



Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) & Πρόγραμμα Προστασίας Προσωπικών Δεδομένων του ΓΠΑ





Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) 679/2016

- Κανονισμός της ΕΕ με άμεση εφαρμογή στα κράτη-μέλη από 25 Μαΐου 2018
- **Ενιαίο θεσμικό πλαίσιο** για την επεξεργασία των προσωπικών δεδομένων που θεσπίζει κανόνες για την προστασία των φυσικών προσώπων και την κυκλοφορία των προσωπικών δεδομένων
- **Δεδομένα Προσωπικού Χαρακτήρα:** κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (όνομα, αριθμός ταυτότητας, δεδομένα θέσης, μισθοδοσία, επιγραμμικό αναγνωριστικό ταυτότητας, κ.α.)
- **Πεδίο Εφαρμογής:** Κάθε οργανισμός που δραστηριοποιείται εντός της Ευρωπαϊκής Ένωσης
- Εφαρμοστικός Νόμος 4624/2019
- Επιβολή διοικητικών προστίμων





Σκοπός και αντικείμενο του ΓΚΠΔ

- Προστατεύει τα δεδομένα προσωπικού χαρακτήρα, δηλαδή κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο
- Προστατεύει και ρυθμίζει τα δικαιώματα των φυσικών προσώπων σχετικά με τα προσωπικά τους δεδομένα, την επεξεργασία τους, την ελεύθερη και ανεμπόδιστη κυκλοφορία και διαβίβαση δεδομένων, τις διαδικασίες διαβίβασης προσωπικών δεδομένων εκτός ΕΟΧ
- Καθορίζει τον κύκλο ζωής των δεδομένων (συλλογή, νόμιμη επεξεργασία, τήρηση και εξασφάλιση, αποθήκευση, μεταβίβαση και διαγραφή)



Ποιους αφορά;

- κάθε οργανισμό που δραστηριοποιείται εντός της ΕΕ:
 - έχει την έδρα του ή εγκαταστάσεις στην ΕΕ ή
 - προσφέρει οποιουδήποτε είδους υπηρεσίες και αγαθά σε Ευρωπαίους πολίτες ή
 - παρακολουθεί την συμπεριφορά Ευρωπαίων πολιτών ως προς τα προσωπικά τους δεδομένα (π.χ. μέσω του Διαδικτύου)
- τελικά αφορά σχεδόν το σύνολο των οργανισμών παγκοσμίως





Πρόστιμα

max 2% του
παγκόσμιου τζίρου ή
€10.000.000 (όποιο
είναι μεγαλύτερο)

max 4% του παγκόσμιου
τζίρου ή €20.000.000
(όποιο είναι μεγαλύτερο)



Στον στενό Δημόσιο Τομέα τα πρόστιμα φθάνουν έως
10.000.000€, βάσει του Ν.4624/2019 (εφαρμοστικός νόμος)



Εξαιρέσεις

Δεν εφαρμόζεται για επεξεργασία:

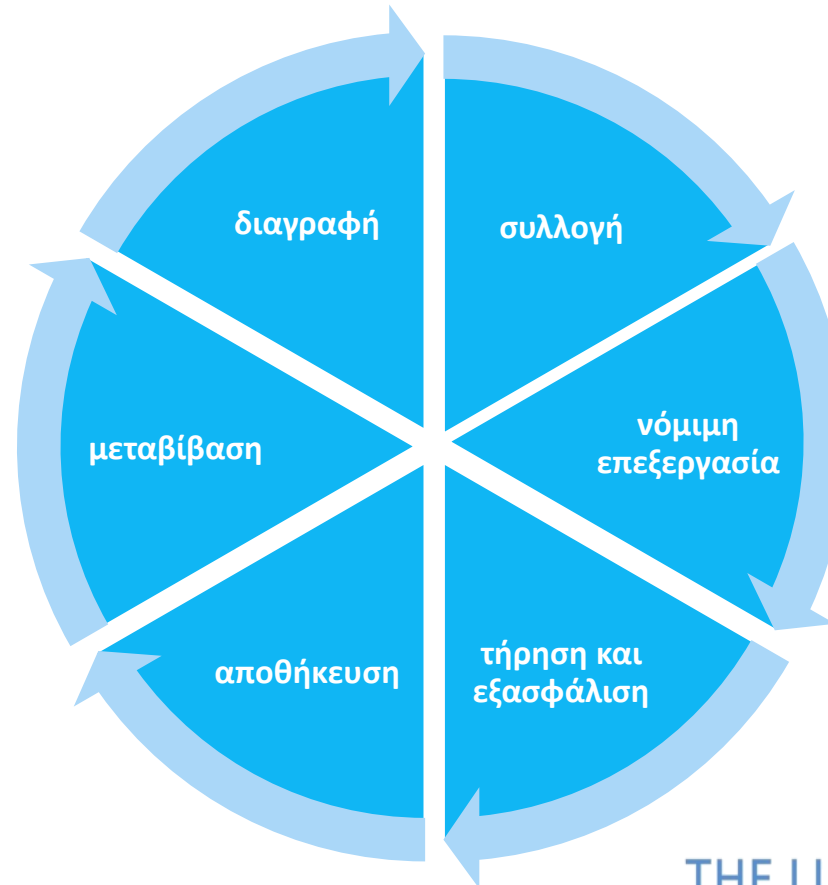
- Από φυσικά πρόσωπα για αυστηρά προσωπική ή οικιακή δραστηριότητα (π.χ. ενέργειες μέσα από προσωπικό λογαριασμό fb)
- Αρμόδιες αρχές για ποινική αδικήματα και δημόσια ασφάλεια
- Αν τα προσωπικά δεδομένα δεν περιλαμβάνονται ή δεν πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης



Τι συνιστά επεξεργασία προσωπικών δεδομένων;

Κάθε πράξη ή σειρά πράξεων με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα ή σε σύνολα δεδομένων, όπως:

- Συλλογή
- Καταχώριση
- Χρήση, Οργάνωση, διάρθρωση, αποθήκευση
- Προσαρμογή ή η μεταβολή
- Ανάκτηση, Αναζήτηση πληροφοριών
- Κοινολόγηση, Διαβίβαση, Διάδοση ή Διάθεση
- Συσχέτιση
- Περιορισμός, διαγραφή ή καταστροφή



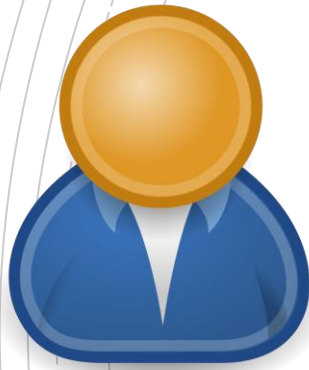
THE LIFE CYCLE OF
PERSONAL DATA





Βασικοί Ρόλοι στην επεξεργασία

προσωπικά δεδομένα



Υποκείμενο των
δεδομένων

κάτοχος των δεδομένων,
φυσικό πρόσωπο



Υπεύθυνος Επεξεργασίας, ΥΕ
(Controller)

