παραβίασης Ασφάλειας Δεδομένων

---

Κάθε τηλεργαζόμενος που αντιλαμβάνεται ή έχει υπόνοια περιστατικού παραβίασης ασφάλειας δεδομένων προσωπικού χαρακτήρα (π.χ. απώλεια, κλοπή ή μόλυνση συσκευής, μη εξουσιοδοτημένη πρόσβαση, αποστολή δεδομένων σε λάθος παραλήπτη) υποχρεούται να ενημερώσει άμεσα τη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών ή/και τον Υπεύθυνο Προστασίας Δεδομένων του Υπουργείου.

Σε περίπτωση ύποπτης μόλυνσης του Σταθμού Τηλεργασίας με κακόβουλο λογισμικό, ο τηλεργαζόμενος αποσυνδέει τη συσκευή από το δίκτυο και δεν επιχειρεί μόνος του διορθωτικές ενέργειες, αναμένοντας οδηγίες από την αρμόδια υπηρεσία.

Το Υπουργείο, μέσω του Υπευθύνου Προστασίας Δεδομένων, αξιολογεί κάθε περιστατικό και, όπου απαιτείται, προβαίνει σε κοινοποίηση προς την ΑΠΔΠΧ εντός 72 ωρών από τη γνώση του περιστατικού, σύμφωνα με το άρθρο 33 ΓΚΠΔ, καθώς και σε ενημέρωση των επηρεαζόμενων υποκειμένων όπου απαιτείται κατά το άρθρο 34 ΓΚΠΔ.

## 19. Έλεγχος Ωραρίου και Απόδοσης

---

Το Υπουργείο δύναται να ελέγχει την τήρηση του συμφωνηθέντος ωραρίου εργασίας και την εκτέλεση της τηλεργασίας, με τη χρήση κατάλληλων μέσων και μεθόδων αυθεντικοποίησης, τηρουμένων των αρχών της αναλογικότητας και της ελαχιστοποίησης των δεδομένων.

Δεν επιτρέπεται η συστηματική, διαρκής και γενικευμένη παρακολούθηση του τηλεργαζομένου, ούτε η λήψη αποφάσεων που αφορούν την απόδοση ή τη συμπεριφορά του αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας δεδομένων, συμπεριλαμβανομένης της κατάρτισης προφίλ, κατά παράβαση του άρθρου 22 ΓΚΠΔ.

Απαγορεύεται η υποχρεωτική συνεχής λειτουργία κάμερας, η χρήση λογισμικού καταγραφής πληκτρολόγησης (keylogger) ή αντίστοιχων εργαλείων παρακολούθησης με αποκλειστικό σκοπό τον έλεγχο απόδοσης του τηλεργαζομένου.

## 20. Διαβιβάσεις Δεδομένων σε Τρίτες Χώρες

---

Εφόσον, κατά την παροχή τηλεργασίας ή τη διενέργεια τηλεδιασκέψεων, απαιτείται διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός Ευρωπαϊκού Οικονομικού Χώρου, το Υπουργείο επιλέγει εφαρμογές και πλατφόρμες που συμμορφώνονται με τις διατάξεις του Κεφαλαίου V του ΓΚΠΔ (άρθρα 44 επ.), με χρήση εγκεκριμένων από την Ευρωπαϊκή Επιτροπή τυποποιημένων συμβατικών ρητρών ή άλλων κατάλληλων εγγυήσεων.

## 21. Μη Συμμόρφωση και Κυρώσεις

---

Η μη τήρηση της παρούσας Πολιτικής από τηλεργαζόμενο δύναται να συνιστά πειθαρχικό παράπτωμα, να επισύρει την ανάκληση της έγκρισης τηλεργασίας και, κατά περίπτωση, να στοιχειοθετεί αστική ή ποινική ευθύνη, σύμφωνα με τις κείμενες διατάξεις, ιδίως εφόσον προκύψει παραβίαση δεδομένων προσωπικού χαρακτήρα ή διαρροή διαβαμισμένης ή εμπιστευτικής πληροφορίας.

## 22. Αναθεώρηση της Πολιτικής

---

Η παρούσα Πολιτική επανεξετάζεται τουλάχιστον σε ετήσια βάση από τη Διεύθυνση Πολιτικής Ασφάλειας Υποδομών και Μεταφορών, σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων, καθώς και εκτάκτως, όποτε μεταβάλλεται το νομικό πλαίσιο, οι τεχνολογικές συνθήκες ή προκύπτουν σχετικά περιστατικά ασφάλειας που καθιστούν αναγκαία την επικαιροποίησή της.

