Σύντομος Οδηγός Καλών Πρακτικών για Υπηρεσιακά Θέματα Προστασίας Προσωπικών Δεδομένων

Ο παρών Οδηγός Καλών Πρακτικών έχει σκοπό να ενισχύσει την κατανόηση του προσωπικού, των ερευνητών και των συνεργατών του Ιδρύματος σχετικά με τη σημασία της προστασίας των Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ ή προσωπικά δεδομένα) και να παρέχει πρακτικές συμβουλές και κατευθυντήριες οδηγίες για την ασφαλή διαχείρισή τους στον εργασιακό χώρο.

Οι πρακτικές και οι συμβουλές του Οδηγού έχουν συμβουλευτικό χαρακτήρα και στοχεύουν στη μείωση του κινδύνου παραβίασης ΔΠΧ, ιδίως στο ψηφιακό περιβάλλον. Δεν αποτελούν εξαντλητική ή δεσμευτική λίστα μέτρων ασφάλειας και δεν υποκαθιστούν τις επίσημες πολιτικές, διαδικασίες ή υποχρεώσεις που απορρέουν από το ισχύον νομικό και κανονιστικό πλαίσιο.

Ο Οδηγός αποσκοπεί στη στήριξη των εμπλεκομένων ως προς τη συμμόρφωση με το ισχύον πλαίσιο προστασίας δεδομένων και, όπου απαιτείται και επιτρέπεται από το ισχύον νομικό πλαίσιο, στη διαβίβαση δεδομένων εντός και εκτός των υπηρεσιακών δομών, σύμφωνα με τον εκάστοτε καθορισμένο σκοπό επεξεργασίας.

Οι ψηφιακοί κίνδυνοι εξελίσσονται συνεχώς. Γι’ αυτό είναι απαραίτητη η τακτική ενημέρωση, η ενίσχυση των γνώσεων και η αναθεώρηση των μέτρων που εφαρμόζονται. Η τεχνολογική ασφάλεια βασίζεται στη μείωση και διαχείριση κινδύνου και όχι σε απόλυτες εγγυήσεις, γεγονός που αναδεικνύει τη σημασία της υιοθέτησης και της συνεπούς εφαρμογής βέλτιστων πρακτικών ασφάλειας πληροφοριών.

Η εφαρμογή των κατευθυντήριων γραμμών του παρόντος Οδηγού δεν απαλλάσσει τα αρμόδια όργανα, τις υπηρεσίες ή τα φυσικά πρόσωπα που συμμετέχουν στην επεξεργασία προσωπικών δεδομένων από τις υποχρεώσεις και τις ευθύνες που απορρέουν από την κείμενη νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα, όπως αυτή εκάστοτε ισχύει.

Η ευθύνη για τη νόμιμη και ορθή επεξεργασία των δεδομένων προσωπικού χαρακτήρα καθορίζεται από το ισχύον κανονιστικό και νομοθετικό πλαίσιο και αφορά, ανάλογα με την περίπτωση, τον Υπεύθυνο Επεξεργασίας και, όπου υφίστανται, τους Εκτελούντες την Επεξεργασία.

Για τεχνικά ζητήματα που ενδέχεται να προκύπτουν κατά την εφαρμογή των προτεινόμενων πρακτικών, το προσωπικό και οι συνεργάτες μπορούν να απευθύνονται στο αρμόδιο τεχνικό προσωπικό του Ιδρύματος, το οποίο είναι υπεύθυνο για τη διαχείριση των πληροφοριακών υποδομών και τη διερεύνηση εναλλακτικών ή συμπληρωματικών λύσεων, εφόσον αυτό κριθεί αναγκαίο.