καθορίζει το σκοπό και
τον τρόπο



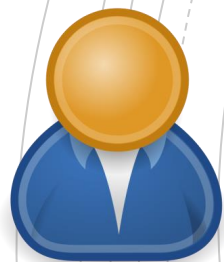
Εκτελών την επεξεργασία, ΕΕ
(Processor)

επεξεργάζεται δεδομένα για
λογαριασμό του υπεύθυνου



Βασικοί Ρόλοι στην επεξεργασία

προσωπικά δεδομένα



Υποκείμενο των
δεδομένων

φυσικό πρόσωπο



Από κοινού Υπεύθυνοι
Επεξεργασίας
(Joint Controllers)

καθορίζουν από κοινού
τον σκοπό και τον τρόπο

Πότε υπάρχει **από κοινού υπευθυνότητα** στην επεξεργασία με τρίτον;

- όταν δύο ή περισσότεροι ΥΕ καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας
- οι ευθύνες για τη συμμόρφωση με τον Κανονισμό καθορίζονται με διαφανή τρόπο μέσω μεταξύ τους συμφωνίας
- ορίζεται σαφώς ποιος εκ των συμβαλλομένων αναλαμβάνει την υποχρέωση ενημέρωσης των ΥΔ
- η συμφωνία τίθεται στη διάθεση του ΥΔ

Ποια θεωρούνται προσωπικά δεδομένα;

- Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, η ταυτότητα του οποίου μπορεί να εξακριβωθεί άμεσα ή έμμεσα
- Μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας (π.χ. όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας, ή σε έναν ή περισσότερους παράγοντες που προσδιορίζουν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του φυσικού προσώπου)
- Ηλεκτρονικά και έγχαρτα αρχεία
- **Ειδικών κατηγοριών δεδομένα:** αυτά που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά ή βιομετρικά δεδομένα, δεδομένα υγείας, δεδομένα σεξουαλικής ζωής ή γενετήσιου προσανατολισμού



Ποια είναι τα προσωπικά δεδομένα που επεξεργάζεται το Πανεπιστήμιο;

- Βασικά δεδομένα προσώπου (π.χ. ον/νυμο, e-mail, τηλέφωνο κιν & σταθερό, τμήμα, σχολή, οικογενειακή κατάσταση, φύλο, πατρώνυμο, μητρώνυμο, e-mail πανεπιστημίου, τόπος γέννησης, δ/νση)
- Μοναδικά Αναγνωριστικά (π.χ. ΑΔΤ, διαβατήριο, ΑΦΜ, ΑΜΚΑ)
- Δεδομένα εκπαίδευσης (π.χ. γνωστικό αντικείμενο, CVs)
- Δεδομένα εργασίας (π.χ. προϋπηρεσία, δημοσιεύσεις, ερευνητική δραστηριότητα κ.λπ.)
- Δεδομένα που σχετίζονται με ποινικές καταδίκες και αδικήματα (π.χ. ποινικό μητρώο, πειθαρχικά, εκκρεμείς υποθέσεις)
- Επιγραμμικά αναγνωριστικά (π.χ. όνομα χρήστη, κωδικός ΑΠΕΛΛΑ)
- Δεδομένα σπουδών (π.χ. πρόγραμμα σπουδών, αναλυτική βαθμολογία)
- Οικονομικά δεδομένα (π.χ. IBAN, μισθοδοσία)



Ποια είναι τα
προσωπικά
δεδομένα που
επεξεργάζεται το
Πανεπιστήμιο;

- Δεδομένα υγείας (π.χ. ειδικές κατηγορίες πάσχοντες με σοβαρές παθήσεις, βεβαίωση ασθένειας)
- Δεδομένα κοινωνικής πρόνοιας (π.χ. πολύτεκνοι)
- Δεδομένα εικόνας (π.χ. φωτογραφίες)
- Δεδομένα συνδεσιμότητας σε λογαριασμούς του Πανεπιστημίου (π.χ. *username/ password* για αυθεντικοποίηση χρήστη, χρόνοι σύνδεσης/ αποσύνδεσης στη περίπτωση διενέργειας εξ αποστάσεως εξετάσεων)



Ποια είναι τα
φυσικά πρόσωπα
που αφορούν το
Πανεπιστήμιο;

- Φοιτητές (Προπτυχιακοί, Μεταπτυχιακοί, Υποψήφιοι Διδάκτορες)
- Φοιτητές στα πλαίσια προγραμμάτων Erasmus
- Συγγενείς φοιτητών
- Απόφοιτοι
- Καθηγητές/ Μέλη ΔΕΠ
- Εκλέκτορες
- Πρόεδρος Τμήματος
- Πρύτανης/ Αντιπρύτανης
- Διδακτικό & Διοικητικό προσωπικό
- Μέλη επιτροπών αξιολόγησης
- Φωτογράφοι
- Τρίτοι



Βασικές αρχές επεξεργασίας





Πότε επιτρέπεται η επεξεργασία;

Προϋποθέσεις Νομιμότητας Επεξεργασίας

Συγκατάθεση
υποκειμένου
δεδομένων

Εκτέλεση
Σύμβασης ή Εν
όψει εκτέλεση
σύμβασης

Εκπλήρωση
καθήκοντος
προς το
δημόσιο
συμφέρον ή
άσκηση
δημόσιας
εξουσίας

Συμμόρφωση
με έννομη
υποχρέωση

Διαφύλαξη
ζωτικού
συμφέροντος
του
υποκειμένου ή
άλλου φυσικού
προσώπου

Έννομο συμφέρον
του Υπεύθυνου
Επεξεργασίας ή
τρίτου), εκτός αν
υπερισχύει το
συμφέρον ή τα
δικαιώματα και οι
ελευθερίες του
υποκειμένου των
δεδομένων, ιδίως
εάν είναι παιδί

Προσοχή!

Η συγκατάθεση δεν αποτελεί τη μόνη βάση νομιμότητας για την επεξεργασία.

Το έννομο συμφέρον δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση καθηκόντων τους.

Η συγκατάθεση δεν μπορεί να θεωρηθεί ελεύθερη όταν ζητείται από δημόσιο φορέα.



Εξαιρέσεις για την επεξεργασία δεδομένων ειδικών κατηγοριών 1/2

Εν γένει η επεξεργασία δεδομένων ειδικών κατηγοριών (π.χ. δεδομένα υγείας) απαγορεύεται από τον ΓΚΠΔ, ωστόσο ορίζονται εξαιρέσεις για τη σύννομη επεξεργασία

Ενδεικτικά:

- Το φυσικό πρόσωπο έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς,
- η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας



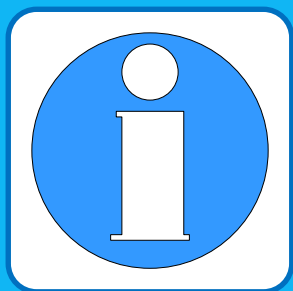
Εξαιρέσεις για την επεξεργασία δεδομένων ειδικών κατηγοριών 2/2

- η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου
- η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών
- η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυννοριακών απειλών κατά της υγείας



Διαφάνεια

- Πληροφόρηση πριν την επεξεργασία
- Υποχρεωτικά στοιχεία πληροφόρησης
- Άρθρα 12-14



