Ένωση Πληροφορικών Ελλάδας
Τ.Θ. 13801
ΤΚ 10310, Αθήνα
http://www.epe.org.gr
e-mail: info@epe.org.gr
Τηλέφωνο/SMS: (+30) 210 5699408

Δελτιο Τυπου

Παρατηρήσεις στο Σχέδιο Νόμου "Θεσμικό πλαίσιο τηλεργασίας, διατάξεις για το ανθρώπινο δυναμικό του δημοσίου τομέα και άλλες ρυθμίσεις του Υπουργείου Εσωτερικών"

Αθήνα, 06-06-2021

Η εφαρμογή της τηλε-εργασίας στο δημόσιο τομέα συνδέεται άμεσα με την ψηφιοποίηση των παρεχόμενων υπηρεσιών με διαδικασίες που εγγυώνται την ασφάλεια των συστημάτων και την προστασία των προσωπικών δεδομένων των πολιτών και προϋποθέτει την ενίσχυση του δημόσιου τομέα με εξειδικευμένο προσωπικό (Πληροφορικούς) που θα υλοποιήσει και θα υποστηρίζει τις σχετικές υπηρεσίες και τους χρήστες των υπηρεσιών αυτών. Απαιτεί διαρκή παρακολούθηση και αναβάθμιση των συστημάτων και των διαδικασιών, ώστε να ανταποκρίνονται στις προδιαγραφές ασφάλειας και προστασίας προσωπικών και κρατικών δεδομένων. Κανένα πληροφοριακό σύστημα δεν μπορεί να είναι ασφαλές χωρίς διαρκή εκπαίδευση των χρηστών στην ορθή χρήση του και την εφαρμογή των σχετικών διαδικασιών και πολιτικών ασφαλείας.

Η τηλε-εργασία δεν μπορεί να είναι αυτοσκοπός. Οφείλει να υπηρετεί το δημόσιο συμφέρον, να μην υποβαθμίζει τις υπηρεσίες που παρέχονται στους πολίτες και να μην εισάγει απειλές για την ασφάλεια των πληροφοριακών συστημάτων και την προστασία των προσωπικών δεδομένων των πολιτών. Με αυτά τα κριτήρια θα πρέπει να αξιολογηθούν οι λειτουργίες των δημοσίων φορέων που θα επιτρέπεται σε περιόδους ομαλής λειτουργίας να εκτελούνται εκτός των εγκαταστάσεων των φορέων. Ιδίως κατά τη δοκιμαστική περίοδο που διανύουμε όπου: δεν έχουν δοκιμαστεί εκτενώς τα νέα συστήματα πληροφορικής, δεν έχουν καταρτιστεί οι απαιτούμενες πολιτικές ασφαλείας και κανονισμοί από τους δημόσιους φορείς, δεν υπάρχει επαρκής τεχνογνωσία και εκπαίδευση του προσωπικού στην χρήση των πληροφοριακών συστημάτων και στην εφαρμογή των απαιτούμενων κανονισμών και διαδικασιών, η γενικευμένη και άκριτη εφαρμογή της τηλε-εργασίας μπορεί να οδηγήσει σε μη αναστρέψιμες βλάβες για τους πολίτες και τους δημόσιους φορείς (διαρροή κρατικών και προσωπικών δεδομένων, υποκλοπή ταυτότητας, παραβίαση εμπορικού απορρήτου σε σχετικούς διαγωνισμούς, κλπ).

Αξιοποίηση της τηλε-εργασίας στην περιφερειακή ανάπτυξη (Στόχοι της αξιολογούμενης ρύθμισης)

