

Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 2016/679 GDPR

T. +30 210 3611 225, +30 210 3611
236,

F. +30 210 3610 227

Email: i.chioni@kanell.gr

a.pavlou@kanell.gr

www.kanell.gr

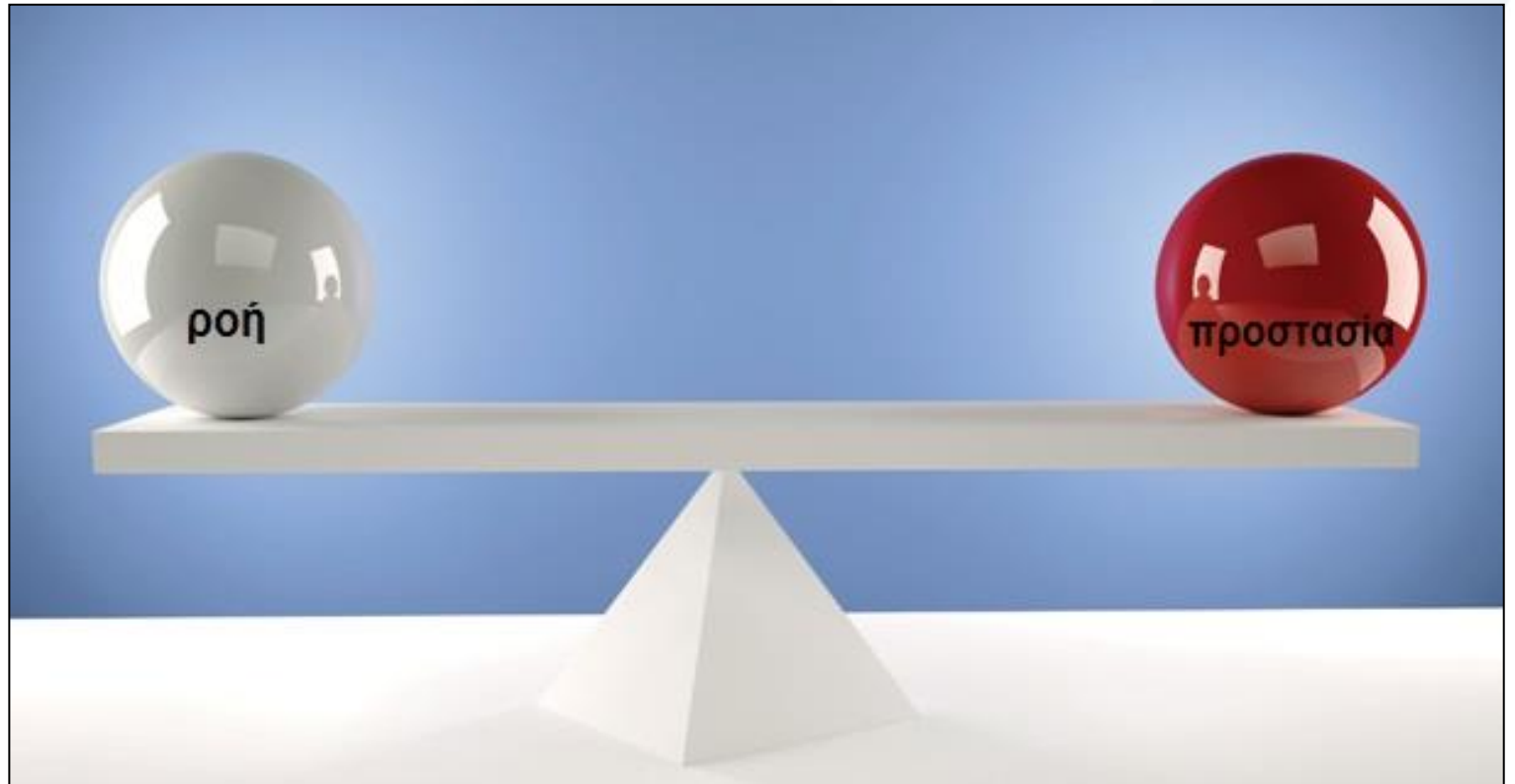
Έηρα Χιώνη
Αναστασία Παύλου

Θέματα Σεμιναρίου

1. Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR)
2. Βασικές Αρχές Επεξεργασίας Δεδομένων – Νόμιμες Βάσεις Επεξεργασίας
3. Case studies
4. Βήματα Συμμόρφωσης με τον Κανονισμό