ταυτότητα και
στοιχεία επικοινωνίας
εταιρείας,
εκπροσώπου και ΥΠΔ

σκοποί επεξεργασίας

νομιμοποιητική βάση

έννομα συμφέροντα
που επιδιώκονται από
τον ΥΕ (όπου ισχύει)

αποδέκτες

πρόθεση διαβίβασης
σε τρίτη χώρα

χρονικό διάστημα
αποθήκευσης

δικαιώματα φυσικών
προσώπων

δικαίωμα ανάκλησης
συγκατάθεσης

δικαίωμα υποβολής
καταγγελίας

εάν αποτελεί
προϋπόθεση για τη
σύμβαση – συνέπειες
μη παροχής

ύπαρξη
αυτοματοποιημένης
λήψης αποφάσεων ή/
και δημιουργία
προφίλ

πηγή λήψης (όταν τα
ΔΠΧ δεν συλλέγονται
απευθείας από τα
φυσικά πρόσωπα)

κατηγορίες των
δεδομένων (όταν τα
ΔΠΧ δεν συλλέγονται
απευθείας από τα
φυσικά πρόσωπα)



Χαρακτηριστικά Πληροφόρησης





Περιπτώσεις που απαιτείται πληροφόρηση:

EXAMPLE

Έντυπες φόρμες εγγραφής φοιτητών

Αίτηση υποψηφίου Erasmus+

Πρόσκληση / ανακοίνωση εκδήλωσης Πανεπιστημίου

Αίτηση για αποκτηση δικαιωμάτων μέλους βιβλιοθήκης, αίτηση για διαδανεισμό βιβλίου, δηλώση έγκρισης ηλεκτρονικής δημοσίευσης διατριβής

Αίτηση Πρακτικής Άσκησης στο εξωτερικό

Σύμβαση με προμηθευτές

Δελτίο Επισκέπτη (Γραφείο Διασύνδεσης)

Αιτήσεις Προσωπικού

Αίτηση – Δήλωση για παροχή δωρεάν σίτισης



Ποια είναι τα χαρακτηριστικά της συγκατάθεσης;

Θετική ενέργεια του προσώπου (opt in)

Δεν ισχύουν πλέον:

opt out επιλογές

προσυμπληρωμένα
κουτάκια

σιωπηρή αποδοχή γενικών
όρων

Εν πλήρει επιγνώσει

*Το κείμενο πρέπει να
είναι:*

εύκολα προσβάσιμο

κατανοητό

διακριτό

σε σαφή και απλή
διατύπωση

Ελεύθερη

Δεν βασίζεται σε:

ανισότητα μερών
(π.χ. εργαζόμενος-εργοδότης)

όρο για την προσφορά
προϊόντος ή υπηρεσίας

έλλειψη δυνατότητας ανάκλησης
συγκατάθεσης



Δικαιώματα φυσικών προσώπων

Παροχή πληροφόρησης

Παροχή πληροφοριών σχετικά με την επεξεργασία των δεδομένων του από τον οργανισμό

Πρόσβαση σε δεδομένα

- πρόσβαση σε όλα τα προσωπικά δεδομένα και σε πληροφορίες επεξεργασίας και παροχή δωρεάν αντιγράφου. Αν ζητηθεί ηλεκτρονικά, παρέχεται σε ηλεκτρονική μορφή.

Διόρθωση δεδομένων

- διόρθωση ανακριβών ή ελλιπών δεδομένων (π.χ. ο πελάτης ζητά από την εταιρεία, να αλλάξει την ηλεκτρονική του διεύθυνση)

Διαγραφή δεδομένων

- αφορά όλες τις μορφές στις οποίες τηρούνται τα δεδομένα (έντυπη, ηλεκτρονική) και όλα τα σημεία τήρησης/ αποθήκευσης, αν δεν υπάρχει υποχρέωση τήρησης

Φορητότητα δεδομένων

- μετάβαση από έναν πάροχο υπηρεσιών σε άλλον δεδομένων που έχουν παρασχεθεί από το φυσικό πρόσωπο σε κατάλληλη για διαχείριση μορφή



Δικαιώματα φυσικών προσώπων

Περιορισμός επεξεργασίας

- περιορισμός λόγω αντιρρήσεων του φυσικού προσώπου για την επεξεργασία π.χ. αμφισβητεί τους λόγους/τη νομιμότητα/την ακρίβεια των δεδομένων της επεξεργασίας

Εναντίωση στην επεξεργασία

- εναντίωση στην επεξεργασία που πραγματοποιείται για λόγους δημοσίου συμφέροντος ή έννομων συμφερόντων του Υπεύθυνου Επεξεργασίας

Μη υποβολή σε αυτοματοποιημένη λήψη αποφάσεων

- Μη υποβολή αν δεν εξασφαλιστεί η ανθρώπινη παρέμβαση στο αποτέλεσμα της απόφασης και η ανάγκη της επεξεργασίας λόγω σύμβασης, δικαίου ή ρητής συγκατάθεσης

Υποβολή καταγγελίας στην εποπτική αρχή

- πληροφόρηση από τον Υπεύθυνο Επεξεργασίας για δυνατότητα υποβολής καταγγελίας



- Υποχρέωση ανταπόκρισης στα αιτήματα του υποκειμένου εντός **1 μήνα** (+2 με πληροφόρηση εντός του 1^{ου} μήνα για τους λόγους καθυστέρησης) και **χωρίς οικονομική επιβάρυνση** (με εύλογο τέλος, για προδήλως αβάσιμα και υπερβολικά αιτήματα)
- Ενημέρωση λοιπών Υπεύθυνων Επεξεργασίας ή Εκτελούντων την Επεξεργασία (συνδέσμων, αντιγράφων, αναπαραγωγών) για διόρθωση, διαγραφή και περιορισμό



Διασφάλιση συνεργατών

Πώς διαχειρίζεται το
Πανεπιστήμιο
συνεργάτες-εκτελούντες
την επεξεργασία;

Υποχρεωτική σύμβαση με συγκεκριμένες απαιτήσεις:

- αντικείμενο επεξεργασίας, διάρκεια, φύση & σκοπός επεξεργασίας, είδος δεδομένων, κατηγορίες φυσικών προσώπων, υποχρεώσεις και δικαιώματα των μερών
- δεσμεύσεις εμπιστευτικότητας των αρμόδιων στελεχών του Εκτελούντος την Επεξεργασία
- ο Εκτελών την Επεξεργασία παρέχει επαρκείς διαβεβαιώσεις, π.χ. πιστοποιήσεις, επιτρέπει έλεγχο (επιθεωρήσεις) και διαθέτει πληροφορίες για απόδειξη της συμμόρφωσης
- απαγορεύεται η υπεργολαβία χωρίς άδεια του Υπεύθυνου Επεξεργασίας
- ο υπεργολάβος του Εκτελούντος την Επεξεργασία έχει ακριβώς τις ίδιες υποχρεώσεις, ενώ στον Εκτελούντα την Επεξεργασία παραμένουν όλες οι ευθύνες
- ο Εκτελών την Επεξεργασία διαγράφει και επιστρέφει δεδομένα και αντίγραφα κατ' εντολή του Υπεύθυνου Επεξεργασίας επικουρεί τον Υπεύθυνο Επεξεργασίας για την ασφάλεια, για γνωστοποιήσεις, για εκτίμηση επιπτώσεων και για απάντηση σε αιτήματα



Πότε επιτρέπεται η
διαβίβαση εκτός
Πανεπιστημίου;



Εντός ΕΟΧ
επιτρέπεται



Εκτός ΕΟΧ
υπό προϋποθέσεις

Προσοχή!