Η τηλε-εργασία θα πρέπει να εντάσσεται στην στρατηγική ανάπτυξης της χώρας και να υπηρετεί σαφείς στόχους. Από τους στόχους εφαρμογής της τηλε-εργασίας (σελίδες 22-23 του σχεδίου νόμου) απουσιάζει η αξιοποίηση των δυνατοτήτων που παρέχει η τηλε-εργασία για ενίσχυση των παραμεθόριων, νησιωτικών, αγροτικών και αραιοκατοικημένων περιοχών με μέτρα διευκόλυνσης της παραμονής ή και της εγκατάστασης εργαζομένων του δημοσίου που θα έχουν τη δυνατότητα να εργάζονται από την κατοικία τους ή από σταθμούς/κέντρα τηλε-εργασίας στις περιοχές αυτές. Σε Ευρωπαϊκό επίπεδο προτείνεται η αξιοποίηση της τηλε-εργασίας των δημοσίων υπαλλήλων ως μέτρο ενίσχυσης της ανάπτυξης των περιοχών αυτών και μάλιστα περιλαμβάνεται στις μελέτες των οργάνων της Ε.Ε. (που αναφέρονται και στις σελ. 22-23 του παρόντος νομοσχεδίου) και ειδικότερα στην σελ 12 του Κέντρου Εμπειρογνωμοσύνης για τη Χρηστή Διακυβέρνηση του Συμβουλίου της Ευρώπης με τίτλο “Toolkit on Teleworking in Public Administrations”. Ο στόχος αυτός εναρμονίζεται με άρθρο 101, παρ. 4 του Συντάγματος που προβλέπει ότι “*ο κοινός νομοθέτης και η Διοίκηση, όταν δρουν κανονιστικά υποχρεούνται να λαμβάνουν υπόψη τις ιδιαίτερες συνθήκες των νησιωτικών και ορεινών περιοχών, μεριμνώντας για την ανάπτυξη τους*”. Έτσι στα κριτήρια επιλογής των υποψηφίων για τηλε-εργασία θα πρέπει να συμπεριληφθεί η μόνιμη κατοικία ή η μετεγκατάσταση σε αγροτικές, νησιωτικές και απομονωμένες περιοχές. Μακροπρόθεσμα η δυνατότητα αυτή θα μπορούσε να αξιοποιηθεί και για την άρση του αποκλεισμού των κατοίκων της περιφέρειας από την εργασία σε πολλούς οργανισμούς δημόσιας διοίκησης που έχουν έδρα την Αθήνα ή τις πρωτεύουσες των περιφερειών.

Επιλογή του τόπου παροχής της τηλε-εργασίας (Άρθρο 11)

Σύμφωνα με άρθρο 11 ο εργαζόμενος οφείλει να διασφαλίσει ότι ο επιλεγόμενος χώρος πληροί τις ελάχιστες απαιτούμενες προδιαγραφές υγιεινής και ασφάλειας. Επισημαίνουμε ότι η υγιεινή και ασφάλεια είναι ευθύνη του εργοδότη (EUR-Lex. Teleworking, 2005) που πρέπει να παρέχει όλες τις απαιτούμενες οδηγίες και εκπαίδευση στον εργαζόμενο, αν εργάζεται στην κατοικία του, για τη διαμόρφωση του χώρου, τη διάταξη του εξοπλισμού, την εργονομία, την ασφάλεια, κλπ.

Η επιλογή του τόπου της τηλε-εργασίας επηρεάζει όχι μόνο την υγιεινή και ασφάλεια του εργαζομένου και την απρόσκοπτη εκτέλεση της εργασίας (άρθρο 11), αλλά και την ασφάλεια των κρατικών δεδομένων και των προσωπικών δεδομένων των πολιτών. Όμως το άρθρο 11 αφήνει στη διακριτική ευχέρεια των εκάστοτε προϊσταμένων και διευθυντών να επιτρέψουν την παροχή τηλε-εργασίας όχι μόνο από την κατοικία του εργαζόμενου αλλά και από οποιοδήποτε άλλο χώρο εντός των συνόρων των κρατών μελών της Ευρωπαϊκής Ένωσης, χωρίς να προσδιορίζεται κανένας

κανόνας ή προδιαγραφή ασφαλείας των δεδομένων, ή υγιεινής εργονομίας και ασφάλειας του εργαζομένου.

Απαιτείται ορισμός των προδιαγραφών του τόπου τηλε-εργασίας στο άρθρο 11 και ρητή πρόβλεψη ότι στο χώρο παροχής της τηλε-εργασίας πρέπει διασφαλίζεται η φυσική και λογική προστασία των προσωπικών δεδομένων των πολιτών και των κρατικών δεδομένων από πρόσβαση τρίτων, μέσω κατάλληλων μηχανισμών υποχρεωτικού χαρακτήρα. Επιπλέον χρειάζεται να διευκρινιστεί αν επιτρέπεται η μεταφορά/χρήση/παραγωγή φυσικού αρχείου εκτός των εγκαταστάσεων του δημόσιου οργανισμού και να προσδιοριστούν τα μέτρα που λαμβάνονται για την προστασία του (ασφαλή φύλαξη, καταστροφή).