Προστασία + Ροή
Δεδομένων
Προσωπικού
Χαρακτήρα



Οδηγία 95/46 ΕΚ

Από την οδηγία 95/46 ΕΚ στον Κανονισμό

Ο Κανονισμός στηρίζεται στην κοινοτική οδηγία 95/46/ΕΚ, διατηρεί ρυθμίσεις της οδηγίας.

Εισάγει νέες έννοιες, επικαιροποιεί δικαιώματα και εισάγει νέα (δικαίωμα στη λήθη – φορητότητα), προβλέπει νέες υποχρεώσεις για τους υπευθύνους επεξεργασίας.

Τεχνολογία

Ραγδαία ανάπτυξη
Διαδικτύου

Υπηρεσίες κοινωνικής
δικτύωσης

Επεξεργασία
μεγαδεδομένων
(megadata)

Νεφοϋπολογιστική
(Cloud computing)

Συστήματα
Γεωεντοπισμού (gps)

Τεχνολογία RFID



**Αύξησαν την ένταση της επεξεργασίας προσωπικών δεδομένων και έκαναν
επιτακτική την ενίσχυση της προστασίας των δεδομένων και της ιδιωτικής ζωής.**

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων-GDPR).

Ο Κανονισμός κατατέθηκε το 2012 και κατόπιν 4ετούς διαπραγμάτευσης ψηφίσθηκε τίθεται σε ισχύ την 25/5/18. Ο Κανονισμός έχει άμεση ισχύ σε όλα τα Κράτη της Ε.Ε.

173 σκέψεις και 99 άρθρα – έκταση 5 φορές μεγαλύτερη από την οδηγία 95/46/ΕΚ

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Ουσιαστικό
και Εδαφικό

Ουσιαστικό (άρθρο 2ΓΚΠΔ)

Ο Κανονισμός εφαρμόζεται στην,
εν όλω ή εν μέρει,
αυτοματοποιημένη ή μη
επεξεργασία δεδομένων
προσωπικού χαρακτήρα φυσικών
προσώπων.

Εδαφικό (άρθρο 3 ΓΚΠΔ)

Εφαρμογή σε Υπευθύνους Επεξεργασίας και Εκτελούντες την Επεξεργασία που λαμβάνει χώρα εντός ΕΕ.

Καταλαμβάνει και δραστηριότητες εγκαταστάσεως υπευθύνου ή εκτελούντος την επεξεργασία εκτός Ε.Ε. όταν η επεξεργασία αφορά σε υποκείμενα που βρίσκονται εντός Ε.Ε. κι οι δραστηριότητες σχετίζονται με:

α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή

β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης (δραστηριότητες e-commerce και profiling)

Κατηγορίες Δεδομένων

- Δεδομένα προσωπικού χαρακτήρα.
- Ειδικές κατηγορίες προσωπικών δεδομένων (ευαίσθητα προσωπικά δεδομένα).

Προσωπικά Δεδομένα

Κάθε πληροφορία που αφορά σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου» (άρθρο 4 αριθ. 1 ΓΚΠΔ).