Για τις διαβιβάσεις σε τρίτους εντός ΕΟΧ θα πρέπει να υπάρχει βάση νομιμότητας για τη διαβίβαση.
Για τις διαβιβάσεις εκτός ΕΟΧ θα πρέπει να υπάρχει εκτός του ανωτέρω και κατάλληλη εγγύηση



Ασφάλεια πληροφοριών

Η προστασία της

εμπιστευτικότητας

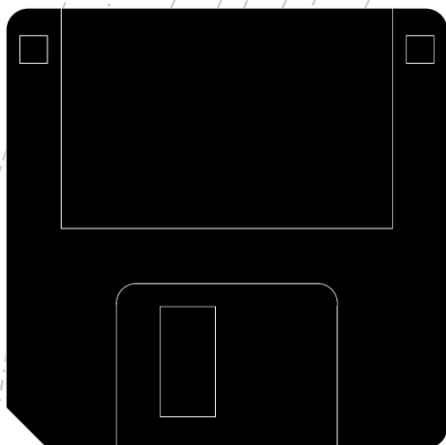
ακεραιότητας

διαθεσιμότητας





Που βρίσκονται τα δεδομένα;



- υποδομές επικοινωνίας πληροφορικής (*email servers, proxy servers, corporate network, wireless network* κ.λπ.)
- hardware (*computers, servers, USB drives, Hard Disk Drives* κ.λπ.)
- software (*Databases, Business Applications, Intranet Site* κ.λπ.)
- συσκευές και λογισμικό υπό των έλεγχο των χρηστών (*smart phones, tablets, internet browser S/W* κ.λπ.)
- έγγραφα σε έντυπη μορφή (*εκτυπώσεις, φωτοαντίγραφα* κ.λπ.)
- ταχυδρομείο (*αποστολή φυσικών εγγράφων*)



Παραδείγματα Κινδύνων Ασφάλειας Πληροφοριών

- Υποκλοπή πληροφορίας (ηλ. μορφής, έντυπης)
- Κλοπή εξοπλισμού
- Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο
- Εγκατάσταση κακόβουλου λογισμικού
- Hackers
- Αστοχία τηλεπικοινωνιών/δικτύου/ρεύματος
- Καταστροφή εξοπλισμού
- Σφάλμα χρήσης
- Πολλά άλλα

ΜΕ ΑΠΟΤΕΛΕΣΜΑ:

- Διαρροή δεδομένων
- Καταστροφή δεδομένων
- Διακοπή της λειτουργίας



Τι είναι περιστατικό
παραβίασης
προσωπικών
δεδομένων;

η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία



Τι είναι περιστατικό παραβίασης προσωπικών δεδομένων;

Παραδείγματα

- απώλεια αρχείων ή εγγράφων με προσωπικά δεδομένα στο χώρο εργασίας μου
- απώλεια εξωτερικού σκληρού δίσκου ο οποίος περιέχει προσωπικά δεδομένα
- τυχαία καταστροφή εγγράφων με προσωπικά δεδομένα (π.χ. πυρκαγιά)
- διαγραφή ή τροποποίηση ηλεκτρονικών αρχείων με προσωπικά δεδομένα
- πρόσβαση σε προσωπικά δεδομένα σε πληροφοριακά συστήματα ή σε κοινόχρηστους φακέλους που δεν θα έπρεπε να έχω
- κοινοποίηση ή απώλεια κωδικών πρόσβασης σε πληροφοριακά συστήματα
- απώλεια προσωπικών δεδομένων από συνεργάτη του Πανεπιστημίου
- διατήρηση δεδομένων (π.χ. ιατρικές διαγνώσεις, βαθμολογίες) σε κοινή θεά



Πώς διασφαλίζει το
Πανεπιστήμιο την
ασφαλή
επεξεργασία
δεδομένων;

- Λήψη τεχνικών μέτρων
- Λήψη οργανωτικών μέτρων



Τεχνικά μέτρα

- ψευδωνυμοποίηση και κρυπτογράφηση ΔΠΧ
- διασφάλιση απορρήτου, ακεραιότητας, διαθεσιμότητας και αξιοπιστίας συστημάτων και υπηρεσιών επεξεργασίας σε συνεχή βάση
- δυνατότητα αποκατάστασης διαθεσιμότητας και πρόσβασης σε ΔΠΧ σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος
- τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας



Χαρακτηριστικά και χειρισμός κωδικών πρόσβασης

- Πρέπει να έχουν μήκος τουλάχιστον 8 χαρακτήρων
- Πρέπει να έχουν τουλάχιστο ένα χαρακτήρα από τις ακόλουθες κατηγορίες:
 - Κεφαλαία γράμματα
 - Μικρά γράμματα
 - Αριθμοί
 - Ειδικοί χαρακτήρες
- Πρέπει να αλλάζουν κάθε ενενήντα ημέρες/ να είναι διαφορετικοί από τους τελευταίους τέσσερις
- Οι κωδικοί πρόσβασης δεν θα πρέπει να συνδέονται με προσωπικά στοιχεία του χρήστη
- Δεν πρέπει να τους γράφουμε σε έντυπα μέσα
- Δεν πρέπει να τους αποθηκεύουμε ηλεκτρονικά σε text αρχεία / να τους στέλνουμε με email
- **Τους προσωπικούς μας κωδικούς δεν τους ανακοινώνουμε σε Κανέναν!!!! Οι κωδικοί είναι απόρρητες πληροφορίες**



Καλές πρακτικές

Εφαρμογή πολιτικής καθαρού γραφείου – καθαρής οθόνης

Αποσυνδεόμαστε από εφαρμογές, απενεργοποιούμε τον υπολογιστή μας και τακτοποιούμε το γραφείο μας όποτε εγκαταλείπουμε την εργασία μας

Δε καταγράφουμε ευαίσθητη πληροφορία σε χαρτιά ή άλλα μέσα αποθήκευσης τα οποία βρίσκονται εκτεθειμένα πάνω στο γραφείο μας. Μετά τη λήξη της εργασίας όλα τα έντυπα πρέπει να τακτοποιούνται και να κλειδώνονται ασφαλώς

Ασφαλίζουμε τους προβλεπόμενους χώρους (αίθουσες, γραφεία, αποθήκες, συρτάρια, φωριαμοί)

Απομακρύνουμε όλα τα έντυπα από τα εκτυπωτικά, και τα φωτοαντιγραφικά μηχανήματα και εάν δεν ασφαρίζονται στις καθορισμένες θέσεις που έχουν προβλεφθεί, τα καταστρέφουμε



Οργανωτικά μέτρα

- Πολιτικές , Διαδικασίες και Οδηγίες (Πρόγραμμα Προστασίας Προσωπικών Δεδομένων)
- Δημιουργία ρόλων