## 23. Έναρξη Ισχύος

---

Η παρούσα Πολιτική ισχύει από την ημερομηνία έγκρισής της από τον Υπηρεσιακό Γραμματέα του Υπουργείου και κοινοποιείται σε κάθε τηλεργαζόμενο πριν από την έναρξη της τηλεργασίας, σύμφωνα με το άρθρο 5 του ΠΔ 13/2025. Κάθε τηλεργαζόμενος οφείλει να λάβει γνώση του περιεχομένου της και να βεβαιώσει την αποδοχή του.

## **ΠΑΡΑΡΤΗΜΑ 1**

Μια Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ / DPIA), σύμφωνα με το άρθρο 35 ΓΚΠΔ, στο πλαίσιο της τηλεργασίας, θα πρέπει να περιλαμβάνει τα εξής βασικά στοιχεία:

### **1. Συστηματική περιγραφή της επεξεργασίας**

- Σκοπός/σκοποί επεξεργασίας (π.χ. οργάνωση τηλεργασίας, έλεγχος ωραρίου, τηλεδιασκέψεις, απομακρυσμένη πρόσβαση σε συστήματα)
- Κατηγορίες δεδομένων που υποβάλλονται σε επεξεργασία (ταυτότητας, επικοινωνίας, τεχνικά/IP, ήχου-εικόνας από τηλεδιασκέψεις κ.λπ.)
- Κατηγορίες υποκειμένων (τηλεργαζόμενοι, λοιποί υπάλληλοι, τρίτα πρόσωπα/πολίτες)
- Αποδέκτες δεδομένων, τυχόν διαβιβάσεις (και ειδικά αν γίνονται εκτός ΕΟΧ)
- Χρόνος τήρησης δεδομένων
- Τεχνική περιγραφή ροής δεδομένων (Σταθμός Τηλεργασίας, VPN, cloud υπηρεσίες, πλατφόρμες τηλεδιάσκεψης)

### **2. Αξιολόγηση αναγκαιότητας και αναλογικότητας**

- Αιτιολόγηση γιατί η επεξεργασία (και κάθε συγκεκριμένο μέτρο, π.χ. σύστημα παρακολούθησης χρόνου εργασίας) είναι αναγκαία για τον σκοπό
- Εξέταση εναλλακτικών, ηπιότερων μέσων
- Αρχή ελαχιστοποίησης δεδομένων ανά περίπτωση χρήσης

### **3. Αξιολόγηση κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων** Ειδικά για την τηλεργασία, τυπικοί κίνδυνοι που πρέπει να εξεταστούν:

- Μη εξουσιοδοτημένη πρόσβαση λόγω μη ασφαλούς οικιακού δικτύου ή χρήσης BYOD
- Απώλεια/κλοπή συσκευής
- Κακόβουλο λογισμικό, phishing
- Πρόσβαση τρίτων (μέλη οικογένειας) σε υπηρεσιακά δεδομένα
- Υπερβολική παρακολούθηση/κατάρτιση προφίλ τηλεργαζομένου (π.χ. keylogger, συνεχής κάμερα)
- Διαρροή μέσω μη κρυπτογραφημένων τηλεδιασκέψεων ή εκτυπώσεων
- Ανεπαρκής διαγραφή δεδομένων από προσωπικές συσκευές

Για κάθε κίνδυνο: πιθανότητα εμφάνισης και σοβαρότητα αντικτύπου.

### **4. Μέτρα αντιμετώπισης των κινδύνων**

- Τεχνικά μέτρα (κρυπτογράφηση, VPN, 2FA, antivirus, sandboxing σε BYOD, απομακρυσμένη διαγραφή)
- Οργανωτικά μέτρα (πολιτικές, εκπαίδευση, διαδικασίες έγκρισης τηλεργασίας/BYOD, διαδικασία διαχείρισης περιστατικών)
- Αποδεικτικά στοιχεία ότι τα μέτρα μειώνουν τον υπολειπόμενο κίνδυνο σε αποδεκτό επίπεδο

### **5. Διαβούλευση**

- Γνώμη του Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ) του Φορέα
- Κατά περίπτωση, διαβούλευση με τους εκπροσώπους των εργαζομένων
- Αν παραμένει υψηλός υπολειπόμενος κίνδυνος, προηγούμενη διαβούλευση με την ΑΠΔΠΧ (άρθρο 36 ΓΚΠΔ)