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα) – άρθρο 9 ΓΚΠΔ

Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό

Βασικοί ορισμοί (άρθρο 4 ΓΚΠΔ)

Επεξεργασία

*Υπεύθυνος
επεξεργασίας*

*Εκτελών την
επεξεργασία*

*Υποκείμενα των
Δεδομένων*

Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (πρέπει να συντρέχουν σωρευτικά)

1) νομιμότητα,
αντικειμενικότητα
και διαφάνεια

2) περιορισμός
του σκοπού

3) ελαχιστοποίηση
των δεδομένων

4) Ακρίβεια

5) περιορισμός
της περιόδου
αποθήκευσης

6) ακεραιότητα
και
εμπιστευτικότητα

7) λογοδοσία

Νομιμότητα της Επεξεργασίας

Θεμέλιο μία τουλάχιστον προϋπόθεση του άρθρου 6 (διαζευκτικά):

1. **Συγκατάθεση** του υποκειμένου των δεδομένων – ορισμός (άρθρο 4, αριθ. 11)

Εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα (λ.χ. εργαζόμενοι)

Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα.

Συγκατάθεση στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα → το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι **σαφώς διακριτό** από τα άλλα θέματα, σε **κατανοητή** και **εύκολα προσβάσιμη μορφή**, χρησιμοποιώντας **σαφή και απλή διατύπωση** (π.χ. εγγραφή σε newsletter)

Νομιμότητα της Επεξεργασίας

Δικαίωμα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή.

Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.

Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της.

Νομιμότητα της Επεξεργασίας

2. Η επεξεργασία είναι σύνηθες όταν είναι **απαραίτητη για την εκτέλεση σύμβασης**

3. η επεξεργασία είναι απαραίτητη για τη **συμμόρφωση με έννομη υποχρέωση** του υπευθύνου επεξεργασίας (λ.χ. τακτοποίηση αυθαιρέτων)

4. η επεξεργασία είναι απαραίτητη για τη **διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων** ή άλλου φυσικού προσώπου

Νομιμότητα της Επεξεργασίας

5. η επεξεργασία είναι απαραίτητη για την **εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον** ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας

6. η επεξεργασία είναι απαραίτητη για τους σκοπούς των **έννομων συμφερόντων** που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης μπορεί να θεωρηθεί ότι διενεργείται χάριν έννομου συμφέροντος

Νομιμότητα της Επεξεργασίας (Ευαίσθητα προσωπικά δεδομένα)

Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα εμπίπτει στον κανόνα της απαγόρευσης, από τον οποίο προβλέπονται εξαιρέσεις.

Διαφορά άρθρου 9 ΓΚΠΔ από τη ρύθμιση του ν. 2472/1997:

Δεν είναι υποχρεωτική η λήψη άδειας από την εποπτική αρχή
(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - ΑΠΔΠΧ).

Ο υπεύθυνος επεξεργασίας, διαπιστώνει τη συνδρομή των προϋποθέσεων για την επεξεργασία και φέρει ανάλογη ευθύνη (σκέψη 51)

Αρχή της Λογοδοσίας (Accountability)

❖ Μεταστροφή του βάρους απόδειξης

Πλέον ο Υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τον Κανονισμό.

Παράδειγμα:

Σύστημα βιντεοεπιτήρησης (κάμερες).
Καταργείται η γνωστοποίηση στην ΑΠΔΠΧ,
παραμένουν οι υποχρεώσεις.

Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει (**λογοδοσία**) ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό.

Δικαιώματα & Υποχρεώσεις

*Δικαιώματα
υποκειμένου
δεδομένων*

*Υποχρεώσεις
υπεύθυνου
επεξεργασίας*

Δικαιώματα του Υποκειμένου των Δεδομένων

Δικαίωμα
ενημέρωσης

Δικαίωμα
πρόσβασης

Δικαίωμα
διόρθωσης

Δικαίωμα
διαγραφής
(δικαίωμα στη
λήθη)

Δικαίωμα
περιορισμού της
επεξεργασίας

Δικαίωμα στην
φορητότητα των
δεδομένων

Δικαίωμα
εναντίωσης

Δικαίωμα στην
ανθρώπινη
παρέμβαση

Υποχρέωση τήρησης αρχείων επεξεργασίας (άρθρο 30 ΓΚΠΔ)

Περιεχόμενο

Στοιχεία υπευθύνου

Σκοποί επεξεργασίας

Κατηγορίες υποκειμένων και δεδομένων

Κατηγορίες αποδεκτών- διαβιβάσεις σε τρίτη χώρα

Προθεσμίες διαγραφής (όπου είναι δυνατό)

