Υγιείς Εργασιακές Σχέσεις, Σύγχρονες Επιχειρήσεις

4η Συνάντηση Δικτύου Επαγγελματιών Εργασιακών Σχέσεων και Διεύθυνσης Ανθρώπινου Δυναμικού

Το έργο συγχρηματοδοτείται από την Κυπριακή Δημοκρατία και το Ευρωπαϊκό Κοινωνικό Ταμείο της Ευρωπαϊκής Ένωσης

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Κυπριακή Δημοκρατία

Διαρθρωτικά Ταμεία
της Ευρωπαϊκής Ένωσης στην Κύπρο

GDPR – Πρακτικές εισηγήσεις για επαγγελματίες στον Τομέα Διεύθυνσης Ανθρώπινου Δυναμικού

Ιωάννης Ε. Γιαννακάκης- Δικηγόρος LLM

DPO Academy – TUV Austria

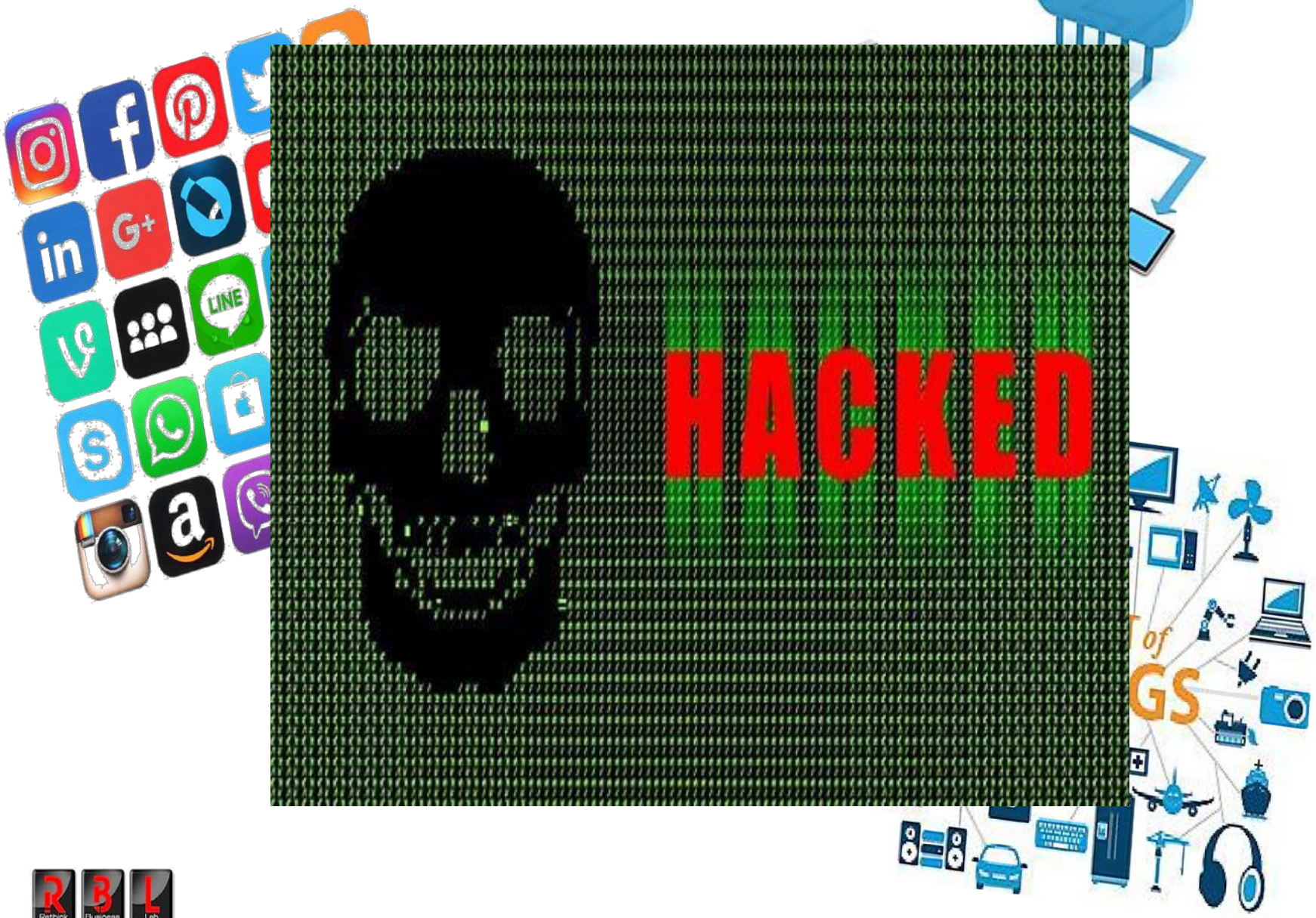
Το έργο συγχρηματοδοτείται από την Κυπριακή Δημοκρατία και το Ευρωπαϊκό Κοινωνικό Ταμείο της Ευρωπαϊκής Ένωσης

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

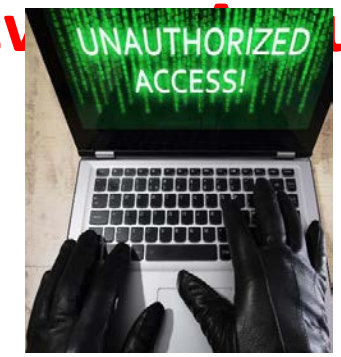
Κυπριακή Δημοκρατία

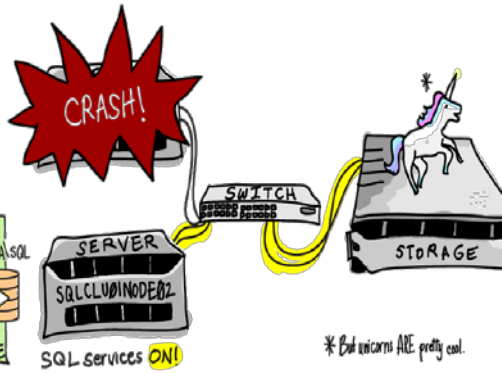
Διαρθρωτικά Ταμεία
της Ευρωπαϊκής Ένωσης στην Κύπρο

Not if
but when


HACKED
LINE

Η Ανατομία της Παραβίασης Δεδομένων - Βασικές





Η Ανατομία της Παραβίασης Δεδομένων

Κατηγορίες Παραβιάσεων & οι Επιπτώσεις:

Major Breach	DDoS	Semantic	Ransom	Fraud	Mechanic
Μαζική Διαρροή Δεδομένων	Υπερφόρτωση - Άρνηση εξυπηρέτησης	Αλλοίωση Δεδομένων	Κλείδωμα & «Ομηρία» Δεδομένων	Παραβίαση Οικονομικών Δεδομένων	Παραβίαση συστημάτων Ελέγχου
Αδυναμία Λειτουργίας – Πολλαπλές Επιπτώσεις	Αδυναμία Λειτουργίας	«Αλλοπρόσαλλα» Δεδομένα	Αδυναμία Λειτουργίας	Οικονομική Αδυναμία	Κίνδυνοι για φυσικές προσβάσεις & κίνδυνοι Υγείας

PROJECT MANAGEMENT ΠΡΟΓΡΑΜΜΑΤΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ GDPR

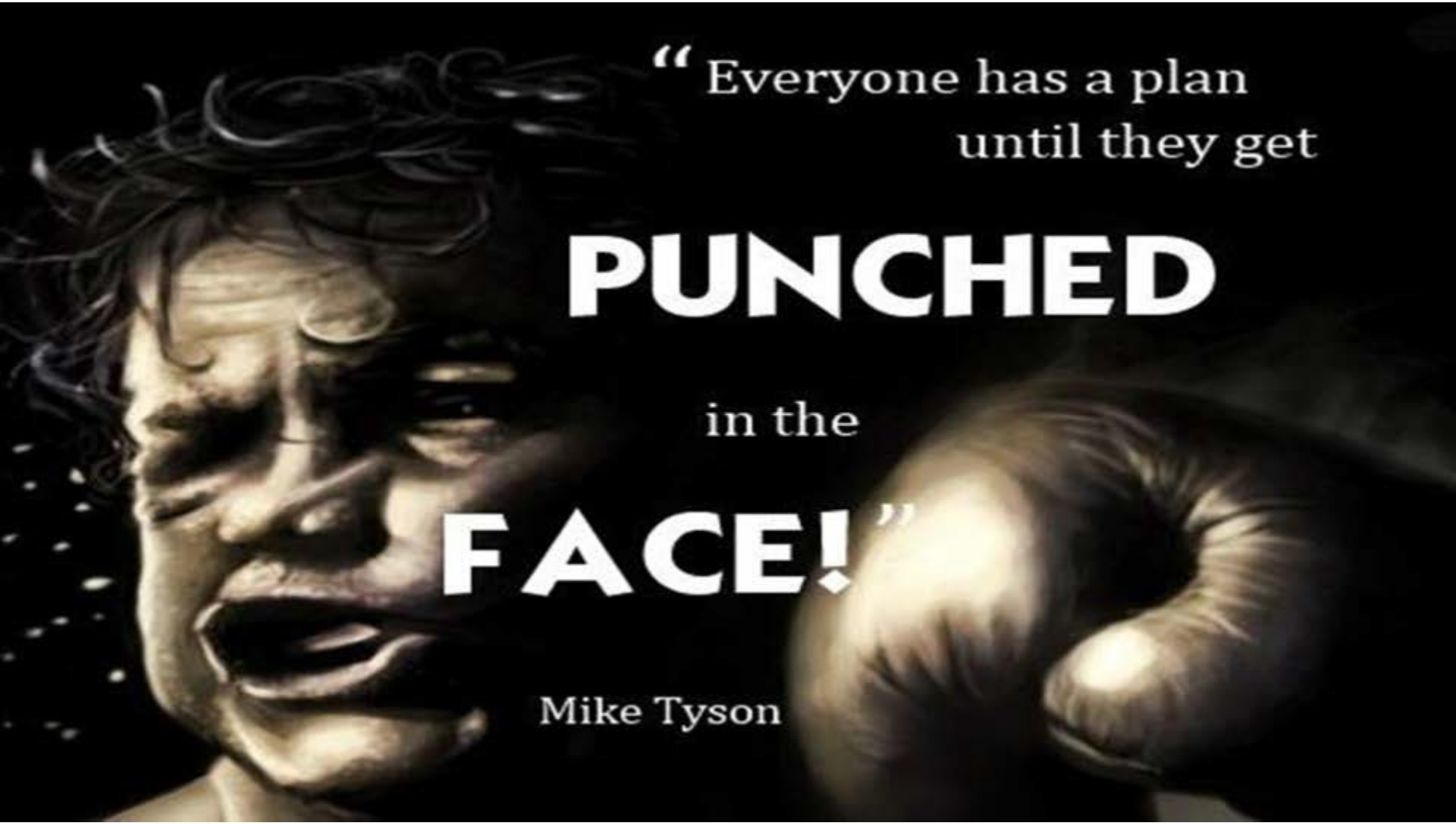
- **Αρθρο 24 Κανονισμού – Κατάλληλα οργανωτικά & τεχνικά μέτρα**