Σταθμός Τηλεργασίας (Άρθρο 12)

Σύμφωνα και με τις ευρωπαϊκές οδηγίες ο εξοπλισμός τηλε-εργασίας παρέχεται από τον εργοδότη (EUR-Lex. Teleworking, 2005). Η διάταξη του άρθρου 12 ότι "*εφόσον ο φορέας δεν έχει τη δυνατότητα να παράσχει Σταθμό Τηλεργασία ο υπάλληλος δύναται, εφόσον το επιθυμεί, να κάνει χρήση του προσωπικού του τεχνολογικού εξοπλισμού*" πρέπει να καταργηθεί διότι επιπλέον θέτει σε κίνδυνο την ασφάλεια των δημόσιων πληροφοριακών συστημάτων και την προστασία των προσωπικών δεδομένων του εργαζομένου και της οικογένειας του, συμπεριλαμβανομένων και των παιδιών που πρέπει να έχουν αυξημένη προστασία.

Θεσμοθέτηση διαφανών διαδικασιών και αντικειμενικών κριτηρίων (Άρθρο 13)

Για την ομαλή και αποτελεσματική εισαγωγή της τηλε-εργασίας στο δημόσιο τομέα πρέπει να θεσμοθετηθούν σαφή και αντικειμενικά κριτήρια όσον αφορά στον ορισμό των θέσεων εργασίας και στην επιλογή του προσωπικού. Όμως, με το άρθρο 13 δίδεται απόλυτη εξουσία στους εκάστοτε προϊσταμένους διευθύνσεων και τμημάτων να ορίζουν τις θέσεις που είναι επιλέξιμες για τηλε-εργασία χωρίς να ορίζονται σαφή κριτήρια και κανόνες.

Αποσύνδεση τηλε-εργαζόμενου (Άρθρο 18)

Με το άρθρο 18 προβλέπεται η αποσύνδεση του τηλε-εργαζόμενου από τα μέσα πληροφορικής και επικοινωνίας που χρησιμοποιεί για την εκτέλεση των καθηκόντων του. Χρειάζεται παρακολούθηση της εφαρμογής και λήψη πρόσθετων μέτρων ώστε να προστατευτεί το δικαίωμα των τηλε-εργαζόμενων στην αποσύνδεση καθώς η υπέρβαση του χρόνου εργασίας και η εργασία το Σαββατοκύριακο αναφέρεται διεθνώς ως μια από τις πιο συχνές αρνητικές επιπτώσεις της τηλε-εργασίας στους εργαζόμενους.

Πολιτικής Ασφαλείας

Όλοι οι δημόσιοι φορείς πρέπει να διαθέτουν Πολιτικής Ασφαλείας που να συμπεριλαμβάνει και τις ρυθμίσεις για την τηλεργασία και εναρμονίζεται με τη σχετική νομοθεσία και της συστάσεις των Ανεξάρτητων Αρχών (Αρχή Διασφάλισης Απορρήτου Επικοινωνιών, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα). Επίσης οφείλουν να εκπαιδεύουν το προσωπικό ώστε να είναι σε θέση να εφαρμόσει την πολιτική αυτή.

Προτεινόμενα τεχνικά μέτρα

Ο υπολογιστής να **παρέχεται στον Υπάλληλο από το Δημόσιο**, και να πληροί συγκεκριμένες προδιαγραφές λειτουργίας και ασφαλείας, μεταξύ των οποίων τις κάτωθι:

Ο υπολογιστής να έχει **κρυπτογράφηση σκληρού δίσκου**, μέσω τεχνολογίας ισχυρών κρυπτογραφικών αλγορίθμων και πρωτοκόλλων, τύπου **bitlocker** ή άλλης αντίστοιχης, ώστε σε περίπτωση κλοπής, διάρρηξης στο σπίτι του Υπαλλήλου, ή απώλειας, να μην μπορούν να ανακτηθούν οι πληροφορίες που περιέχει.

Η χρήση του υπολογιστή να μπορεί να γίνει μόνο μέσω διαδικασίας **2 way authentication (password, και pin με sms στο κινητό)** κατ' ελαχιστο, ενώ σε εμπιστευτικές θέσεις Υπαλλήλων να απαιτείται χρήση **3 way authentication (αναγνώστη βιομετρικού χαρακτηριστικού** στον υπολογιστή, όπως δακτυλικού αποτυπώματος, επιπλέον των ανωτέρω).