Γενική περιγραφή μέτρων ασφαλείας (όπου είναι δυνατό)

Εξαιρέσεις από υποχρέωση : < 250 άτομα εκτός αν συντρέχουν κίνδυνος, μη περιστασιακή επεξεργασία ή επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα

Γνωστοποίηση παραβίασης δεδομένων

Α) Στην ΑΠΔΠΧ

εντός 72 ωρών από τη γνώση του γεγονότος

Στη γνωστοποίηση αυτή αναφέρεται, κατ' ελάχιστο:

- α) η περιγραφή της φύσης της παραβίασης προσωπικών δεδομένων,
- β) το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας για πληροφορίες,
- γ) η περιγραφή των ενδεχόμενων συνεπειών από την παραβίαση δεδομένων,
- δ) η περιγραφή των μέτρων που λήφθηκαν ή πρόκειται να ληφθούν για την αντιμετώπιση της παραβίασης

Β) Στο υποκείμενο των δεδομένων

Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Διαβιβάσεις δεδομένων προς τρίτες χώρες ή διεθνείς οργανισμούς

Ως διασυνοριακή ροή δεδομένων νοείται η διαβίβαση ή μεταφορά δεδομένων προσωπικού χαρακτήρα εκτός ΕΕ ή/και ΕΟΧ

Όχι πλέον προϋπόθεση η λήψη άδειας από την ΑΠΔΠΧ, όπως στο ν. 2472/1997 αλλά **τήρηση διατυπώσεων** άρθρου 44 ΓΚΠΔ:

Α. Αποφάσεις επάρκειας (άρθρο 45).

Β. Κατάλληλες εγγυήσεις (όπως δεσμευτικοί εταιρικοί κανόνες ή οι τυποποιημένες ρήτρες προστασίας, οι εγκεκριμένοι κώδικες δεοντολογίας, συναίνεση υποκειμένου δεδομένων κλπ)

Υπεύθυνος Προστασίας Δεδομένων – ΥΠΔ (Data Protection Officer - DPO)

Πρόσωπο με ειδικές γνώσεις στο δίκαιο προστασίας των δεδομένων

Συνδρομή στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατά την παρακολούθηση της εσωτερικής συμμόρφωσης προς τον κανονισμό

Υποχρέωση Ορισμού όταν:

1. Η επεξεργασία διενεργείται από **δημόσια αρχή ή φορέα**
2. Βασική δραστηριότητα => επεξεργασία με **τακτική και συστηματική παρακολούθηση** των υποκειμένων των δεδομένων σε μεγάλη κλίμακα
3. **μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων** ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα

Υπεύθυνος Προστασίας Δεδομένων – ΥΠΔ (Data Protection Officer - DPO)

Καθήκοντα ΥΠΔ

1. Ενημερώνει και συμβουλεύει για τις υποχρεώσεις σχετικά με την προστασία δεδομένων
2. Παρακολουθεί τη συμμόρφωση με τον Κανονισμό κλπ
3. Παρέχει συμβουλές για την εκτίμηση αντικτύπου
4. Συνεργάζεται με ΑΠΔΠΧ
5. Αποτελεί σημείο επικοινωνίας για την ΑΠΔΠΧ
6. Πραγματοποιεί διαβουλεύσεις με την ΑΠΔΠΧ

Προσφυγές, ευθύνη και κυρώσεις

Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (άρθρο 77 ΓΚΠΔ)

Αν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία παραβιάζει τον κανονισμό

Δικαίωμα δικαστικής προσφυγής κατά νομικά δεσμευτικής απόφασης εποπτικής αρχής που το αφορά ή εφόσον η αρχή δεν εξετάσει την καταγγελία ή δεν ενημερώσει το υποκείμενο (άρθρο 78 ΓΚΠΔ) ή κατά Υπευθύνου ή εκτελούντος την επεξεργασία (άρθρο 79).