### **6. Ειδικά στοιχεία που απαιτεί το ΠΔ 13/2025**

- Τεκμηρίωση ότι η χρήση συστήματος παρακολούθησης χρόνου εργασίας δεν επιφέρει υψηλό κίνδυνο (άρθρο 3 παρ. 4)
- Χωριστή ΕΑΠΔ αν εγκρίνεται τηλεργασία εκτός ΕΟΧ (άρθρο 9 παρ. 4)
- Πρέπει να διενεργείται **πριν** την έναρξη κάθε προγράμματος τηλεργασίας (άρθρο 3 παρ. 3 ΠΔ 13/2025, άρθρο 6 παρ. 9 ν. 4807/2021)

#### **7. Συμπέρασμα και έγκριση**

- Τελική κρίση αν ο υπολειπόμενος κίνδυνος είναι αποδεκτός
- Ημερομηνία, υπεύθυνος σύνταξης, έγκριση από αρμόδιο όργανο, πρόβλεψη περιοδικής επανεξέτασης

## ΥΠΟΥΡΓΕΙΟ ΥΠΟΔΟΜΩΝ ΚΑΙ ΜΕΤΑΦΟΡΩΝ

Πολιτική Τηλεργασίας — Παράρτημα 2

### ΕΝΤΥΠΟ ΒΕΒΑΙΩΣΗΣ ΔΙΑΓΡΑΦΗΣ ΔΕΔΟΜΕΝΩΝ

που έχουν μεταφορτωθεί σε προσωπική συσκευή τηλεργαζομένου (άρθρο 15 της Πολιτικής Τηλεργασίας)

Σύμφωνα με την Ενότητα 15 της Πολιτικής Τηλεργασίας του Υπουργείου Υποδομών και Μεταφορών, τα δεδομένα που περιλαμβάνονται σε αρχεία τα οποία έχουν μεταφορτωθεί σε προσωπικές συσκευές τηλεργαζομένων διαγράφονται αμέσως μόλις ολοκληρωθεί ο σκοπός της επεξεργασίας τους, με ευθύνη του τηλεργαζομένου, ο οποίος βεβαιώνει εγγράφως τη διαγραφή στο Υπουργείο. Το παρόν έντυπο συμπληρώνεται και υπογράφεται από τον τηλεργαζόμενο για τον σκοπό αυτό.

#### Α. Στοιχεία Τηλεργαζομένου

Όνοματεπώνυμο:

Θέση / Κλάδος:

Διεύθυνση / Τμήμα Υπηρεσίας:

Αριθμός Απόφασης Έγκρισης  
Τηλεργασίας:

#### Β. Στοιχεία Προσωπικής Συσκευής

Τύπος συσκευής (H/Y, tablet, κ.λπ.):

Μοντέλο / Αναγνωριστικό συσκευής:

#### Γ. Στοιχεία Διαγραφής Δεδομένων

Περιγραφή / κατηγορία δεδομένων που  
διαγράφηκαν:

Σκοπός επεξεργασίας για τον οποίο  
είχαν μεταφορτωθεί:

Ημερομηνία ολοκλήρωσης του σκοπού  
επεξεργασίας:

Ημερομηνία διαγραφής δεδομένων:

Μέθοδος διαγραφής:

#### Δ. Δήλωση Τηλεργαζομένου

Με το παρόν βεβαιώνω υπεύθυνα ότι τα ανωτέρω δεδομένα, τα οποία είχαν μεταφορτωθεί στην προσωπική μου συσκευή στο πλαίσιο παροχής τηλεργασίας, έχουν διαγραφεί πλήρως και οριστικά, άμεσα μετά την ολοκλήρωση του σκοπού για τον οποίο είχαν μεταφορτωθεί, σύμφωνα με την Ενότητα 15 της Πολιτικής Τηλεργασίας του Υπουργείου Υποδομών και Μεταφορών και το άρθρο 15 του ν. 4807/2021.

Τόπος: .....

Ημερομηνία: .....

Ο/Η Τηλεργαζόμενος/-η

(υπογραφή)

Το παρόν έντυπο παραλαμβάνεται από την Υπηρεσία Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων (Δ9) ή/και την αρμόδια Διεύθυνση, και τηρείται στον σχετικό φάκελο τηλεργασίας του υπαλλήλου.