Πρόγραμμα Προστασίας Προσωπικών Δεδομένων

- είναι το σύνολο των πολιτικών και διαδικασιών που καθορίζει τον τρόπο με τον οποίο επεξεργαζόμαστε καθημερινά προσωπικά δεδομένα.
- αποτελείται από Πολιτικές, Διαδικασίες και Οδηγίες
- υιοθετείται & εφαρμόζεται από όλο το προσωπικό
- είναι το πλαίσιο εκπαίδευσης του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων
- οι Πολιτικές αποτελούν δεσμεύσεις της Διοίκησης του Πανεπιστημίου



Σχέδιο αντιμετώπισης περιστατικών παραβίασης

- Σε περίπτωση ύπαρξης περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων πραγματοποιείται μία πρώτη καταγραφή για το περιστατικό στο έντυπο «Αναφορά παραβίασης προσωπικών δεδομένων»
- Εκτιμάται το μέγεθος της επίπτωσης που ενδέχεται να έχει για τα φυσικά πρόσωπα
- ο Υπεύθυνος Προστασίας Δεδομένων αναζητά τα αίτια της παραβίασης και συλλέγει στοιχεία τα οποία μπορούν να χρησιμοποιηθούν για να προσδιοριστεί αν θα απαιτηθεί η λήψη μέτρων για την αντιμετώπισή της.
- Τηρείται «Μητρώο παραβιάσεων προσωπικών δεδομένων»
- Το συμβάν αξιολογείται προκειμένου να προβεί το Πανεπιστήμιο σε γνωστοποίηση στην ΑΠΔΠΧ ή/και στο φυσικό πρόσωπο



Διαδικασίες

- Διαδικασίες διαχείρισης αιτημάτων
- Διαδικασία για ασφαλή καταστροφή προσωπικών δεδομένων
- Διαδικασία διαχείρισης παραπόνων
- Διαδικασία για την απόκτηση έγκυρης συναίνεσης
- Διαδικασία Διαχείρισης Αρχείου Δραστηριοτήτων Επεξεργασίας
- Διαδικασίες διαχείρισης παραβιάσεων προσωπικών δεδομένων και κοινοποίησης της παραβίασης
- Διαδικασία συνεχούς παρακολούθησης και ενημέρωσης
- Διαδικασία για τις Δευτερεύουσες χρήσεις προσωπικών δεδομένων
- Διαχείριση Αρχείου Δραστηριοτήτων Επεξεργασίας



Διαδικασία κοινοποίησης της παραβίασης και υποβολή αναφορών

(Δ12)

- Αν το περιστατικό κριθεί σύμφωνα με το «Σχέδιο αντιμετώπισης περιστατικών παραβίασης, πιθανό να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ότι απαιτείται η γνωστοποίηση στην ΑΠΔΠΧ, τότε ο Υπεύθυνος Προστασίας Δεδομένων ενημερώνει τη Διοίκηση του Πανεπιστημίου.
- Ο Υπεύθυνος Προστασίας Δεδομένων γνωστοποιεί το περιστατικό **εντός 72 ωρών** από τον εντοπισμό του περιστατικού παραβίασης, χρησιμοποιώντας τις «Φόρμες γνωστοποίησης παραβίασης» της ΑΠΔΠΧ
- Αν ο κίνδυνος της παραβίασης είναι υψηλός για τα δικαιώματα και ελευθερίες του φυσικού προσώπου, το Πανεπιστήμιο έχει την υποχρέωση να ανακοινώσει την παραβίαση και προς τα φυσικά πρόσωπα.
- Διατηρείται το έντυπο «Αναφορά παραβίασης προσωπικών δεδομένων» και το «Μητρώο παραβιάσεων προσωπικών δεδομένων» για την τήρηση αρχείου παραβιάσεων.



Διαδικασία για την απόκτηση έγκυρης συναίνεσης

(Δ14)

Αφορά μόνο τις επεξεργασίες για
τις οποίες το Πανεπιστήμιο ενεργεί
ως Υπεύθυνος Επεξεργασίας

- Οι προϊστάμενοι των Διευθύνσεων/ Τμημάτων/Δομών έχουν στη διάθεσή τους (λόγω υφιστάμενης επεξεργασίας) ή δημιουργούν (αν πρόκειται για νέα επεξεργασία) κείμενα συγκατάθεσης για τη δραστηριότητα που είναι αρμόδιοι.
- Τα νέα κείμενα συγκατάθεσης πρέπει να ελεγχθούν και να εγκριθούν από τη Νομική Υπηρεσία και τον Υπεύθυνο Προστασίας Δεδομένων προτού χρησιμοποιηθούν.
- Η συγκατάθεση λαμβάνεται από τα φυσικά πρόσωπα πριν τη διενέργεια της επεξεργασίας
- Στο έντυπο «Μητρώο Πληροφορήσεων και Συγκαταθέσεων» καταγράφονται οι συγκαταθέσεις.
- Σε περιοδική βάση (τουλάχιστον ετησίως) οι προϊστάμενοι προβαίνουν σε ανασκόπηση των συγκαταθέσεων σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων



Διαδικασία για την απόκτηση έγκυρης συναίνεσης

(Δ01)

- Τα φυσικά πρόσωπα έχουν το δικαίωμα ανάκλησης της συγκατάθεσής τους για έναν ή περισσότερους σκοπούς επεξεργασίας, για τους οποίους την έχουν παρέχει, και μέσω του τρόπου ανάκλησης που τους παρέχει το Πανεπιστήμιο κατά περίπτωση και για τον οποίο έχουν ενημερωθεί από τα κείμενα συγκατάθεσης.
- Το αίτημα ανάκλησης αξιολογείται από τον προϊστάμενο της αρμόδιας Διεύθυνσης/ ή του Τμήματος/ ή της Δομής σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων και τη Νομική Υπηρεσία του Πανεπιστημίου προκειμένου να αξιολογηθεί αν απαιτείται ο περιορισμός της επεξεργασίας ή η διαγραφή των δεδομένων λόγω της ανάκλησης συγκατάθεσης ή η τήρησή τους λόγω νομικής υποχρέωσης ή δημόσιου συμφέροντος του Πανεπιστημίου
- Κατόπιν της αξιολόγησης, το Πανεπιστήμιο προβαίνει σε ενέργειες περιορισμού επεξεργασίας ή διαγραφής των δεδομένων ή ενημέρωσης του φυσικού προσώπου για τους λόγους που υποχρεώνουν το Πανεπιστήμιο να τηρήσει τα δεδομένα.



Παραδείγματα Λήψης Συναίνεσης

- Επεξεργασία δεδομένων εικόνας (φωτογραφιών) κατά την συμμετοχή σε εκδηλώσεις και συμμετοχή σε διαγωνισμούς.
- Σημειώνεται πως η συγκατάθεση δεν αποτελεί συνήθη νομική βάση για τις επεξεργασίες που διενεργεί το Πανεπιστήμιο και χρησιμοποιείται μόνο σε συγκεκριμένες επεξεργασίες, εφόσον ο Υπεύθυνος Προστασίας Δεδομένων και η Νομική Υπηρεσία κρίνουν πως απαιτείται.