- Τα κατάλληλα οργανωτικά και τεχνικά μέτρα που θα εφαρμόσει η επιχείρηση θα πρέπει να είναι προσαρμοσμένα στην φύση των προσωπικών δεδομένων που θα τύχουν επεξεργασίας από αυτήν, ώστε να διασφαλίζεται η προστασία τους απο τυχόν παραβίασή τους και να ελαχιστοποιείται η ζημιά των υποκειμένων των δεδομένων αυτών σε περίπτωση παραβίασης
- Ο υπεύθυνος επεξεργασίας **πρέπει να λάβει τα κατάλληλα οργανωτικά μέτρα για να διασφαλίσει την αξιοπιστία των υπαλλήλων του** οι οποίοι θα έχουν πρόσβαση στα προσωπικά δεδομένα που θα τύχον επεξεργασίας απο τον υπεύθυνο επεξεργασίας ή **τους εκτελούντες αυτήν για λογαριασμό του**

PROJECT MANAGEMENT ΠΡΟΓΡΑΜΜΑΤΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ GDPR

Οι Επιχειρήσεις θα πρέπει να έχουν:

- **εκπαιδεύσει** κατάλληλα το ανθρώπινο δυναμικό τους
- σαφή **κατανομή ρόλων**, **αρμοδιότητων** και **ευθυνών** του ανθρώπινου δυναμικού για την επεξεργασία των προσωπικών δεδομένων
- **πολιτικές & διαδικασίες** προστασίας προσωπικών δεδομένων
- πλάνα **Data Recovery & Business Continuity** τα οποία μπορούν να εξασφαλίσουν την διαθεσιμότητα της πληροφορίας
- **Πλάνο Αντιμετωπίσης Περιστατικών Παραβίασης & Απώλειας προσωπικών δεδομένων (Incident Response Plan)** το οποίο θα επιτρέπει την οργανωμένη και συστηματική αντιμετώπιση οποιουδήποτε περιστατικού


" Everyone has a plan
until they get
PUNCHED
in the
FACE! "
Mike Tyson

PROJECT MANAGEMENT ΠΡΟΓΡΑΜΜΑΤΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ GDPR

1. Στόχοι (Goal and Objectives).
2. Εκτίμηση κατάστασης & κίνδυνοι (Assumptions and Risks).
3. Απαιτήσεις πόρων (Resources).
4. Υιοθέτηση πλαισίου κύκλου ζωής προστασίας ΔΠΧ (Data Protection Life-Cycle Framework).
5. ονοδιάγραμμα για τη συμμόρφωση (Time Plan).
6. Απαιτούμενες φάσεις.

Έτοιμοι για τον ΓΚΠΔ σε 12 βήματα

1. Διορίστε τα υπεύθυνα άτομα και – αν κριθεί απαραίτητο – ένα Υπάλληλο Προστασίας Δεδομένων («ΥΠΔ»)
2. Δημιουργείστε κατάλογο των διεργασιών επεξεργασίας προσωπικών δεδομένων και κάνετε μια ανάλυση διαφορών.
3. Εάν κριθεί απαραίτητο, διεξάγετε μια Εκτίμηση Αντικτύπου της Προστασίας Δεδομένων (ΕΑΠΔ)
4. Εισάγετε μια πολιτική ελαχιστοποίησης δεδομένων (αποφασίστε τις περιόδους κατακράτησης)
5. Καθιερώστε ένα μητρώο / διαχείριση και καταγράψτε τις διεργασίες επεξεργασίας
6. Ανανεώστε την πολιτική ασφαλείας σας και εφαρμόστε την Ιδιωτικότητα μέσω Σχεδιασμού και Ιδιωτικότητα μέσω Προεπιλογής
7. Ενσωματώστε εργαλεία για να σεβαστείτε τα νέα δικαιώματα των υποκειμένων των δεδομένων
8. Ανανεώστε την πολιτική ιδιωτικότητας
9. Σχεδιάστε ένα πρωτόκολλο παραβίασης και κρατήστε αρχείο
10. Ελέγξτε τους εκτελούντες την επεξεργασία και τα συμφωνητικά επεξεργασίας δεδομένων
11. Ανανεώστε τη ροή εγγραφών για να επιτύχετε έννομη συναίνεση
12. Βρείτε σε ποιά αρχή επιθεώρησης δίνετε αναφορά

Βήμα 1

Διορίστε τα υπεύθυνα άτομα και – αν κριθεί απαραίτητο – ένα Υπάλληλο Προστασίας Δεδομένων («ΥΠΔ»)

Αρχικά, είναι σημαντικό να αναγνωρίσετε ποιός, εντός του οργανισμού σας, είναι υπεύθυνος για τη συμμόρφωση όσον αφορά την ιδιωτικότητα, και ποιός άλλος συμπεριλαμβάνεται σε αυτό. Αυτά είναι τα κατ' αρχήν άτομα τα οποία είναι εξουσιοδοτημένα να λαμβάνουν αποφάσεις για σημαντικά θέματα εκ μέρους του οργανισμού, αλλά είναι επίσης άτομα που γνωρίζουν τη νομοθεσία, την τεχνολογία και την επεξεργασία δεδομένων εντός ενός οργανισμού. Είναι σημαντικό αυτοί οι άνθρωποι να αναγνωρίζουν τη σημασία της συμμόρφωσης με την Προστασία Προσωπικών Δεδομένων

- Οργανώστε μια συνάντηση έναρξης διεργασιών ή μια σειρά συναντήσεων με τα σχετικά άτομα. Αυτές μπορεί να περιλαμβάνουν:
  - Διοικητικό
  - Συμβούλιο
  - Αυτούς που χαράσσουν πολιτική
  - Δικηγόρους
  - Άλλα άτομα που σχετίζονται με τα προσωπικά δεδομένα όπως το προσωπικό
- HR , υποστήριξη πελατών, τμήμα IT κλπ.
- τους πληροφορίες σχετικά με τον ΓΚΠΔ και τη σημασία του για τη συμμόρφωση όσον αφορά την Προστασία Προσωπικών Δεδομένων
- Καθορίστε, σε γενικές γραμμές, τις πιο σημαντικές περιοχές/κινδύνους προσήλωσης για τον οργανισμό σας. Αυτό, εν μέρει, εξαρτάται από την κύρια δραστηριότητα του οργανισμού σας.
- Καθορίστε ποιός είναι υπεύθυνος για τη συμμόρφωση και πώς θα διανεμηθούν οι εργασίες. Πώς θα λαμβάνονται οι αποφάσεις; Πότε και σε ποιό βαθμό να πρέπει να αναμειγνύεται το Διοικητικό Συμβούλιο; Ποιός θα είναι υπεύθυνος και/ή αναμεμειγμένος στην εφαρμογή, κλπ.;