Ιανουάριος 2026

dpo@eap.gr

- Η επεξεργασία προσωπικών δεδομένων θα πρέπει να στηρίζεται σε κατάλληλη νομική βάση σύμφωνα με το άρθρο 6 του GDPR, όπως για την εκπλήρωση νομικής υποχρέωσης, την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον ή την άσκηση δημόσιας εξουσίας. Όταν δεν υπάρχει άλλη κατάλληλη νομική βάση, η επεξεργασία μπορεί να βασίζεται σε συγκατάθεση των υποκειμένων των δεδομένων.
- Η αποστολή, λήψη και αποθήκευση προσωπικών ή υπηρεσιακών δεδομένων συνιστάται να γίνεται μέσω επίσημων υπηρεσιακών καναλιών του Ιδρύματος, όπως το ιδρυματικό email ή άλλες πλατφόρμες που παρέχονται (π.χ. OneDrive ιδρυματικού λογαριασμού, κοινόχρηστοι φάκελοι υπηρεσίας), αποφεύγοντας προσωπικούς λογαριασμούς, κοινωνικά δίκτυα ή εφαρμογές τρίτων για διοικητικά έγγραφα υπαλλήλων. Η πρόσβαση στα αρχεία πρέπει να είναι περιορισμένη ανά χρήστη και, μετά την ολοκλήρωση του σκοπού, συνιστάται να αφαιρούνται τα δικαιώματα πρόσβασης και να διακόπτεται η σύνδεση.
- Συνιστάται να αποφεύγεται η αναγραφή προσωπικών δεδομένων στη γραμμή θέματος των ηλεκτρονικών μηνυμάτων και, όπου είναι δυνατόν, να περιορίζονται στο κύριο σώμα του email, ιδίως όταν πρόκειται για δεδομένα προσωπικού χαρακτήρα ειδικής κατηγορίας, καθώς αυτά ενδέχεται να παραμένουν αποθηκευμένα σε διακομιστές ηλεκτρονικής αλληλογραφίας.
- Ιδιαίτερη προσοχή συνιστάται κατά την αποστολή email σε διευθύνσεις εκτός του domain του Ιδρύματος, καθώς δεν είναι γνωστό το πλαίσιο διαχείρισης ή τα μέτρα ασφάλειας, αυξάνοντας τον κίνδυνο για τα προσωπικά δεδομένα. Σε αυτές τις περιπτώσεις, συνιστάται να μην αναγράφονται ονόματα ή άλλες πληροφορίες που ταυτοποιούν άμεσα το άτομο στη γραμμή θέματος. Αντίθετα, συνιστάται να αναφέρεται μόνο ο γενικός σκοπός ή τύπος του αρχείου, ενώ τα πραγματικά δεδομένα να περιλαμβάνονται σε ασφαλές, κρυπτογραφημένο ή προστατευμένο με ισχυρό κωδικό συνημμένο.
- Η αποστολή email συνιστάται να περιορίζεται σε παραλήπτες που σχετίζονται άμεσα με τον σκοπό της επεξεργασίας. Για την προστασία των διευθύνσεων και την εμπιστευτικότητα των δεδομένων, προτείνεται η χρήση του πεδίου BCC (κρυφή κοινοποίηση) όταν υπάρχουν περισσότεροι παραλήπτες. Συνιστάται οι δημόσιες ή υπηρεσιακές διευθύνσεις ηλεκτρονικού ταχυδρομείου να χρησιμοποιούνται για διακίνηση εντός των αρμοδιοτήτων της Υπηρεσίας.
- Συνιστάται η εφαρμογή της αρχής της ελαχιστοποίησης των δεδομένων, ώστε να διακινούνται μόνο τα προσωπικά δεδομένα που είναι απολύτως αναγκαία για κάθε θεμιτό και συγκεκριμένο σκοπό. Πριν από οποιαδήποτε διαβίβαση, συνιστάται να αξιολογείται ποια δεδομένα είναι ουσιαστικά απαραίτητα (π.χ. αν επαρκεί η αναφορά μόνο στον αριθμό μητρώου, δεν αποστέλλονται πρόσθετα στοιχεία) και να εξετάζεται προσεκτικά σε ποιους φορείς ή συναδέλφους είναι αναγκαία η κοινοποίηση, με σκοπό την αποφυγή περιττής ή μη εξουσιοδοτημένης πρόσβασης.
- Για αρχεία που περιέχουν προσωπικά δεδομένα, συνιστάται η χρήση κρυπτογράφησης ή προστασίας με ισχυρό κωδικό πρόσβασης. Για παράδειγμα, ένα έγγραφο Excel μπορεί να συμπιεστεί σε αρχείο zip/rar με μοναδικό κωδικό τουλάχιστον 10 χαρακτήρων, συνδυάζοντας κεφαλαία και πεζά γράμματα, αριθμούς και σύμβολα. Η γνωστοποίηση του κωδικού καλό είναι να γίνεται μέσω διαφορετικού καναλιού επικοινωνίας (π.χ. δεύτερο email, SMS ή κατά προτίμηση τηλεφωνικά).
- Συνιστάται η ανάρτηση ανακοινώσεων με τρόπο που να περιορίζει την ταυτοποίηση φυσικών προσώπων, ώστε να μειώνεται ο κίνδυνος ακούσιας ή μη εξουσιοδοτημένης αποκάλυψης προσωπικών δεδομένων, όπως, για