Διαδικασίες διαχείρισης Αιτημάτων

(Δ 02-Δ08)

Οι διαδικασίες περιγράφουν τον τρόπο διαχείρισης αιτημάτων των φυσικών προσώπων για:

- πρόσβαση σε προσωπικά δεδομένα,
- διόρθωση προσωπικών δεδομένων,
- εξαίρεση, περιορισμό της επεξεργασίας ή αντιρρήσεις στην επεξεργασία,
- παροχή πληροφόρησης,
- φορητότητας δεδομένων,
- διαγραφή δεδομένων,

Διασφαλίζουν την έγκαιρη και αποτελεσματική ικανοποίηση των δικαιωμάτων τους.



Πώς διαχειρίζομαι ένα αίτημα;

Διαδικασίες Αιτημάτων (Δ 02-Δ08)

- λήψη αιτήματος μέσω:
 - ✓ Email
 - ✓ ταχυδρομικής επιστολής στη διεύθυνση του Πανεπιστημίου
 - ✓ Με χρήση έντυπου «Αίτημα Διαχείρισης Προσωπικών Δεδομένων»
- Πιστοποίηση ταυτότητας φυσικού προσώπου που υποβάλει το αίτημα από τον λήπτη του αιτήματος
- προώθηση αιτήματος σε DPO για αξιολόγηση εγκυρότητας και νομιμότητας
- υλοποίηση του αιτήματος σύμφωνα με τις οδηγίες του DPO
- απάντηση στο φυσικό πρόσωπο εντός ένα μήνα ή εντός δύο μηνών εφόσον έχει αιτιολογηθεί



Πώς διαχειρίζομαι ένα αίτημα;

Διαδικασίες Αιτημάτων (Δ 02-Δ08)

- ενημερώνω γραπτώς σχετικά με την καθυστέρηση ικανοποίησης του αιτήματος, τους λόγους που την προκαλούν και τον τελικό χρόνο υλοποίησης
- ενημερώνω τα τρίτα μέρη (π.χ. εξωτερικούς συνεργάτες) σχετικά με τα αιτήματα των φυσικών προσώπων στην περίπτωση που εμπλέκονται στην επεξεργασία
- Ενημερώνω άμεσα τον Υπεύθυνο Επεξεργασίας σχετικά με τα αιτήματα των φυσικών προσώπων στην περίπτωση που το Πανεπιστήμιο ενεργεί ως Εκτελών την Επεξεργασία



Παραδείγματα αιτημάτων

- Αίτημα φοιτητή για πρόσβαση στα δεδομένα του
- Αίτημα φοιτητή για διόρθωση των δεδομένων του (π.χ. αλλαγή διεύθυνσης ή τόπου διαμονής)
- Αίτημα απόφοιτων για διαγραφή των δεδομένων του. Προσοχή! Στην περίπτωση αιτήματος διαγραφής δεδομένων πρέπει να εξετάσει αν είναι δυνατή η διαγραφή τους ή υποχρεούται σύμφωνα με το ισχύον νομοθετικό πλαίσιο να τα διατηρήσει. Σε κάθε περίπτωση πρέπει να ενημερώσει το φυσικό πρόσωπο για τη πορεία του αιτήματος του



Διαδικασία για την ασφαλή καταστροφή των προσωπικών δεδομένων

(Δ10)

- Τα αιτήματα για καταστροφή πόρων δημιουργούνται από τους Ιδιοκτήτες τους όταν συντρέχει ανάγκη καταστροφής παρωχημένου πληροφοριακού εξοπλισμού ή διαγραφής πληροφοριών από τα πληροφοριακά συστήματα ή καταστροφής φυσικού αρχείου με χρήση του εντύπου «Αίτημα Καταστροφής Πόρων»
- Εξετάζονται τα αιτήματα.
- Προσδιορίζεται ο Υπεύθυνος Καταστροφής (π.χ. προσωπικό ή εξωτερικός συνεργάτης) και η ανάγκη λήψης πρόσθετων μέτρων ασφάλειας
- Τηρείται Μητρώο Καταστροφής πόρων



Διαδικασία καταγραφής παραπόνων σχετικά με την προστασία των προσωπικών δεδομένων

Δ11

- Ως παράπονο ορίζεται η άμεση ή έμμεση έκφραση της δυσaréσκειας του φυσικού προσώπου σχετικά με την προστασία των προσωπικών δεδομένων στις υπηρεσίες που παρέχονται από το Πανεπιστήμιο ή τους χώρους των εγκαταστάσεων του Πανεπιστημίου
- Τα φυσικά πρόσωπα έχουν τη δυνατότητα παραπόνων είτε αυτοπροσώπως είτε μέσω αντιπροσώπου (άλλο φυσικό πρόσωπο με εξουσιοδότηση ή νομικό πρόσωπο, κ.λπ.) με χρήση του εντύπου «Αίτημα Παραπόνου»
- Ο λήπτης του παραπόνου πρέπει να πιστοποιήσει την ταυτότητα του φυσικού προσώπου
- Ο Υπεύθυνος Προστασίας Δεδομένων καταγράφει τα παράπονα σε Μητρώο Παραπόνων και ενημερώνει τη Σύγκλητο και την αρμόδια Διεύθυνση/Τμήμα/Δομή για την επεξεργασία για την οποία αφορά το παράπονο.
- Το παράπονο αξιολογείται και το Πανεπιστήμιο προβαίνει στις κατάλληλες ενέργειες (π.χ. διαχείριση ως καταγγελία, απόρριψη, λήψη διορθωτικών μέτρων)



Διαδικασία συνεχούς
παρακολούθησης και
ενημέρωσης για νέες
απαιτήσεις
συμμόρφωσης
(Δ13)

Εξετάζεται συνολικά η καταλληλότητα, η επάρκεια και η αποτελεσματικότητα των Διαδικασιών και Πολιτικών Διασφάλισης των Προσωπικών Δεδομένων. Οι απαραίτητες ενέργειες για την επίτευξη των ανωτέρω είναι:

- Η ενημέρωση για το ισχύον νομικό και κανονιστικό πλαίσιο που αφορά την προστασία των προσωπικών δεδομένων, ώστε να εξασφαλιστεί η πλήρης αναγνώριση των νομικών, ρυθμιστικών και κανονιστικών απαιτήσεων στις οποίες πρέπει να συμμορφωθεί το Πανεπιστήμιο
- Η διαχείριση αστοχιών – προληπτικές ενέργειες
- Η μέτρηση της απόδοσης – στοχοθεσία
- Η διενέργεια συμβουλίου της Διοίκησης του Πανεπιστημίου με σκοπό την ανασκόπηση των Διαδικασιών και Πολιτικών Διασφάλισης των Προσωπικών Δεδομένων.