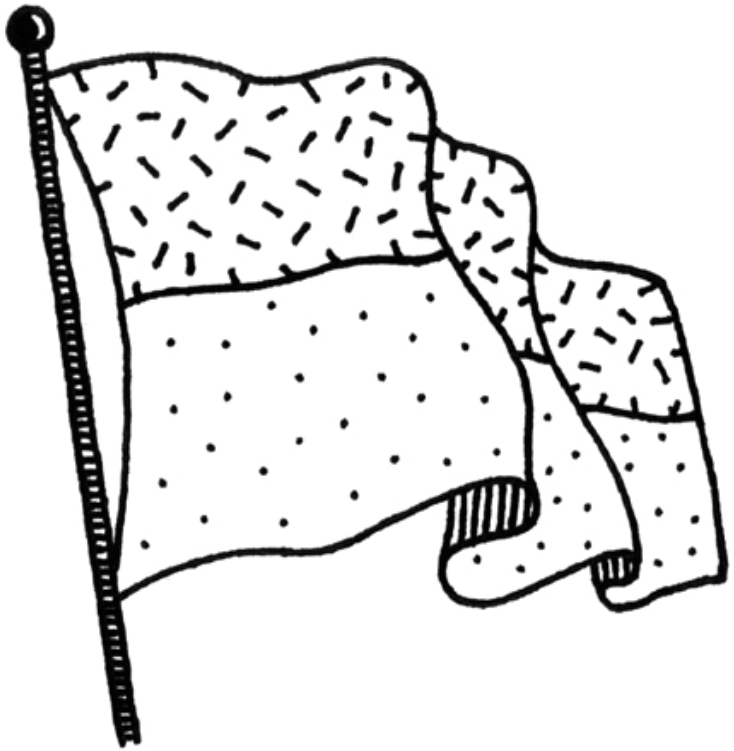
Υπεύθυνος Προστασίας Δεδομένων

Υπό τον ΓΚΠΔ ο οργανισμός σας δύναται να είναι υποχρεωμένος να διορίσει έναν Υπάλληλο Προστασίας Δεδομένων ή «ΥΠΔ». Ακόμη και εάν δεν είναι υποχρεωτικό, μπορείτε να διορίσετε έναν ΥΠΔ. Αποφασίστε τώρα εάν ο οργανισμός σας χρειάζεται έναν. Σε κάθε περίπτωση, οφείλετε να διορίσετε ΥΠΔ (i) εάν είστε δημόσια αρχή, (ii) εάν το αντικείμενο της εργασίας σας περιλαμβάνει διεργασίες επεξεργασίας που ανέρχονται σε τακτική και συστηματική παρατήρηση ατόμων σε μεγάλη κλίμακα, ή εάν (iii) η εργασία σας περιλαμβάνει την επεξεργασία ειδικών προσωπικών δεδομένων σε μεγάλη κλίμακα (δείτε **Βήμα 2**).

Ο ΥΠΔ είναι κάτι σαν εσωτερική αρχή επιθεώρησης. Ο ΥΠΔ ενημερώνει και συμβουλεύει τον οργανισμό σχετικά με τις υποχρεώσεις βάση του ΓΚΠΔ και λοιπών υποχρεώσεων στον τομέα της προστασίας δεδομένων, και εξασφαλίζει συμμόρφωση με τις υποχρεώσεις αυτές. Αυτός ή αυτή είναι επίσης το πρόσωπο-σύνδεσμος του οργανισμού με την αρχή επιθεώρησης και τα υποκείμενα των δεδομένων.

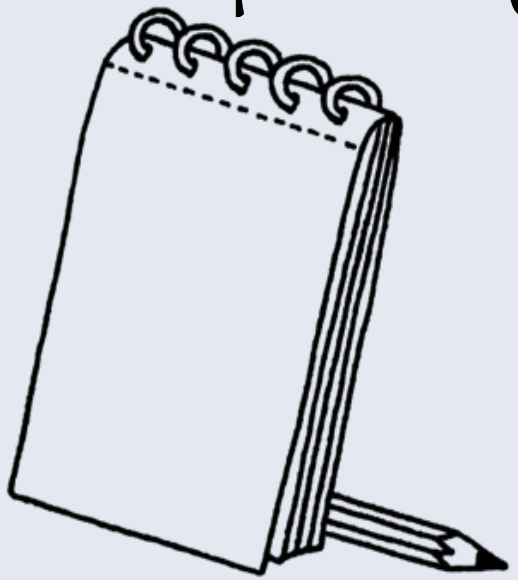
Για να διεξάγει τα καθήκοντα αυτά, ο ΥΠΔ οφείλει να είναι ειδήμων στους τομείς της νομοθεσίας και της πρακτικής που σχετίζεται με την προστασία των προσωπικών δεδομένων. Αυτός ή αυτή οφείλει επίσης να παράσχει επαρκή υποστήριξη και πόρους για την εφαρμογή τους και να έχει κάποιο βαθμό αυτονομίας.

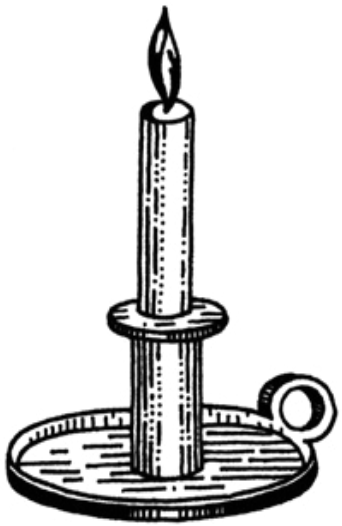
- Αποφασίστε εάν ο διορισμός ενός ΥΠΔ απαιτείται ή είναι επιθυμητός.
- Αποφασίστε ποιός πρέπει να είναι ο ΥΠΔ και εξασφαλίστε ότι το άτομο αυτό έχει επαρκή εκπαίδευση.
- Καθορίστε το σκοπό των καθηκόντων του ΥΠΔ και εξασφαλίστε ότι αυτός ή αυτή έχει επαρκή υποστήριξη και πόρους.
- Διορίστε τον ΥΠΔ και καταχωρίστε τον στην Αρχή Προστασίας Δεδομένων.



ΒΗΜΑ 3

- Εάν κριθεί απαραίτητο, διεξάγετε μια Εκτίμηση Αντικτύπου της Προστασίας Δεδομένων (ΕΑΠΔ)





Υπό τον ΓΚΠΔ μπορεί να είστε υποχρεωμένοι να διεξάγετε μια εκτίμηση αντικτύπου προστασίας δεδομένων («ΕΑΠΔ»). Η ΕΑΠΔ είναι ένα εργαλείο που σας επιτρέπει να δημιουργήσετε κατάλογο των διεργασιών επεξεργασίας προτού μια τέτοια διεργασία λάβει χώρα, ώστε να μπορούν να ληφθούν μέτρα απομείωσης των κινδύνων.

Πότε χρειάζεται μια ΕΑΠΔ;

Μια ΕΑΠΔ είναι απαραίτητη για τις (προβλεπόμενες) διεργασίες επεξεργασίας δεδομένων, οι οποίες, δεδομένης της φύσης τους, του περιεχομένου τους και του στόχου τους, παρουσιάζουν αυξημένους κινδύνους για την ιδιωτικότητα. Υπάρχει σίγουρα

αυξημένος κίνδυνος στις ακόλουθες περιπτώσεις αξιολογείτε άτομα βάση των προσωπικών χαρακτηριστικών τους και βασίζετε τις αποφάσεις στα χαρακτηριστικά αυτά. Αυτό περιλαμβάνει τη δημιουργία προφίλ και προβλέψεων.

●Εάν επεξεργάζεστε ευαίσθητα προσωπικά δεδομένα, όπως δεδομένα που σχετίζονται με την υγεία, ποινικά δεδομένα ή πολιτικές προτιμήσεις, σε μεγάλη κλίμακα.

●Εάν παρακολουθείτε ανθρώπους σε δημόσιους χώρους συστηματικά και σε μεγάλη κλίμακα (π.χ. Παρακολούθηση μέσω καμερών).

Σε όλες τις υπόλοιπες περιπτώσεις οφείλετε να αποφασίσετε εάν μια διεργασία εμπεριέχει «υψηλό κίνδυνο». Εάν η διεργασία επεξεργασίας σας πληροί δύο ή περισσότερα από τα παρακάτω κριτήρια, μπορείτε να θεωρήσετε ότι οφείλετε να διεξάγετε μια ΕΑΠΔ:

●Δημιουργείτε προφίλ ατόμων.

●Λαμβάνετε αυτόματες αποφάσεις που επηρεάζουν φυσικά το υποκείμενο δεδομένων.

- Διεξάγετε συστηματική παρακολούθηση σε μεγάλη κλίμακα.
- Επεξεργάζεστε ευαίσθητα προσωπικά δεδομένα.
- Διεξάγετε επεξεργασία δεδομένων σε μεγάλη κλίμακα, πχ επεξεργασία που περιλαμβάνει πολλά άτομα, πολλά δεδομένα, μεγάλη χρονική περίοδο ή μεγάλη περιοχή.
- Συνδυάζετε ή συσχετίζετε διαφορετικές συλλογές δεδομένων.
- Επεξεργάζεστε δεδομένα που σχετίζονται με ευάλωτα άτομα, όπως παιδιά, εργαζόμενοι, ή ασθενείς.
- Χρησιμοποιείτε νέες τεχνολογίες, πχ εφαρμογές Internet of Things (IoT).
- Μεταβιβάζετε προσωπικά δεδομένα σε χώρες εκτός της Ε.Ε.
- Η διεργασία επεξεργασίας δεδομένων σημαίνει ότι τα άτομα δεν μπορούν να ασκήσουν ένα δικαίωμά τους, να χρησιμοποιήσουν μια υπηρεσία ή να εισέλθουν σε συμβόλαιο.

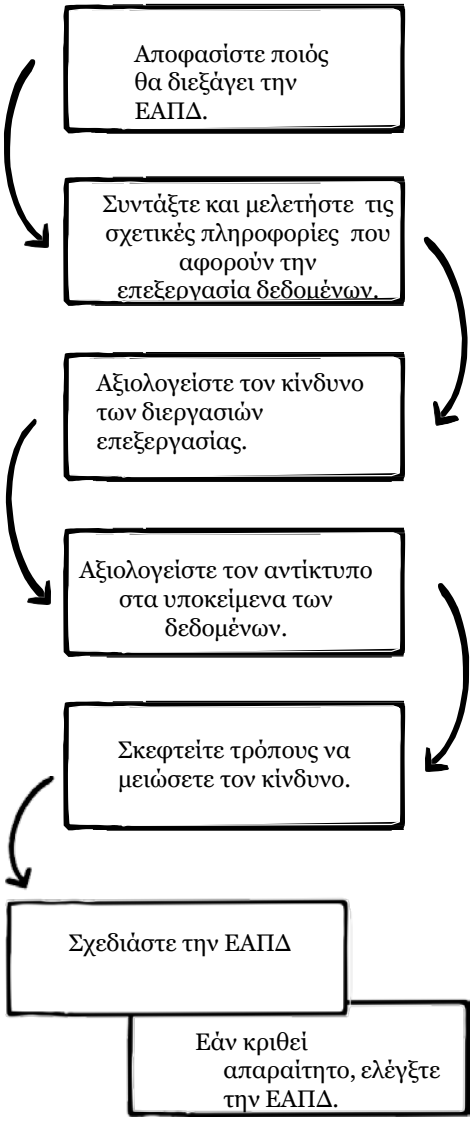
Η Αρχή Προστασίας Δεδομένων θα δημοσιεύσει μια λίστα διεργασιών επεξεργασίας για τις οποίες η ΕΑΠΔ είναι υποχρεωτική.