παράδειγμα, με τη χρήση μέρους του αριθμού μητρώου ή άλλου μοναδικού κωδικού (π.χ. αριθμού αίτησης) αντί της αναγραφής ονομάτων σε πίνακες αποτελεσμάτων.

- Συνιστάται η πρόσβαση σε πληροφοριακά συστήματα ή αρχεία που περιέχουν προσωπικά δεδομένα να περιορίζεται μόνο στο απολύτως αναγκαίο προσωπικό και στα δεδομένα που είναι απαραίτητα για την άσκηση των συγκεκριμένων εκπαιδευτικών ή θεσμικών αρμοδιοτήτων, ώστε να μειώνεται ο κίνδυνος ακούσιας ή μη εξουσιοδοτημένης πρόσβασης, όπως, για παράδειγμα, με την παροχή πρόσβασης στα μέλη ΔΕΠ μόνο στα απαραίτητα στοιχεία των φοιτητών που παρακολουθούν τα μαθήματά τους και μόνο στον βαθμό που απαιτείται για τον εκπαιδευτικό σκοπό και τις υποχρεώσεις τους, όπως αυτές απορρέουν από σχετικές αποφάσεις του Ιδρύματος**.**
- Συνιστάται η χρήση προσωπικών δεδομένων σε ερευνητικές δραστηριότητες να περιορίζεται στον απολύτως αναγκαίο βαθμό, ώστε να μειώνεται ο κίνδυνος ακούσιας ή μη εξουσιοδοτημένης αποκάλυψής τους. Για παράδειγμα, σε εργασίες φοιτητών ή έρευνες που περιλαμβάνουν συνεντεύξεις, συνιστάται οι συμμετέχοντες να ανωνυμοποιούνται κατά την παρουσίαση των αποτελεσμάτων ή την ανάρτηση του σχετικού υλικού.
- Για ασφαλέστερη διαχείριση έντυπων εγγράφων που περιέχουν προσωπικά δεδομένα, συνιστάται να αποφεύγεται η παραμονή τους εκτεθειμένων σε γραφεία, αίθουσες συναντήσεων ή άλλους κοινόχρηστους χώρους. Ειδικότερα, κατάλογοι ή έγγραφα με προσωπικά στοιχεία συνιστάται να μην αφήνονται σε φωτοτυπικά μηχανήματα ή άλλα κοινόχρηστα σημεία, όπου υπάρχει κίνδυνος μη εξουσιοδοτημένης πρόσβασης.
- Συνιστάται το άμεσο κλείδωμα της οθόνης ή η ελαχιστοποίηση των παραθύρων που εμφανίζουν προσωπικά δεδομένα όταν απομακρύνεται κάποιος από τον υπολογιστή, ώστε να μειώνεται ο κίνδυνος ακούσιας ή μη εξουσιοδοτημένης πρόσβασης.
- Συνιστάται να αποφεύγεται η αποστολή ή η πρόσβαση σε υπηρεσιακά δεδομένα μέσω δημόσιων ή μη αξιόπιστων Wi-Fi δικτύων, όπως ενδεικτικά ανοικτά δίκτυα χωρίς κωδικό ή δίκτυα των οποίων ο πάροχος/ιδιοκτήτης δεν είναι γνωστός, καθώς δύναται να αυξηθεί ο κίνδυνος υποκλοπής. Όπου είναι εφικτό, η αποστολή αρχείων εκτός των εγκαταστάσεων του Ιδρύματος μπορεί να γίνεται μέσω ασφαλούς σύνδεσης, όπως VPN.
- Η χρήση υπηρεσιακών συσκευών του Ιδρύματος προτιμάται, καθώς έχουν ρυθμιστεί από το αρμόδιο τεχνικό προσωπικό για την παροχή επιπλέον μέτρων ασφάλειας. Σε περίπτωση που απαιτείται η χρήση USB, άλλου φορητού μέσου αποθήκευσης ή προσωπικού υπολογιστή, συνιστάται η εφαρμογή κρυπτογράφησης ή η προστασία με ισχυρό κωδικό πρόσβασης, ώστε να περιορίζεται ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης σε περίπτωση απώλειας ή κλοπής.
- Η ορθή διαχείριση του κύκλου ζωής των προσωπικών δεδομένων συμβάλλει στη συμμόρφωση με το ισχύον νομικό πλαίσιο και στη μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης. Συνιστάται τα δεδομένα να διατηρούνται μόνο για όσο χρονικό διάστημα απαιτείται για τον σκοπό της επεξεργασίας και σύμφωνα με τυχόν ισχύουσες νομικές ή κανονιστικές υποχρεώσεις ή αποφάσεις του Ιδρύματος. Όταν ολοκληρωθεί ο αρχικός σκοπός επεξεργασίας ή όταν δεν υφίσταται πλέον σχετική υποχρέωση διατήρησης, συνιστάται να εξετάζεται η ασφαλής διαγραφή ή, όπου ενδείκνυται, η αρχειοθέτηση των δεδομένων.
- Η διαχείριση αιτημάτων υποκειμένων δεδομένων (π.χ. πρόσβαση, διόρθωση, διαγραφή, περιορισμός επεξεργασίας, φορητότητα) σύμφωνα με τις