Διαδικασία Διαχείρισης Αρχείου Δραστηριοτήτων Επεξεργασίας Διαδικασία

(Δ15)

Η διαδικασία προσδιορίζει τον τρόπο με τον οποίο γίνεται:

- ο καθορισμός των δραστηριοτήτων του Πανεπιστημίου που περιλαμβάνουν επεξεργασία δεδομένων προσωπικού χαρακτήρα,
- η κατάρτιση των σχετικών αρχείων δραστηριοτήτων επεξεργασίας (ανάλογα με το ρόλο του Πανεπιστημίου, π.χ. Υπεύθυνος ή Εκτελών την Επεξεργασία)
- η τακτική και συστηματική επικαιροποίηση του



Τι είναι το αρχείο δραστηριοτήτων επεξεργασίας;

Διαδικασία Διαχείρισης Αρχείου
Δραστηριοτήτων (Δ15)

- είναι το Αρχείο που περιγράφει τις ροές των προσωπικών δεδομένων για κάθε σκοπό επεξεργασίας
- επικαιροποιείται σε ετήσια βάση ή κάθε φορά προκύπτει ουσιαστική αλλαγή
- Κάθε Διεύθυνση/ Τμήμα / ή Δομή του Πανεπιστημίου είναι **ενήμερη** για τη ροή των δεδομένων που τον αφορά
- οι επικεφαλές των τμημάτων/διευθύνσεων/δομών ειδοποιούν τον Υπεύθυνο Προστασίας Δεδομένων σε περίπτωση ανάγκης για τροποποίηση του αρχείου



Οδηγίες

- Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στη χρήση των κοινωνικών μέσων δικτύωσης
- Οδηγία για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στη χρήση καμερών
- Οδηγία για λογαριασμούς ηλεκτρονικού ταχυδρομείου των εργαζομένων και των μελών της ακαδημαϊκής κοινότητας
- Οδηγίες για ενσωμάτωση προστασίας ΔΠΧ σε πρακτικές υγείας και ασφάλειας
- Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές διαδικασίες του Bring Your Own Device



Οδηγίες για χρήση των κοινωνικών μέσων δικτύωσης

- Αποφυγή ενεργειών επιλογής (κλικ) πάνω σε διαφημίσεις, banners προσφορών και γενικότερα σε pop-up παράθυρα.
- Απαγόρευση δημιουργίας λογαριασμών σε κοινωνικά μέσα δικτύωσης με τα ίδια αναγνωριστικά (username ή / και password) που χρησιμοποιούνται ήδη για πρόσβασή σε πληροφοριακούς πόρους του Πανεπιστημίου
- Δεν κοινοποιούνται φωτογραφίες φυσικών προσώπων που έχουν αιτηθεί να μην χρησιμοποιηθούν οι φωτογραφίες τους στα προφίλ που διαθέτει το Πανεπιστήμιο στα κοινωνικά μέσα δικτύωσης
- Σε περίπτωση ανάρτηση φωτογραφιών φυσικών προσώπων σε μέσα κοινωνικής δικτύωσης, πρέπει να έχει διασφαλιστεί πρωτίτερα η νομιμότητα της επεξεργασίας (π.χ. λήψη συγκατάθεσης)
- Δεν απαντώνται αιτήματα πολιτών μέσω social media και ειδικότερα αυτά που εμπεριέχουν δεδομένα ειδικών κατηγοριών (π.χ. δεδομένα υγείας), αλλά δίνεται στο φυσικό πρόσωπο πληροφόρηση για τον επίσημο τρόπο υποβολής του αιτήματός του.



Οδηγία για χρήση κάμερας

cctv

- Η εγκατάσταση και η λειτουργία του συστήματος βιντεοεπιτήρησης αξιολογείται όσον αφορά στη αναγκαιότητα και τη νομιμότητα της επεξεργασίας
- Ο σκοπός παρακολούθησης θα πρέπει να τεκμηριώνεται εγγράφως και να εξειδικεύεται για κάθε κάμερα που χρησιμοποιείται
- Ανάρτηση ενημερωτικής πινακίδας σε εμφανές σημείο πριν την είσοδο στο χώρο όπου γίνεται βιντεοεπιτήρηση ως πρώτο επίπεδο πληροφόρησης και ένα πιο αναλυτικό κείμενο ως δεύτερο επίπεδο που θα παρέχει τη εις βάθος ανάλυση της επεξεργασίας
- Απαγορεύεται η βιντεοεπιτήρηση δημόσιων χώρων (π.χ. πεζοδρόμιο, πλατείες κ.λπ.), χώρων υψηλής ιδιωτικότητας καθώς και η βιντεοεπιτήρηση για επιτήρηση των εργαζομένων
- Κάθε διαβίβαση δεδομένων αποτελεί ξεχωριστή επεξεργασία για την οποία το Πανεπιστήμιο πρέπει να εξετάζει τη νομιμότητα της
- Τα δεδομένα εικόνας διατηρούνται έως και 72 ώρες (εκτός από ορισμένες περιπτώσεις)
- Το Πανεπιστήμιο φροντίζει για την ικανοποίηση των δικαιωμάτων των φυσικών προσώπων



Οδηγία για χρήση κάμερας

Τηλεδιασκέψεις

- Η διενέργεια τηλεδιάσκεψης δύναται να πραγματοποιηθεί για τα ακόλουθα:
 - για την παροχή από τους διδάσκοντες εξ αποστάσεως μαθημάτων ή των εξ αποστάσεως συναντήσεων με χρήση πλατφόρμων ή εφαρμογών του Πανεπιστημίου
 - για την πραγματοποίηση εξ αποστάσεως συγκεντρώσεων/ συνελεύσεων συλλογικών οργάνων του Πανεπιστημίου,
 - για την πραγματοποίηση εκλεκτορικών διαδικασιών και
 - για την υποστήριξη διδακτορικών διατριβών
- Η διενέργεια τηλεδιάσκεψης αξιολογείται όσον αφορά στη αναγκαιότητα και τη νομιμότητα της επεξεργασίας.
- Το Πανεπιστήμιο ενημερώνει σε προγενέστερο χρόνο τους συμμετέχοντες, αναφορικά με τη βιντεοσκόπηση και τη διενεργούμενη επεξεργασία
- Απαγορεύεται η βιντεοσκόπηση και ηχογράφηση της τηλεδιάσκεψης από τους συμμετέχοντες και η περαιτέρω χρήση του βιντεοσκοπημένου υλικού για σκοπό άλλο από αυτόν για τον οποίο συλλέχθηκε
- Δίνονται συστάσεις προς τους συμμετέχοντες στην τηλεδιάσκεψη, οι οποίες θα κατατείνουν στην υποβολή σε επεξεργασία των ελάχιστων δυνατών προσωπικών τους δεδομένων (π.χ. απενεργοποίηση καμερών)



Οδηγία για λογαριασμούς ηλεκτρονικού ταχυδρομείου

- Επιβεβαιώνεται ότι το μήνυμα που θα στείλει απευθύνεται στον σωστό παραλήπτη με τη σωστή ηλεκτρονική διεύθυνση
- Δεν επιτρέπεται η αποστολή μαζικών ηλεκτρονικών μηνυμάτων σε ομάδες ατόμων, όπου τα στοιχεία τους είναι ορατά από όλους τους παραλήπτες
- Οι χρήστες κρυπτογραφούν τα αρχεία με εμπιστευτικές πληροφορίες ή πληροφορίες που αφορούν ειδικές κατηγορίες δεδομένων που διακινούνται με email
- Οι χρήστες δεν ανοίγουν αρχεία που είναι συνημμένα σε emails όταν δεν είναι απολύτως σίγουροι για την ταυτότητα του αποστολέα
- Δεν θα πρέπει να αποκαλύπτεται σε καμία περίπτωση κανένα αναγνωριστικό (username – password) ηλεκτρονικών λογαριασμών
- Σε περίπτωση που υπάρχει υποψία ότι ένα e-mail περιέχει ιό, θα πρέπει να ενημερώνεται άμεσα ο DPO
- Το email (mailbox) δεν είναι αποθηκευτικός χώρος