Πώς πρέπει να διεξάγω μια ΕΑΠΔ;

Μπορείτε να διαλέξετε εσείς πώς θα διεξάγετε την ΕΑΠΔ, αλλά θα πρέπει πάντοτε να περιλαμβάνει τα ακόλουθα:

- Συστηματική περιγραφή των προβλεπόμενων διεργασιών επεξεργασίας δεδομένων και των σκοπών των διεργασιών αυτών. Εάν στηρίζεστε σε εύλογο ενδιαφέρον ως βάση για την επεξεργασία, οφείλετε να εξηγήσετε το ενδιαφέρον αυτό στην περιγραφή.
- Αξιολόγηση της ανάγκης και της αναλογικότητας των διεργασιών επεξεργασίας. Είναι η διεργασία επεξεργασίας απαραίτητη για την επίτευξη του στόχου σας; Και είναι η παραβίαση ιδιωτικότητας αναλογική σε σχέση με το στόχο αυτό;
- Εκτίμηση των κινδύνων ιδιωτικότητας για τα υποκείμενα των δεδομένων.
- Τα προτεινόμενα μέτρα για (I) την αντιμετώπιση κινδύνων (όπως η χρήση ψευδωνύμων) και (II) την επίδειξη συμμόρφωσης με τον ΓΚΠΔ.

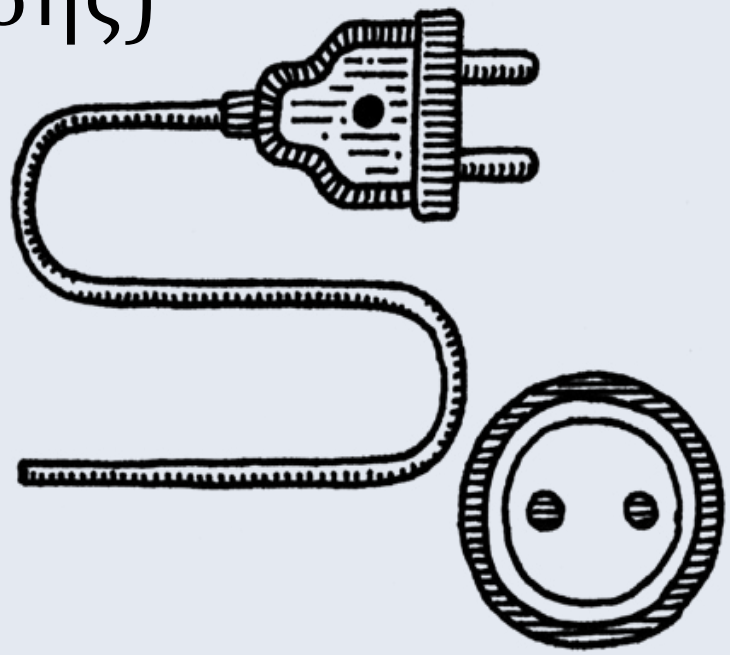
Έχει η ΕΑΠΔ αποκαλύψει ότι η προβλεπόμενη επεξεργασία εμπεριέχει υψηλό κίνδυνο; Και είστε ανίκανοι να βρείτε μέτρα για να περιορίσετε τον κίνδυνο αυτό; Στην περίπτωση αυτή, οφείλετε να συζητήσετε για τα θέματα αυτά με την Αρχή Προστασίας Δεδομένων προτού ξεκινήσετε με τις διεργασίες επεξεργασίας. Αυτό ονομάζεται προγενέστερη γνωμοδότηση. Στο στάδιο αυτό αξιολογείστε εάν πρέπει να διεξάγετε ΕΑΠΔ, και κάντε το. Εάν δράσετε γρήγορα, θα είναι πιο εύκολο για εσάς να συμμορφωθείτε με τις υπόλοιπες υποχρεώσεις σύμφωνα με τον ΓΚΠΔ.



ΒΗΜΑ 4

Εισάγετε μια πολιτική ελαχιστοποίησης

- δεδομένων (αποφασίστε τις περιόδους κατακράτησης)



Ο ΓΚΠΔ δίνει έμφαση στην υποχρέωση να μη γίνεται επεξεργασία περισσότερων προσωπικών δεδομένων απ' ότι είναι απαραίτητο. Αυτό αναφέρεται επίσης και ως ελαχιστοποίηση δεδομένων. Υπό αυτό το πλαίσιο είναι σημαντικό να καθορίσουμε πόσο χρονικό διάστημα θα παρακρατάτε τα προσωπικά δεδομένα και να εξασφαλίσετε ότι τα δεδομένα θα αφαιρούνται εγκαίρως.

Τι χρειάζεται να κάνετε;

●Βάση της επισκόπησης που δημιουργήσατε για τα διάφορα δεδομένα (δείτε **Βήμα 2**), καθορίστε για ποιούς σκοπούς τα χρησιμοποιείτε και για πόσο καιρό θα πρέπει να τα παρακρατάτε για τους σκοπούς

- Υπάρχει μέγιστη ή ελάχιστη θεσμοθετημενη περίοδος παρακράτησης (για κάθε τύπο εγγράφου / πληροφορίας); Για παράδειγμα:
  - Προσωπικά δεδομένα από αιτούντες εργασία: μέγιστη διάρκεια 4 εβδομάδες μετά τη λήξη της διαδικασίας αιτήσεων.
  - Συμβόλαια εργασίας για τους εργαζομένους: μέγιστη διάρκεια 2 έτη από τη λήξη της σύμβασης.
  - Δηλώσεις εισοδήματος και αντίγραφο ταυτότητας εργαζομένων: ελάχιστη διάρκεια 5 έτη από τη λήξη της σύμβασης.
  - Καταγραφές από κλειστό σύστημα τηλεόρασης: μέγιστη διάρκεια 4 εβδομάδες από τη δημιουργία της καταγραφής.
- Υπάρχει ανάγκη παρακράτησης προσωπικών δεδομένων; Μήπως μπορούν κάποια δεδομένα να διαγραφούν από τη βάση δεδομένων;
- Μπορεί να γίνει χρήση ψευδωνύμων στα δεδομένα;
- Καθορίστε την περίοδο παρακράτησης, το αρχικό σημείο για το χρονικό όριο, και πώς η περίοδος παρακράτησης θα εφαρμόζεται
- .
  για παράδειγμα, πότε και για πόσο καιρό αρχειοθετούνται τα φυσικά έγγραφα (π.χ. Στο τέλος κάθε μήνα σε φάκελο με ημερομηνία δημιουργίας και ημερομηνία καταστροφής) και ποιός θα είναι υπεύθυνος για την καταστροφή.
  •Δημιουργείστε ρυθμίσεις για την (τεχνική) αρχειοθέτηση ή διαγραφή κάθε εφαρμογής/βάσης δεδομένων, συμπεριλαμβανομένων ρυθμίσεων για τη διαγραφή των αρχειοθετημένων δεδομένων.

ΒΗΜΑ 5

- Καθιερώστε ένα μητρώο / διαχείριση και καταγράψτε τις διεργασίες επεξεργασίας

Ο ΓΚΠΔ εισάγει τις υποχρεώσεις για τους οργανισμούς οι οποίοι είναι ξεκάθαρα και πλήρως υπεύθυνοι και υπόλογοι για τον τρόπο με τον οποίο χειρίζονται τα προσωπικά δεδομένα. Οφείλετε να είστε σε θέση να επιδείξετε ότι ο οργανισμός σας λειτουργεί σε συμφωνία με τον ΓΚΠΔ. Ως μέρος αυτού οφείλετε να κρατάτε αρχείο όλων των διεργασιών επεξεργασίας εντός του οργανισμού ή υπό την ευθύνη του οργανισμού. Οι αρχές επιθεώρησης δύναται να απαιτήσουν να έχουν πρόσβαση στο αρχείο αυτό.

Μπορείτε να χρησιμοποιήσετε την επισκόπηση που δημιουργήσατε στο **Βήμα 2** ως βάση για αυτό.

Τα ακόλουθα δεδομένα οφείλουν να καταγραφούν στο αρχείο:

●Όνομα και στοιχεία επικοινωνίας του υπεύθυνου ατόμου (αναφερόμενο στον ΓΚΠΔ ως ο «υπεύθυνος επεξεργασίας»)

●Όνομα και στοιχεία επικοινωνίας του αντιπροσώπου και/ή του ΥΠΔ, όπου αυτό εφαρμόζεται

●Σκοποί επεξεργασίας

●Κατηγορίες των υποκειμένων των δεδομένων

●Κατηγορίες των προσωπικών δεδομένων

●Τυχόν παραλήπτες

- Μεταφορές, όπου εφαρμόζεται, συμπεριλαμβανομένου του ονόματος της οντότητας ή του ατόμου που μεταφέρονται τα δεδομένα και καταγραφή που σχετίζεται με τις κατάλληλες εγγυήσεις:

●Περίοδοι κατακράτησης

- Μια γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας.