κανονιστικές διατάξεις είναι ιδιαίτερα σημαντική στο πλαίσιο των υποχρεώσεων του Ιδρύματος ως Υπεύθυνου Επεξεργασίας. Συνιστάται τα αιτήματα να γνωστοποιούνται άμεσα στον DPO, ώστε να ακολουθηθεί η προβλεπόμενη διαδικασία και να ενημερωθεί ο Υπεύθυνος Επεξεργασίας (Πρύτανης). Για παράδειγμα, αν ένας φοιτητής ζητήσει τη διαγραφή των προσωπικών του δεδομένων, το προσωπικό ενημερώνει τον DPO, ο οποίος στη συνέχεια ενημερώνει τον Πρύτανη, προκειμένου να εξεταστεί και να απαντηθεί το αίτημα σύμφωνα με το ισχύον νομικό πλαίσιο.

- Σε περίπτωση υπόνοιας ή διαπίστωσης παραβίασης προσωπικών δεδομένων (π.χ. απώλεια, μη εξουσιοδοτημένη πρόσβαση, εσφαλμένη κοινοποίηση), συνιστάται η άμεση ενημέρωση των αρμόδιων προσώπων του Ιδρύματος όπως ο Υπεύθυνος Επεξεργασίας (Πρύτανης), ο αρμόδιος Αντιπρύτανης, ο Προϊστάμενος του Τμήματος Εγκαταστάσεων, οι υπεύθυνοι Πληροφοριακών Συστημάτων και ο DPO ώστε να εξεταστεί το περιστατικό και να ληφθούν τα κατάλληλα μέτρα στο πλαίσιο των αρμοδιοτήτων τους.
- Κατά την υποβολή αίτησης συμμετοχής σε έρευνα, συνιστάται οι συμμετέχοντες να ενημερώνονται σαφώς για τον σκοπό της επεξεργασίας, τη διάρκεια τήρησης των δεδομένων και τα δικαιώματά τους. Όταν απαιτείται συγκατάθεση, για παράδειγμα για επεξεργασία δεδομένα προσωπικού χαρακτήρα ειδικής κατηγορίας ή για ανάλυση πέρα από το πλαίσιο σπουδών, συνιστάται να παρέχεται ελεύθερα, συγκεκριμένα και να τεκμηριώνεται, με δυνατότητα ανάκλησης ανά πάσα στιγμή, χωρίς να επηρεάζεται η συμμετοχή σε άλλες δραστηριότητες του Ιδρύματος.
- Σε περίπτωση αποστολής email που περιέχει προσωπικά δεδομένα σε εσφαλμένο ή μη εξουσιοδοτημένο παραλήπτη, συνιστάται να αποστέλλεται άμεσα μήνυμα συνέχειας προς τον λανθασμένο παραλήπτη, με αίτημα διαγραφής του αρχικού μηνύματος και υπενθύμιση ότι δεν επιτρέπεται η περαιτέρω χρήση των