Δικαίωμα αποζημίωσης και αστική ευθύνη

Δικαίωμα του υποκειμένου για αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του κανονισμού.

Ο εκτελών την επεξεργασία ευθύνεται για τη ζημία που προκάλεσε η επεξεργασία μόνο εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του κανονισμού ή υπερέβη τις νόμιμες εντολές του υπευθύνου.

Αυστηρά διοικητικά πρόστιμα (άρθρο 83)

1η κατηγορία παραβάσεων - Έως **10.000.000** ή για επιχειρήσεις το **2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο

2η κατηγορία παραβάσεων - Έως **20.000.000** ή για επιχειρήσεις το **4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο

(ομοίως & για μη συμμόρφωση προς αποφάσεις Αρχής)

Case Studies

- Τακτοποίηση αυθαιρέτων
- Έκδοση Οικοδομικής Άδειας
- Κτηματολόγιο
- Ενεργειακά πιστοποιητικά
- Εξωτερικές Συνεργασίες
- Τεχνικός Ασφαλείας

Γενικά σημεία προσοχής

- ❖ Σημεία προσοχής
 - Πού αποθηκεύονται τα δεδομένα (φυσική/ ηλεκτρονική ασφάλεια)
 - Συλλογή μόνο των αναγκαίων στοιχείων
 - Διαβίβαση δεδομένων (τήρηση εμπιστευτικότητας)
 - Χρόνος τήρησης
 - Δέσμευση συνεργατών ή/και εργαζομένων (συμβατικές υποχρεώσεις)

Προετοιμασία επιχειρήσεων σε 10 βήματα (Οδηγίες ΑΠΔΠΧ)

1. ΕΝΗΜΕΡΩΣΗ - ΕΤΟΙΜΟΤΗΤΑ: Ενημερώστε το ανθρώπινο δυναμικό της Εταιρείας/ συνεργάτες για τις μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων.

2. ΚΑΤΑΓΡΑΦΗ: Οφείλετε να τηρείτε ειδικά αρχεία επεξεργασιών; Αν ναι, καταγράψτε ενδελεχώς τα δεδομένα που τηρείτε και διαβιβάζετε, τις επεξεργασίες στις οποίες προβαίνετε, τον σκοπό τους και τη νομική βάση.

3. ΕΛΕΓΧΟΣ ΤΗΡΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ: Εξετάζετε συνεχώς αν κατά την επεξεργασία των δεδομένων τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των υποκειμένων.

4. ΕΛΕΓΧΟΣ ΝΟΜΙΜΟΤΗΤΑΣ: Εξετάστε τις μεθόδους για εξασφάλιση νομιμότητας για κάθε επιδιωκόμενο σκοπό επεξεργασίας.

5. ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ: Θα πρέπει να είστε σε θέση να εκτιμήσετε τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.

Προετοιμασία επιχειρήσεων σε 10 βήματα (Οδηγίες ΑΠΔΠΧ)

6. ΔΗΜΙΟΥΡΓΙΑ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ: Κυρίως ιστοσελίδα (Πολιτική Απορρήτου, Πολιτική Cookies). Λοιπές Πολιτικές ανάλογα με την κλίμακα επεξεργασίας.

7. ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: Μόνο για μεγάλες επιχειρήσεις/ φορείς δημοσίου. Στις υπόλοιπες περιπτώσεις ορισμός υπεύθυνου επικοινωνίας

8. ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ: Υιοθετήστε μεθόδους για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων.

9. ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΕ: Αν διαβιβάζετε δεδομένα και σε τρίτες χώρες, επιλέξτε κάποιο μηχανισμό διαβίβασης, όπως δεσμευτικούς εταιρικούς κανόνες (BCRs), τυποποιημένες συμβατικές ρήτρες (SCCs), πιστοποιήσεις στο Privacy Shield (για τις ΗΠΑ).

10. ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ: Ασφαλής τήρηση προσωπικών δεδομένων τόσο σε ηλεκτρονικά όσο και σε φυσικά αρχεία.

Ερωτήσεις



Σας Ευχαριστούμε!!!