Συνεπώς, να μην παραλείψετε να καθιερώσετε ένα τέτοιο αρχείο και να το κρατάτε ενήμερο. Αυτό μπορεί να γίνει μέσω ενσωμάτωσης μιας εφαρμογής χαρτογράφησης δεδομένων, αλλά επίσης και μια επισκόπηση σε ένα αρχείο Excel.

Υπάρχουν και άλλα διαφορετικά εργαλεία στην αγορά τα οποία μπορούν να σας βοηθήσουν να επιτύχετε συμμόρφωση με αυτή την υποχρέωση.

Παρακαλώ σημειώστε: η υποχρέωση αυτή δεν ισχύει για οργανισμούς με λιγότερους από 250 εργαζομένους, αλλά ισχύει εάν (i) η διεργασία επεξεργασίας εμπεριέχει κινδύνους για τα υποκείμενα των δεδομένων, (ii) η διεργασία επεξεργασίας δεν είναι περιστασιακή ή, (iii) ειδικές κατηγορίες δεδομένων υπόκεινται επεξεργασία.

ΒΗΜΑ 6

Ανανεώστε την πολιτική ασφαλείας σας

- και εφαρμόστε την Ιδιωτικότητα μέσω Σχεδιασμού και Ιδιωτικότητα μέσω Προεπιλογής

Βάσει του ΓΚΠΔ οφείλετε να λάβετε «κατάλληλα τεχνικά και οργανωτικά μέτρα» για να ασφαλίσετε τα προσωπικά δεδομένα. Το τι θεωρείται κατάλληλο εξαρτάται από τους κινδύνους της επεξεργασίας. Οφείλετε να επιδείξετε ότι έχετε λάβει κατάλληλα μέτρα και ότι είστε σε θέση να κάνετε εύκολα κατανοητές τις εκτιμήσεις σας. Είναι, εν μέρει εξαιτίας αυτού, σημαντικό να ελέγχετε εάν η πολιτική ασφαλείας σας επιδεικνύει συμμόρφωση και να την ενημερώνετε

Ο ΓΚΠΔ .εισάγει υποχρεώσεις στον τομέα της Ιδιωτικότητας μέσω Σχεδιασμού και της Ιδιωτικότητας μέσω Προεπιλογής. Αυτό σημαίνει ότι τη στιγμή που θα διαλέξετε ένα μέσο για επεξεργασία δεδομένων ή όταν σχεδιάζετε συστήματα ή εφαρμογές, θα πρέπει να λαμβάνετε την προστασία προσωπικών δεδομένων υπόψη μέσω της ενσωμάτωσης μέτρων ασφαλείας και ελαχιστοποίηση δεδομένων, για παράδειγμα. Οι πρότυπες ρυθμίσεις οφείλουν να είναι έτσι ώστε προσωπικά δεδομένα μόνο να υπόκεινται επεξεργασία με συγκεκριμένο στόχο. Τα δικαιώματα αυτών που επηρεάζονται πρέπει να λαμβάνονται υπόψη

© όλες τις στιγμές, κάτι που περιλαμβάνει και κατά το σχεδιασμό της διεργασίας επεξεργασίας

Τι πρέπει να κάνετε:

●Για κάθε τύπο διεργασίας επεξεργασίας, κάνετε απογραφή των οργανωτικών και των τεχνικών μέτρων ασφαλείας τα οποία έχετε λάβει ή πρόκειται να λάβετε.

●Αξιολογήστε το κατά πόσο, δεδομένου του κινδύνου της επεξεργασίας και της κατάστασης της τεχνολογίας, αυτά είναι (ακόμη) επαρκή.

●Διερευνήστε εάν τα δεδομένα μπορούν να κρυπτογραφηθούν ή να γίνει χρήση ψευδωνύμων.

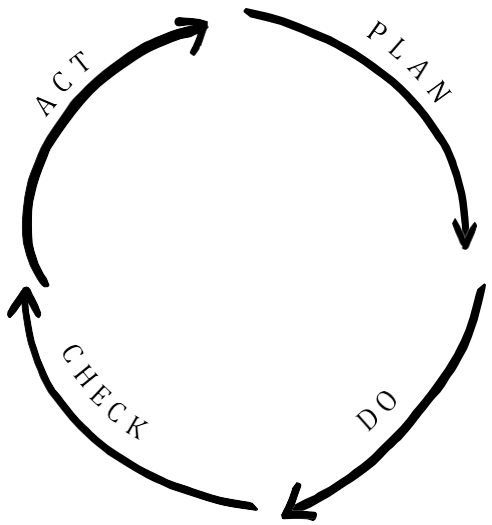
●Ελέγξτε εάν οι διεργασίες επεξεργασίας και/ή οι περίοδοι παρακράτησης μπορούν να περιοριστούν.

●Ελέγξτε εάν έχουν ενσωματωθεί μέτρα που εξασφαλίζουν τα δικαιώματα των υποκειμένων των δεδομένων (δείτε **Βήμα 7**).

●Ενσωματώστε επιπρόσθετα μέτρα όπου αυτό είναι απαραίτητο.

●Αποφασίστε πότε θα ελέγξετε και θα αξιολογήσετε τα μέτρα ασφαλείας σας.

●Δημιουργήστε μια πολιτική ασφαλείας η οποία περιγράφει τα μέτρα, τις αξιολογήσεις και την περιοδική αξιολόγηση.



Ο ΓΚΠΔ δίνει ιδιαίτερη σημασία στα δικαιώματα των υποκειμένων των δεδομένων. Για παράδειγμα, τα υποκείμενα των δεδομένων έχουν το δικαίωμα πρόσβασης και διόρθωσης των δεδομένων τους. Επιπλέον, δίνονται περισσότερες ευκαιρίες στα άτομα να έχουν το λόγο όσον αφορά την επεξεργασία των δεδομένων τους. Τα δικαιώματά τους ενισχύονται και επεκτείνονται.

Ο ΓΚΠΔ εισάγει μια σειρά νέων δικαιωμάτων όπως:

●Το δικαίωμα της λήψης αναλυτικής πληροφόρησης, με τον ΓΚΔΠ να εξειδικεύει ποιές πληροφορίες οφείλουν να βελτιώνονται σε κάθε περίπτωση (δείτε **Βήμα 8**).

●Το δικαίωμα στην ένσταση στη δημιουργία προφίλ και στην αυτόματη λήψη αποφάσεων

●Το δικαίωμα στη λήθη. Υπό κάποιες συνθήκες, τα άτομα έχουν το δικαίωμα να ζητήσουν τη διαγραφή των προσωπικών τους δεδομένων. Εάν ένας οργανισμός έχει δημοσιεύσει δεδομένα (π.χ. τα έχει δημοσιεύσει στο διαδίκτυο), πρέπει να ληφθούν εύλογα μέτρα για να μεταδοθεί η εντολή διαγραφής σε όλους τους οργανισμούς που επεξεργάζονται τα δεδομένα (υποχρέωση προώθησης).

●Το δικαίωμα στη φορητότητα των δεδομένων, ή στην ικανότητα μεταφοράς των προσωπικών δεδομένων. Τα άτομα αποκτούν το δικαίωμα – ανάλογα με τις συνθήκες – να λάβουν τα προσωπικά τους δεδομένα σε πρότυπη μορφή (format), ώστε αυτά να μπορούν εύκολα να μεταφερθούν σε άλλο προμηθευτή παρόμοιας υπηρεσίας. Για παράδειγμα, εάν επιθυμούν να απεγγραφούν από έναν ιστότοπο κοινωνικής δικτύωσης και να εγγραφούν σε έναν άλλο. Μπορούν να ζητήσουν από τον οργανισμό να στείλει τα προσωπικά τους στοιχεία στον καινούριο πάροχο υπηρεσιών, εάν αυτό είναι τεχνικά δυνατόν.

●Το δικαίωμα να απαγορέψουν την επεξεργασία των προσωπικών τους δεδομένων.

●Το δικαίωμα να μην υποστούν αποκλειστικά διαδικασία αυτόματης λήψης αποφάσεων, όπως η δημιουργία προφίλ.

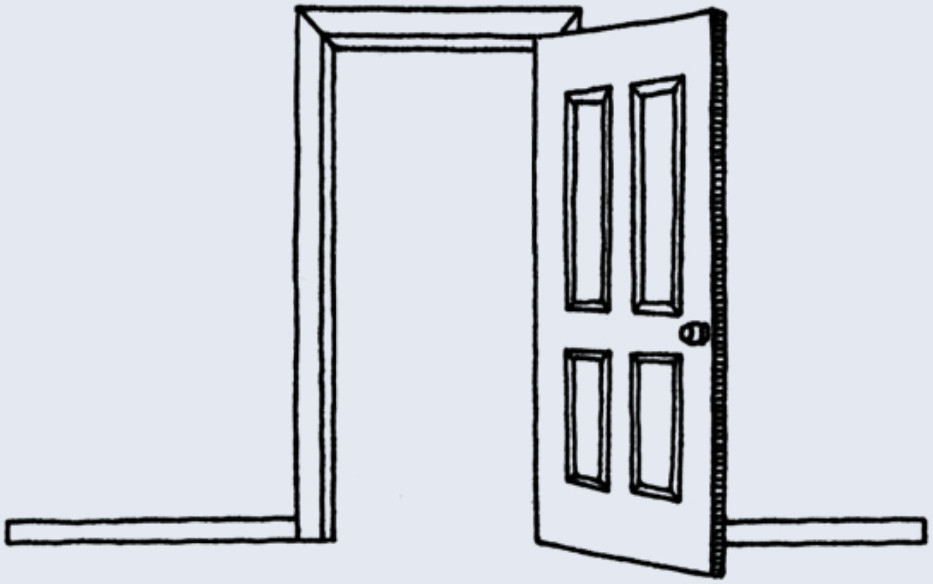
Ο ΓΚΠΔ περιέχει επίσης μια ξεχωριστή πρόβλεψη σχετικά με τη συναίνεση, για την οποία δείτε περισσότερα στο **Βήμα 9.**

Βλέπετε ότι υπάρχουν πολλά νέα δικαιώματα, τα οποία οφείλετε να σεβαστείτε. Συνεπώς, αξιολογείστε τις διαδικασίες απόκτησης πρόσβασης, κλπ., και καθορίστε τις συνθήκες ώστε τα άτομα να μπορούν να ασκήσουν τα δικαιώματά τους υπό τον ΓΚΠΔ εντός του οργανισμού σας. Καθορίστε εάν είναι κατάλληλη η ανάπτυξη τεχνικών πόρων για αυτό εντός του οργανισμού σας, όπως, για παράδειγμα, υπό το πλαίσιο της μεταφοράς δεδομένων. Οι πόροι αυτοί μπορεί να περιλαμβάνουν προγράμματα λήψης (download) που επιτρέπουν στα άτομα να λαμβάνουν εύκολα τα δεδομένα τους και την παροχή διεπιφανειών εφαρμογών προγραμμάτων (application programming interfaces, APIs).