Οδηγίες στη περίπτωση Bring Your Own Device

- Η προστασία των φορητών συσκευών είναι σημαντική για το Πανεπιστήμιο προκειμένου να διατηρείται η εμπιστευτικότητα των πληροφοριών που αποθηκεύονται σε αυτές.
- Δημιουργία και εφαρμογή κατάλληλης πολιτικής ασφάλειας πληροφοριών και προσδιορισμό κατάλληλων απαιτήσεων παραμετροποίησης των φορητών συσκευών.
- Οι χρήστες φορητών συσκευών:
 - Θα πρέπει να λαμβάνουν όλα τα απαραίτητα μέτρα, ώστε να προστατεύουν τις φορητές συσκευές και τις πληροφορίες που αυτές περιέχουν.
 - δεν θα πρέπει να αφήνουν ανεπιτήρητες τις φορητές συσκευές σε δημόσιους χώρους.
 - Όταν χρησιμοποιούν τις φορητές συσκευές σε δημόσιους χώρους, θα πρέπει να μεριμνούν ώστε να μην είναι εύκολη η ανάγνωση πληροφοριών από την οθόνη της συσκευής, από άτομα που βρίσκονται στον ίδιο χώρο.
 - Θα πρέπει να αναφέρουν άμεσα στον Υπεύθυνο Προστασίας Δεδομένων περιπτώσεις απώλειας ή κλοπής φορητής συσκευής.

Πολιτικές

- Πολιτική Προστασίας Προσωπικών Δεδομένων
- Πολιτική προστασίας προσωπικών δεδομένων των εργαζομένων
- Πολιτική για τη συλλογή και τη χρήση ευαίσθητων προσωπικών δεδομένων
- Πολιτική/ διαδικασίες για τη διατήρηση αρχείων
- Πολιτική για τη διατήρηση της ποιότητας των δεδομένων
- Πολιτική για τη διαγραφή των προσωπικών δεδομένων
- Πολιτική για δευτερεύουσες χρήσεις προσωπικών δεδομένων
- Πολιτική Cookies και των μηχανισμών παρακολούθησης
- Πολιτική για ασφαλή καταστροφή προσωπικών δεδομένων
- Πολιτική για την απόκτηση έγκυρης συναίνεσης
- Πολιτική Συνεργατών



Πολιτική Συνεργατών

- Η Πολιτική περιγράφει τη δέσμευση του Πανεπιστημίου ως προς τη διαχείριση των συνεργατών του
- Οι συνεργάτες πρέπει να συμμορφώνονται με τις απαιτήσεις του Πανεπιστημίου αναφορικά με την προστασία των προσωπικών δεδομένων



Πολιτική Συνεργατών

- Οι προϊστάμενοι αρμόδιων Διευθύνσεων/Τμημάτων του Πανεπιστημίου πληροφορούν τον Υπεύθυνο Προστασίας Δεδομένων πριν τη συνεργασία με τρίτο μέρος
- Αξιολογείται η νέα συνεργασία, κατηγοριοποιείται ο ρόλος του συνεργάτη (π.χ. Εκτελών την Επεξεργασία, Από Κοινού Υπεύθυνος, Αποδέκτης) και καταρτίζεται σύμβαση που περιέχει όρους επεξεργασίας προσωπικών δεδομένων
- Το Πανεπιστήμιο δύναται να ζητήσει από το συνεργάτη του τεκμηρίωση της συμμόρφωσης του με το GDPR
- Ενημέρωση του «Αρχείου Δραστηριοτήτων Επεξεργασίας» με τα στοιχεία του τρίτου μέρους στην αντίστοιχη δραστηριότητα επεξεργασίας.
- Ενημέρωση του «Μητρώου Εκτελούντων την Επεξεργασία»
- Σε περιοδική βάση ανασκοπούνται οι συνεργασίες με τρίτα μέρη



Παραδείγματα συνεργασιών

*(σύμφωνα με το Αρχείο
Δραστηριοτήτων Επεξεργασίας)*

- Ψυχολόγος
- Εταιρεία παροχής εφαρμογής MyCloud (Western Digital) EASY SMS
- Εξωτερικός Συνεργάτης (π.χ. τυπογραφείο, φωτογράφος)
- OTS Α.Ε.
- Microsoft (π.χ. για Teams)
- Διαφημιστικές Εταιρείες



Κώδικας Δεοντολογίας

- περιλαμβάνει άρθρα για την Προστασία Προσωπικών Δεδομένων



Λοιπά παραδοτέα στο πλαίσιο του έργου συμμόρφωσης με τον GDPR

- Αρχείο Δραστηριοτήτων
- Ανάλυση Αποκλίσεων – Πλάνο Ενεργειών
- Μελέτη Εκτίμησης Αντικτύπου για τη Προστασία Δεδομένων
- Αποτίμηση Επικινδυνότητας
- Υλικό Εκπαιδεύσεων
- Αναφορά Επιθεώρησης



Data Protection Officer – Υπεύθυνος Προστασίας δεδομένων

- ενημερώνει και συμβουλεύει το Πανεπιστήμιο και τους εργαζόμενους
- παρακολουθεί τη συμμόρφωση με τον κανονισμό και άλλες κανονιστικές απαιτήσεις
- αναθέτει αρμοδιότητες, ευθύνη για εκπαίδευση, ευαισθητοποίηση
- παροχή συμβουλών για την αξιολόγηση των επιπτώσεων και την υλοποίησή της
- συνεργάζεται και είναι το σημείο επαφής με την ΑΠΔΠΧ
- επικοινωνεί με φυσικά πρόσωπα για σχετικά θέματα/ διαχειρίζεται αιτήματα
- Υπεύθυνος για την επικαιροποίηση του Αρχείου Δραστηριοτήτων

Υποστηρικτική ομάδα DPO





Ρόλοι και ευθύνες ανάλογα τη θέση εργασίας

- Συμμετέχω στην δημιουργία /επικαιροποίηση του Αρχείου Δραστηριοτήτων (π.χ. Υπεύθυνοι Τμημάτων/Γραφείων)
- Συμμετέχω στην υλοποίηση κάποιας ενέργειας που προέκυψε μετά την ανάλυση Αποκλίσεων ή την Μελέτη Εκτίμησης Αντικτύπου (π.χ. Τμήμα Δικτύων Διαδικτύου)
- Εντοπίζω την ανάγκη δημιουργίας κειμένου συγκατάθεσης / πληροφόρησης
- Διαχειρίζομαι αιτήματα φυσικών προσώπων /διαβιβάζω στον DPO (π.χ. Γραμματείες Τμημάτων)
- Ενημερώνω σε περίπτωση που εντοπίζω περιστατικό Παραβίασης
- Έδιευκολύνω διαδικασία Εσωτερικών επιθεωρήσεων ή Ελέγχων από την Αρχή (ΑΠΔΠΧ)
- Μελετώ και ακολουθώ τις διαδικασίες και τις Οδηγίες του Προγράμματος