πληροφοριών. Παράλληλα, συνιστάται η άμεση ενημέρωση του Υπευθύνου Επεξεργασίας (Πρύτανη) και του DPO, προκειμένου ο Υπεύθυνος Επεξεργασίας να αξιολογήσει το περιστατικό και να δρομολογήσει τις προβλεπόμενες ενέργειες, σύμφωνα με το ισχύον νομικό πλαίσιο, συμπεριλαμβανομένης, όπου απαιτείται, της ενημέρωσης του αρμόδιου τεχνικού ή διοικητικού προσωπικού, με τον DPO για ενημέρωση και παροχή συμβουλών, εφόσον αυτές ζητηθούν.
- Τα δεδομένα που μπορούν να διατηρηθούν συνιστάται να αρχειοθετούνται κατά τρόπο που να επιτρέπει πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες και να κατηγοριοποιούνται με βάση τη φύση, τον τύπο, τον σκοπό και το πλήθος τους (π.χ. απλά δεδομένα προσωπικού χαρακτήρα, δεδομένα προσωπικού χαρακτήρα ειδικής κατηγορίας ή υπηρεσιακά δεδομένα), ώστε να εφαρμόζονται τα κατάλληλα μέτρα προστασίας, ανά περίπτωση, όπως έλεγχοι πρόσβασης και κρυπτογράφηση, όταν αυτό κρίνεται αναγκαίο.
- Συνιστάται να αποφεύγεται το άνοιγμα ύποπτων συνημμένων ή συνδέσμων από μη εξουσιοδοτημένες πηγές, καθώς και μηνυμάτων που φέρουν παραποιημένα υπηρεσιακά ονόματα. Τα ύποπτα email συνιστάται να γνωστοποιούνται άμεσα στο αρμόδιο τεχνικό προσωπικό του Ιδρύματος για έλεγχο.
- Η συμμετοχή σε εκδηλώσεις του Ιδρύματος και η λήψη φωτογραφιών ή βίντεο που ενδέχεται να περιλαμβάνουν προσωπικά δεδομένα συνιστάται να πραγματοποιούνται με σεβασμό στην προστασία των προσώπων. Πριν από τη λήψη ή τη δημοσίευση του σχετικού υλικού, συνιστάται οι συμμετέχοντες να ενημερώνονται σαφώς για τον σκοπό, τον τρόπο χρήσης και τη διάρκεια τήρησής του και, όπου απαιτείται, να παρέχεται η δυνατότητα συγκατάθεσης ή ανάκλησής της. Η κοινοποίηση του υλικού σε μη εξουσιοδοτημένα άτομα ή σε δημόσιες

πλατφόρμες συνιστάται να πραγματοποιείται μόνο κατόπιν λήψης απαιτούμενης συγκατάθεσης ή σχετικής έγκρισης.