ΒΗΜΑ 8

Ανανεώστε την πολιτική Απορρήτου

-
-



Υπό τον ΓΚΠΔ οφείλετε να ενημερώσετε τα υποκείμενα δεδομένων σχετικά με την επεξεργασία προσωπικών δεδομένων. Η ενημέρωση οφείλει να είναι περιεκτική, διαφανής, κατανοητή και εύκολα προσβάσιμη.

Υπό τον ΓΚΠΔ οφείλετε να παρέχετε πληροφορίες σχετικά, μεταξύ άλλων:

- Την ταυτότητά σας και τα στοιχεία επικοινωνίας σας, και εάν είναι δυνατό, αυτά του ΥΠΔ.
- Τους σκοπούς της επεξεργασίας και της νομικής βάσης αυτών των σκοπών.
- Τις κατηγορίες προσωπικών δεδομένων που επεξεργάζεστε.
- Η περίοδος αποθήκευσης των προσωπικών δεδομένων (δείτε **Βήμα 4**).
- Τα δικαιώματα του υποκειμένου του δεδομένου, όπως το δικαίωμα να καταθέσει παράπονο, το δικαίωμα στην πρόσβαση, διόρθωση και διαγραφή, και το δικαίωμα άρσης συναίνεσης σε οποιαδήποτε στιγμή (δείτε **Βήμα 7** και **11**).
- Την πηγή των δεδομένων.
- Τυχόν αποδέκτες ή κατηγορίες αποδεκτών των προσωπικών δεδομένων.
- Το κατά πόσο τα δεδομένα μεταφέρονται σε χώρες εκτός της Ε.Ε.
- Όπου εφαρμόζεται: πιο εύλογο συμφέρον εξυπηρετείται από την επεξεργασία.
- Εάν δημιουργείτε προφίλ, και εάν ναι, πώς επηρεάζεται το υποκείμενο των δεδομένων από αυτό.
- Εάν το υποκείμενο των δεδομένων υποχρεώνεται να παρέχει τα προσωπικά δεδομένα και ποιές είναι οι επιπτώσεις μη παροχής των δεδομένων αυτών.

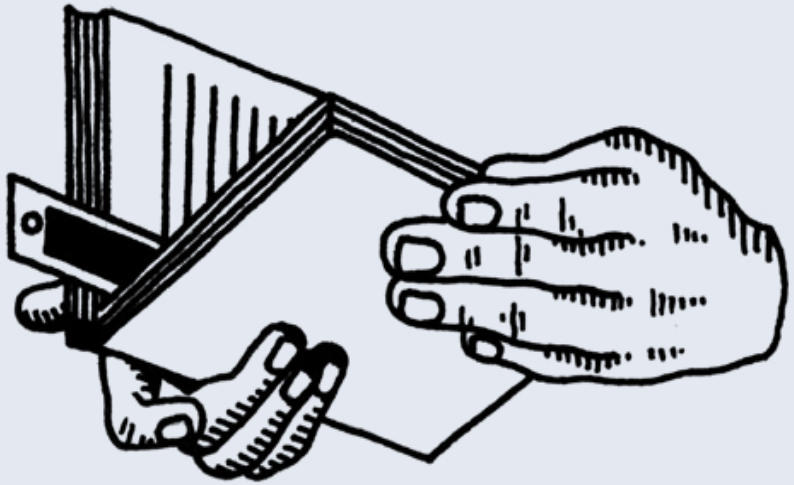
Ο ΓΚΠΔ προβλέπει επίσης τη μελλοντική χρήση πρότυπων εικόνων ώστε οι πληροφορίες να παρέχονται στους καταναλωτές με εύκολο τρόπο.

Οι πληροφορίες οφείλουν, κατά βάση, να παρέχονται τη στιγμή που συλλέγονται τα προσωπικά δεδομένα.

Είναι η ώρα, έτσι, να ενημερώσετε την πολιτική Απορρήτου ώστε να ενσωματώσετε τις επιπρόσθετες υποχρεώσεις όσον αφορά τα δεδομένα που εισάγει ο ΓΚΠΔ.

ΒΗΜΑ 9

Σχεδιάστε ένα πρωτόκολλο παραβίασης και κρατήστε αρχείο



Υπό τον ΓΚΠΔ δύναται να είστε υποχρεωμένοι να αναφέρετε μια παραβίαση δεδομένων στην αρμόδια αρχή και/ή στα υποκείμενα των δεδομένων. Μια παραβίαση δεδομένων αναφέρεται στην πρόσβαση ή καταστροφή, τροποποίηση ή αποκάλυψη προσωπικών δεδομένων σε έναν οργανισμό χωρίς αυτό να είναι εσκεμμένο. Η Παραβίαση Δεδομένων, συνεπώς, αφορά όχι μόνο την αποκάλυψη (παραβίαση) δεδομένων αλλά και την παράνομη επεξεργασία δεδομένων και την μη εσκεμμένη καταστροφή τους. Αυτό μπορεί να περιλαμβάνει την απώλεια ενός USB δίσκου που περιέχει προσωπικά δεδομένα, ένα κλεμμένο laptop, την παραβίαση ενός φακέλου δεδομένων από ένα χάκερ, ή μια πυρκαγιά που προκαλεί την απώλεια μιας CRM βάσης δεδομένων που δεν είχε αντίγραφο ασφαλείας.

Υπό τον ΓΚΠΔ είστε υποχρεωμένος να αναφέρετε οποιαδήποτε παραβίαση δεδομένων στην αρχή επιθεώρησης χωρίς καθυστέρηση, εντός 72 ωρών όπου αυτό είναι δυνατόν. Αυτό δεν είναι απαραίτητο εάν κριθεί ότι είναι απίθανο η παραβίαση δεδομένων να αποτελέσει σημαντικό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων. Το υποκείμενο των δεδομένων οφείλει να ενημερωθεί εάν μια παραβίαση δεδομένων είναι πιθανό να καταλήξει σε σημαντικό κίνδυνο για τα δικαιώματα και τις ελευθερίες του ατόμου, διαφορετικά αυτό δεν είναι απαραίτητο.

Πρωτόκολλο διαρροής δεδομένων

Για να είστε σε θέση να συμμορφωθείτε με τις προαναφερθείσες υποχρεώσεις, οφείλετε να εξασφαλίσετε ότι (i) είστε ενημερωμένοι για μια παραβίαση δεδομένων τη στιγμή που αυτή συμβεί και (ii)κάνατε τις κατάλληλες ενέργειες αμέσως. Όσον αφορά το πρώτο, οφείλετε να εξασφαλίσετε ότι εφαρμόζεται μέτρα που επισημαίνουν τις παραβιάσεις δεδομένων ως τμήμα της ασφάλειας (δείτε **Βήμα 6**). Όσον αφορά το δεύτερο μέρος, είναι σημαντικό να έχετε ένα πρωτόκολλο παραβίασης δεδομένων. Στο πρωτόκολλο αυτό μπορείτε να καταγράφετε (i) τα βήματα που πρέπει να ληφθούν εάν ο οργανισμός σας αντιμετωπίσει μια παραβίαση δεδομένων, (ii) ποιές πληροφορίες πρέπει να συλλεχθούν/καταγραφούν και/ή αναφερθούν, (iii) από ποιόν, και (iv) εντός ποιού χρονικού πλαισίου.

Επίσης, προβείτε σε ξεκάθαρες συμφωνίες με τους εκτελούντες την επεξεργασία σχετικά με τις παραβιάσεις δεδομένων. Ανακαλύψτε τι περιλαμβάνεται στο συμφωνητικό επεξεργασίας δεδομένων σχετικά με τις παραβιάσεις δεδομένων (δείτε επίσης το **Βήμα 10**).

Αρχείο καταγραφής παραβίασης δεδομένων

Επιπρόσθετα, ο ΓΚΠΔ επιβάλει το προαπαιτούμενο ότι όλες οι παραβιάσεις δεδομένων – αναφερθείσες ή μη – που έλαβαν χώρα εντός του οργανισμού σας, οφείλουν να καταγράφονται σε ένα αρχείο.