Να υπάρχει κεντρικά διαχειρίσιμη **πολιτική passwords**, η οποία να περιλαμβάνει κατ' ελάχιστο απαίτηση ορισμού strong password, απαίτηση περιοδικής αλλαγής του password, ασφαλή διαδικασία reset password, λήψη του αρχικού password και των reset passwords με sms στο κινητό τηλέφωνο του Υπαλλήλου, κλπ.

Να μην υπάρχουν ευαίσθητα δεδομένα τοπικά αποθηκευμένα στον υπολογιστή. Όλα τα δεδομένα (αρχεία, emails, κλπ) **να αποθηκεύονται στο ασφαλές κυβερνητικό cloud**.

Να γίνεται χρήση **Virtual desktop**, ώστε να μην χρειάζεται εγκατάσταση, συντήρηση και αναβάθμιση των εφαρμογών τοπικά στον υπολογιστή, αλλά να μπορεί να διαμορφώνεται το περιβάλλον εργασίας του υπολογιστή μέσω κεντρικής διαχείρισης, να είναι τυποποιημένο ανάλογα με τις ανάγκες κάθε θέσης, να επαναφέρεται άμεσα σε περίπτωση αντικατάστασης του υπολογιστή, κλπ.

Όλες οι συνδέσεις μέσω δικτύου να πραγματοποιούνται μέσω **virtual private network (VPN)** με πλήρως καθορισμένη Πολιτική Ασφάλειας και σχετικά ψηφιακά πιστοποιητικά.

Ο υπολογιστής να έχει κεντρικά διαχειρίσιμη προστασία **firewall, antivirus και email security**.

Ο υπολογιστής να έχει κεντρικά διαχειρίσιμη **πολιτική backup** των δεδομένων του στο κυβερνητικό cloud.

Ο υπολογιστής να έχει κεντρικά διαχειρίσιμη **πολιτική αυτόματων ενημερώσεων** του λειτουργικού του συστήματος, των εφαρμογών του ασφαλείας (firewall, antivirus, κλπ), και των λοιπών τοπικών εφαρμογών του, με ενημερώσεις ασφάλειας, νέες εκδόσεις και αναβαθμίσεις.

Ο υπολογιστής να έχει κεντρικά διαχειρίσιμη πολιτική προστασίας κρίσιμων δεδομένων DLP (**Data Loss Prevention**), κρατικών και προσωπικών δεδομένων, ώστε να μην μπορεί ο Υπάλληλος να εξάγει δεδομένα από τον υπολογιστή, μέσω usb stick, δίσκων, email, messaging, upload στο internet, και άλλων μέσων, στο βαθμό που αυτό είναι καθορισμένο από την Πολιτική Ασφάλειας της εκάστοτε υπηρεσίας.

Ο υπολογιστής να έχει κεντρικά διαχειρίσιμη προστασία **web / content filtering**, ώστε να μην επιτρέπεται η χρήση επικίνδυνων ή μη απαραίτητων για την εργασία του Υπαλλήλου ιστοτόπων και υπηρεσιών (π.χ. social media, κλπ).

Ο υπολογιστής να είναι **φορητός** και να συνοδεύεται από πρόσθετη εξωτερική οθόνη, πληκτρολόγιο, ποντίκι για εργονομική εργασία, ώστε να διευκολύνει την τηλε-εργασία από άλλο εγκεκριμένο χώρο και όχι μόνο από το σπίτι του Υπαλλήλου, να μπορεί να αποθηκεύεται / κλειδώνεται σε ασφαλές μέρος, κλπ.

Ο υπολογιστής να είναι **ανθεκτικός** (προδιαγραφή IP55, κλπ) σε συνήθη μικροατυχήματα, όπως αν χυθούν πάνω του υγρά (π.χ. νερό ή καφές), στην σκόνη, σε μικροχτυπήματα και σε πτώσεις από γραφείο (ύψος ενός μέτρου), ώστε να μην μπορεί να πάθει βλάβη εύκολα κατά την χρήση του, με αποτέλεσμα να μην μπορεί να εργαστεί ο Υπάλληλος και να υποβάλλεται το Δημόσιο σε δαπάνες επισκευής ή αντικατάστασης.