Βάση αυτού, η αρμόδια αρχή μπορεί να ελέγξει εάν έχετε συμμορφωθεί με την υποχρέωση της αναφοράς

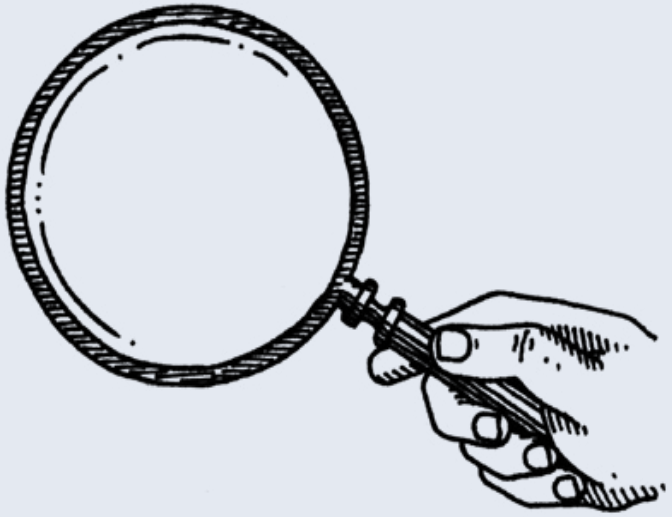
Ετοξυαςσ·φαλίστε ότι για κάθε παραβίαση δεδομένων καταγράφετε τις ακόλουθες πληροφορίες:

- Δεδομένα και λεπτομέρειες που σχετίζονται με τη φύση της παραβίασης δεδομένων.
- Τις κατηγορίες των ατόμων που επηρεάζονται και – όπου αυτό είναι δυνατόν – τον αριθμό των υποκειμένων των δεδομένων.
- Τον (πιθανό) αντίκτυπο της παραβίασης δεδομένων.
- Τα μέτρα που ο οργανισμός σας έχει λάβει για να αντιμετωπίσει την παραβίαση δεδομένων και να περιορίσει τον αντίκτυπό της.
- Έχει αναφερθεί η παραβίαση δεδομένων στην Αρχή;
- Έχει η παραβίαση δεδομένων αναφερθεί στο υποκείμενο των δεδομένων; Εάν ναι, συμπεριλάβετε το κείμενο της ειδοποίησης που δόθηκε στο υποκείμενο των δεδομένων κατά την επισκόπηση.

ΒΗΜΑ 10

Ελέγξτε τους εκτελούντες την

- επεξεργασία και τα συμφωνητικά επεξεργασίας δεδομένων



Ο εκτελών την επεξεργασία είναι ένα τρίτο πρόσωπο που επεξεργάζεται προσωπικά δεδομένα για λογαριασμό ενός οργανισμού. Αυτό μπορεί να περιλαμβάνει παρόχους υπηρεσιών που εκτελούν λογιστικά μισθοδοσίας, αλλά μπορεί επίσης να περιλαμβάνει όλων των ειδών υπηρεσίες IT ή cloud όπου ο πάροχος υπηρεσιών αποθηκεύει ή αποκτά πρόσβαση στα προσωπικά σας δεδομένα.

Υποχρεούστε να εισέλθετε σε συμφωνητικό με τον κάθε εκτελούντα την επεξεργασία. Μεταξύ άλλων, το συμφωνητικό οφείλει να περιλαμβάνει το γεγονός ότι ο εκτελών την επεξεργασία:

- Θα επεξεργάζεται προσωπικά δεδομένα μόνο κατ' εντολή σας
- Θα λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας
- Θα επιβάλει καθήκοντα εμπιστευτικότητας με τα άτομα που εκτελούν χρέη επεξεργασίας προσωπικών δεδομένων
- Θα παρέχει βοήθεια όσον αφορά τη συμμόρφωση με τις υποχρεώσεις που είναι σχετικές με τα δικαιώματα των υποκειμένων των δεδομένων
- Θα διαγράφει τα δεδομένα ή θα τα επιστρέφει στον υπεύθυνο επεξεργασίας αφού αυτά έχουν υποστεί επεξεργασία.
- Θα κάνει διαθέσιμες τις πληροφορίες που είναι απαραίτητες για ελέγχους ή επιθεωρήσεις από τις αρχές επιθεώρησης

Οπότε, τώρα είναι η στιγμή να ελέγξετε τα συμφωνητικά σας με τους εκτελούντες την επεξεργασία και πιθανώς να τα επαναδιαπραγματευθείτε.

- Δημιουργείστε κατάλογο με τους εκτελούντες την επεξεργασία.
- Ελέγξτε εάν τα συμφωνητικά σας συμμορφώνονται με τον ΓΚΠΔ
- Όπου κριθεί απαραίτητο, τροποποιήστε τα συμφωνητικά ή συνάψτε νέα συμφωνητικά επεξεργασίας δεδομένων

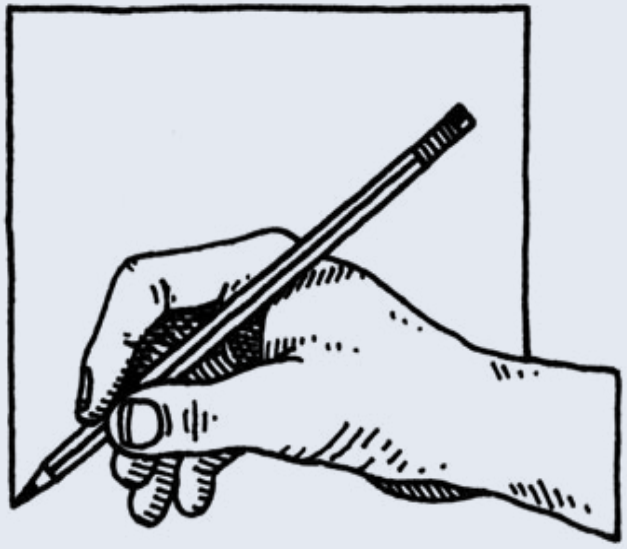
Επιπρόσθετα, ο ΓΚΠΔ περιέχει ένα μεγάλο αριθμό υποχρεώσεων για τον εκτελούντα την επεξεργασία. Για παράδειγμα, σύμφωνα με τον ΓΚΠΔ οι εκτελούντες την επεξεργασία οφείλουν να:

- Καθιερώσουν ένα αρχείο για όλες τις διεργασίες επεξεργασίας (δείτε **Βήμα 5**)
- Διορίστε έναν ΥΠΔ εάν κριθεί απαραίτητο (δείτε **Βήμα 1**)
- Αναζητήστε άδεια από τον υπεύθυνο επεξεργασίας για τον διορισμό υπό-εκτελούντων την επεξεργασία.
- Αναφέρετε τις παραβιάσεις δεδομένων στον υπεύθυνο επεξεργασίας
- Συνεργαστείτε με την αρχή επιθεώρησης
- Δράστε σε συμφωνία με τις απαιτήσεις για μεταφορά προσωπικών δεδομένων σε χώρες εκτός της Ε.Ε.
- Διεξάγετε ΕΑΠΔ (δείτε **Βήμα 3**)

Παρά τις υποχρεώσεις που προκύπτουν από τον ΓΚΠΔ, σας συνιστούμε να συζητήσετε τα σημεία με τους εκτελούντες την επεξεργασία και καθορίστε με κοινή συμφωνά πως αυτά θα εφαρμοσθούν στην πράξη.

ΒΗΜΑ 11

Ανανεώστε τη ροή εγγραφών για να επιτύχετε έννομη συναίνεση



Ένας αριθμός των διεργασιών επεξεργασίας δεδομένων πιθανώς βασίζονται στην αρχή της συναίνεσης.

Η έννομη συναίνεση ισχύει μόνο εάν είναι «ελεύθερα δοσμένη, εξειδικευμένη, ενημερωμένη και σαφής», χωρίς την ύπαρξη εξαναγκασμού. Αυτό μπορεί να συμβεί μέσω δήλωσης ή καταφατικής πράξης, όπως «τσεκάρισμα» κουτιού φόρμας, εάν παρέχονται επίσης επαρκείς πληροφορίες. Η αυτόματη, υπονοούμενη υπόθεση συναίνεση ή η χρήση προ-συμπληρωμένων κουτιών φόρμας δεν επαρκούν για την απόκτηση έγκυρης σΗυνσαυί**ν**αείσνηεσσ.η, σύμφωνα με τον ΓΚΠΔ δεν δίνεται «ελεύθερα» εάν το υποκείμενο των δεδομένων δεν έχει πραγματική επιλογή, δηλαδή, δεν είναι σε θέση να αρνηθεί ή η απόσυρση συναίνεσης δημιουργεί προδιαθέσεις εναντίον του. Αυτό μπορεί να συμβεί όταν η λύση μιας σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, εξαρτάται από τη συναίνεση του υποκειμένου των δεδομένων να γίνει επεξεργασία προσωπικών δεδομένων που δεν είναι απαραίτητη για την επιτέλεση του έργου. Η συναίνεση δεν δίνεται «ελεύθερα» εάν δεν μπορεί να δοθεί ξεχωριστά συναίνεση για τις διάφορες διεργασίες επεξεργασίας δεδομένων, ακόμη και αν αυτό θα ήταν κατάλληλο στην συγκεκριμένη περίπτωση.

Οφείλετε να είστε σε θέση να επιδείξετε ότι έχετε αποκτήσει την έγκυρη συναίνεση των υποκειμένων των δεδομένων για να επεξεργαστείτε τα προσωπικά τους Εδεπδιπομρόένσαθ.ετα τα υποκείμενα των δεδομένων δικαιούνται να αποσύρουν τη συναίνεσή τους σε οποιαδήποτε στιγμή. Αυτό είναι όσο απλό όσο το η παροχή συναίνεσης, και προτού τα υποκείμενα των δεδομένων παράσχουν συναίνεση, πρέπει να ενημερωθούν για αυτό το δικαίωμά τους. Διαφορετικά η συναίνεση είναι άκυρη. Εάν επεξεργαστείτε ειδικά προσωπικά δεδομένα, η συναίνεση (που εξαρτάται από την εφαρμογή μιας εξαίρεσης) οφείλει να είναι «ξεκάθαρη». Αυτό σημαίνει ότι το υποκείμενο των δεδομένων έχει ξεκάθαρα εκφράσει την επιθυμία του με λέξεις, γραπτώς ή μέσω συμπεριφοράς.

Τι χρειάζεται να κάνετε;

- Καθορίστε ποιές διεργασίες επεξεργασίες βασίζονται στην αρχή της συναίνεσης (δείτε **Βήμα 2**)
- Ελέγξτε εάν ο τρόπος που αναζητείτε, αποκτάτε και καταγράφετε τη συναίνεση είναι συμβατή με τον ΓΚΠΔ
- Ανανεώστε τις διεργασίες σας αν κριθεί απαραίτητο
- Εξασφαλίστε επίσης ότι τα υποκείμενα των δεδομένων μπορούν να αποσύρουν εύκολα τη συναίνεσή τους.

ΒΗΜΑ 12

Βρείτε ποιά Αρχή Προστασίας

- Δεδομένων Προσωπικού Χαρακτήρα σας εποπτεύει

Ο ΓΚΠΔ λειτουργεί στη βάση του «κατάστημα-μιας-στάσης».

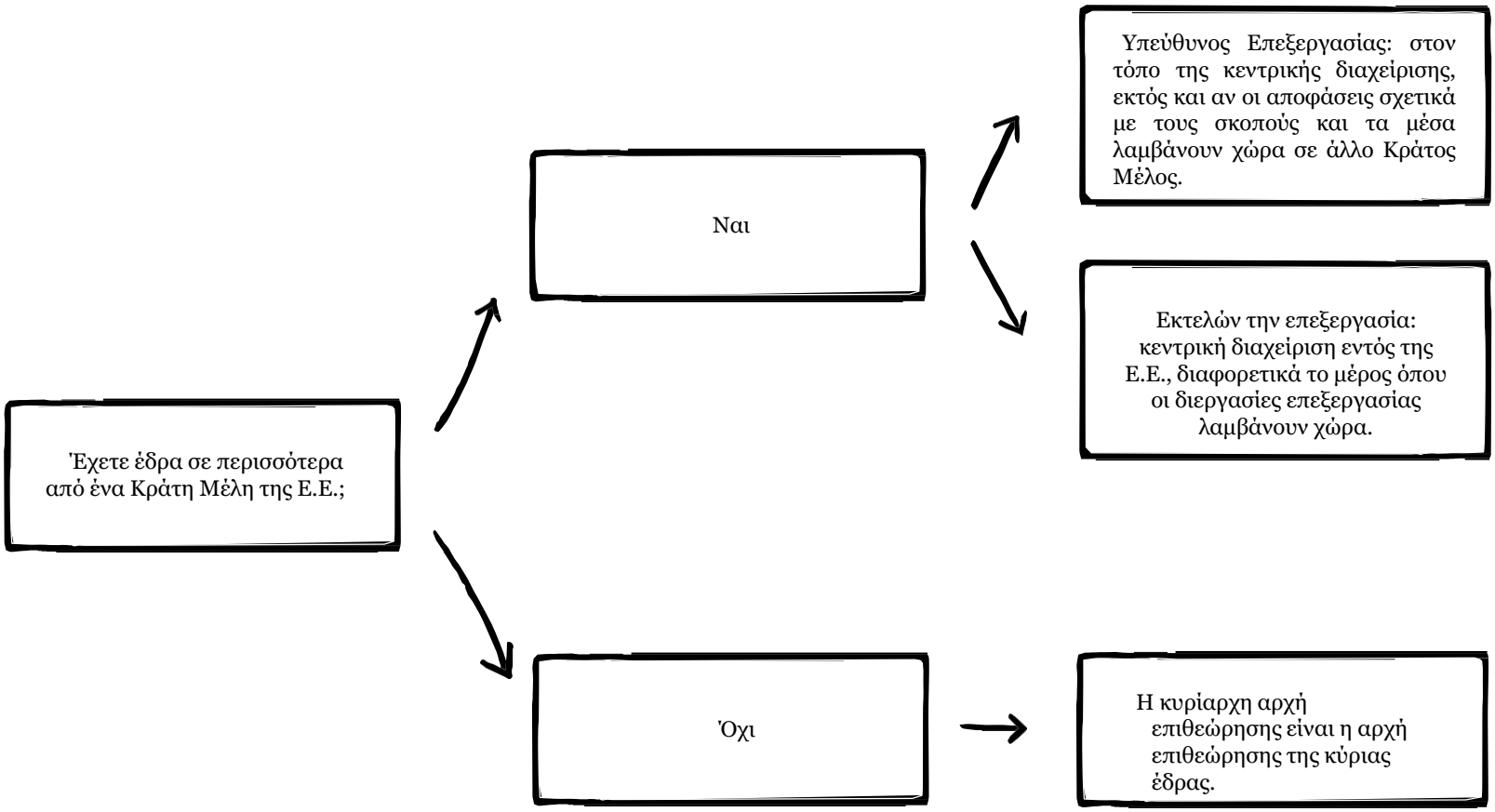
Η ιδέα είναι ότι αντιμετωπίσετε μία αρχή επιθεώρησης, ακόμη και αν ο οργανισμός σας έχει έδρες σε περισσότερες από μία χώρες της Ε.Ε. ή εάν οι διεργασίες επεξεργασίες δεδομένων έχουν αντίκτυπο σε περισσότερες από μία χώρες της Ε.Ε. Αυτή η αρχή επιθεώρησης ονομάζεται «κυρίαρχη αρχή επιθεώρησης».

Η κυρίαρχη αρχή επιθεώρησης είναι η αρχή επιθεώρησης της Χώρας Μέλους της Ε.Ε. όπου η κύρια έδρα (ή η μοναδική έδρα) του οργανισμού βρίσκεται. Αυτός είναι ο τόπος όπου η κεντρική διαχείριση του υπεύθυνου επεξεργασίας βρίσκεται εντός της Ε.Ε. Αυτό αλλάζει εάν οι αποφάσεις που σχετίζονται με τους σκοπούς και τα μέσα των διεργασιών επεξεργασίας προσωπικών δεδομένων γίνονται σε άλλη έδρα. Στην περίπτωση αυτή, η άλλη αυτή έδρα αποτελεί την κύρια έδρα. Για τους εκτελούντες την επεξεργασία, η κύρια έδρα είναι η έδρα όπου βρίσκεται η κεντρική διαχείριση, ή – εάν δεν υπάρχει κεντρική διαχείριση - η έδρα όπου οι κύριες διεργασίες επεξεργασίας λαμβάνουν χώρα.

Η κυρίαρχη αρχή επιθεώρησης είναι κυρίως υπεύθυνη για την επίβλεψη των οργανισμών με δια-συνοριακές διεργασίες επεξεργασίες δεδομένων. Η κυρίαρχη αρχή επιθεώρησης μπορεί να έχει επίσης ρόλο εφαρμοστή στις δια-συνοριακές διεργασίες επεξεργασίας του οργανισμού που επιτηρεί.

Εάν μια διεργασία επεξεργασίας λαμβάνει χώρα μόνο σε ένα Κράτος Μέλος διαφορετικό από αυτό της κυρίαρχης αρχής επιθεώρησης, ή εάν μια διεργασία επεξεργασίας έχει φυσικό αντίκτυπο στα υποκείμενα των δεδομένων ενός Κράτους Μέλους, τότε μπορεί να διατυπωθεί παράπονο και στην αρχή επιθεώρησης εκείνου του Κράτους Μέλους. Αυτή η υπερ-αρχή επιθεώρησης οφείλει όμως να ενημερώνει αμέσως την κυρίαρχη αρχή επιθεώρησης και να συνεργάζεται μαζί τΑηπξό· την άλλη, η κυρίαρχη αρχή επιθεώρησης οφείλει να συντονίζει τις δράσεις της με τις λοιπές Εποπτικές Αρχές σε άλλες χώρες της Ε.Ε. όπου η επεξεργασία δεδομένων έχει αντίκτυπο. Η κυρίαρχη αρχή επιθεώρησης συντονίζει τις δραστηριότητες, συμπεριλαμβάνει τις υπόλοιπες σχετικές αρχές επιθεώρησης και τους καταθέτει τις αρχικές αποφάσεις.

Είναι η βασική σας έδρα στην Ολλανδία; Με άλλα λόγια, λαμβάνετε αποφάσεις σχετικά με τους σκοπούς και τα μέσα των διεργασιών επεξεργασίας στην Ολλανδία; Ή έχετε απλώς την έδρα σας στην Ολλανδία; Εάν ναι, τότε ανήκετε υπό την εποπτεία του Ολλανδικού ρυθμιστή δηλαδή στην Ολλανδική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα


Έχετε έδρα σε περισσότερα από ένα Κράτη Μέλη της Ε.Ε.;
Ναι
Όχι
Υπεύθυνος Επεξεργασίας: στον τόπο της κεντρικής διαχείρισης, εκτός και αν οι αποφάσεις σχετικά με τους σκοπούς και τα μέσα λαμβάνουν χώρα σε άλλο Κράτος Μέλος.
Εκτελών την επεξεργασία: κεντρική διαχείριση εντός της Ε.Ε., διαφορετικά το μέρος όπου οι διεργασίες επεξεργασίας λαμβάνουν χώρα.
Η κυρίαρχη αρχή επιθεώρησης είναι η αρχή επιθεώρησης της κύριας έδρας.