Ο υπολογιστής να διαθέτει ενσωματωμένη **κάμερα και μικρόφωνο,** και να συνοδεύεται από headset ακουστικών και μικροφώνου, για να μπορούν να πραγματοποιούνται τηλεδιασκέψεις.

Ο υπολογιστής να διαθέτει **μηχανικά κουμπιά ή διακόπτες απενεργοποίησης της κάμερας και του μικροφώνου**, ώστε να μην ελέγχεται η απενεργοποίηση και η ενεργοποίησή τους μόνο από λογισμικό, αλλά να μπορεί ο Χρήστης να έχει τον πλήρη έλεγχο των συγκεκριμένων συσκευών.

Ο υπολογιστής να διαθέτει κεντρικά διαχειρίσιμη εφαρμογή **VoiP softphone**, ώστε να μεταφέρονται σε αυτόν οι υπηρεσιακές τηλεφωνικές κλήσεις του Υπαλλήλου, και αντίστοιχα ο Υπάλληλος να μπορεί να πραγματοποιεί τηλεφωνικές κλήσεις μέσω του υπολογιστή.

Για την επικοινωνία να γίνεται αξιοποίηση της Κρατικής υποδομής **ΣΥΖΕΥΞΙΣ**.

Ο υπολογιστής να συνοδεύεται από **mobile stick (5G/4G/3G modem)** ώστε να μπορεί να συνδεθεί και να εργαστεί ο Υπάλληλος σε περίπτωση που διακοπεί η σταθερή σύνδεση Internet, λόγω τεχνικών εργασιών, βλάβης, κλπ.

Αρχικά για μείωση του κόστους της τηλε-εργασίας, ο ανωτέρω εξοπλισμός τηλε-εργασίας μπορεί να παρέχεται στον υπάλληλο αποκλειστικά για το διάστημα τηλε-εργασίας του και κατόπιν να **μεταβιβάζεται** σε άλλον υπάλληλο που ξεκινά τηλεργασία.

Ύπαρξη συγκροτημένου και επαρκούς **Helpdesk** για την υποστήριξη των Υπαλλήλων σε περίπτωση δυσλειτουργίας, αποριών, κλπ.

Πέραν της ύπαρξης του hekpdesk, οι υπάλληλοι, θα πρέπει να **εκπαιδεύονται** στην χρήση του ανωτέρου εξοπλισμού, την τήρηση των απαιτούμενων μέτρων ασφαλείας για την διασφάλιση των κρατικών και προσωπικών δεδομένων, και την ορθή χρήση των εφαρμογών που τους αφορούν, και να έχουν στην διάθεσή τους αναλυτικές έγγραφες οδηγίες για τα ανωτέρω. Λόγω της φύσης της (κρατικά δεδομένα, διαβαθμισμένες πληροφορίες, κλπ), η εκπαίδευση αυτή πρέπει να γίνεται από κρατικούς Φορείς, όπως η Εθνική Σχολή Δημόσιας Διοίκησης, και όχι από ιδιωτικούς φορείς.

Για το ΔΣ της Ένωσης Πληροφορικών Ελλάδας

Η Πρόεδρος
Χαρά Ξανθάκη
proedros@epe.org.gr

Ο Γενικός Γραμματέας
Χάρης Γεωργίου
gen_grammateas@epe.org.gr

Ένωση Πληροφορικών Ελλάδας, Τ.Θ. 13801, Τ.Κ. 10310, Αθήνα
Email: info@epe.org.gr – Τηλέφωνο: (+30) 210 5699408

Σύνδεσμοι

Σχέδιο νόμου «Θεσμικό πλαίσιο τηλεργασίας, διατάξεις για το ανθρώπινο δυναμικό του δημοσίου τομέα και άλλες ρυθμίσεις του Υπουργείου Εσωτερικών»
https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=74c7e7bd-60b8-462f-8b9d-ad3a015becad

EUR-Lex. Teleworking.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ac10131

Council of Europe. Centre of Expertise for Good Governance. Toolkit on Teleworking in Public Administrations (2020).
https://rm.coe.int/tpa-toolkit-on-teleworking-in-public-administration/1680a11fc1

Eurofound and ILO (2017), Working anytime, anywhere. The effects on the world of work.
https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef1658en.pdf