ADACOM

SECURITY
BUILT ON TRUST

Εκπαίδευση για τον ΓΚΠΠΔ

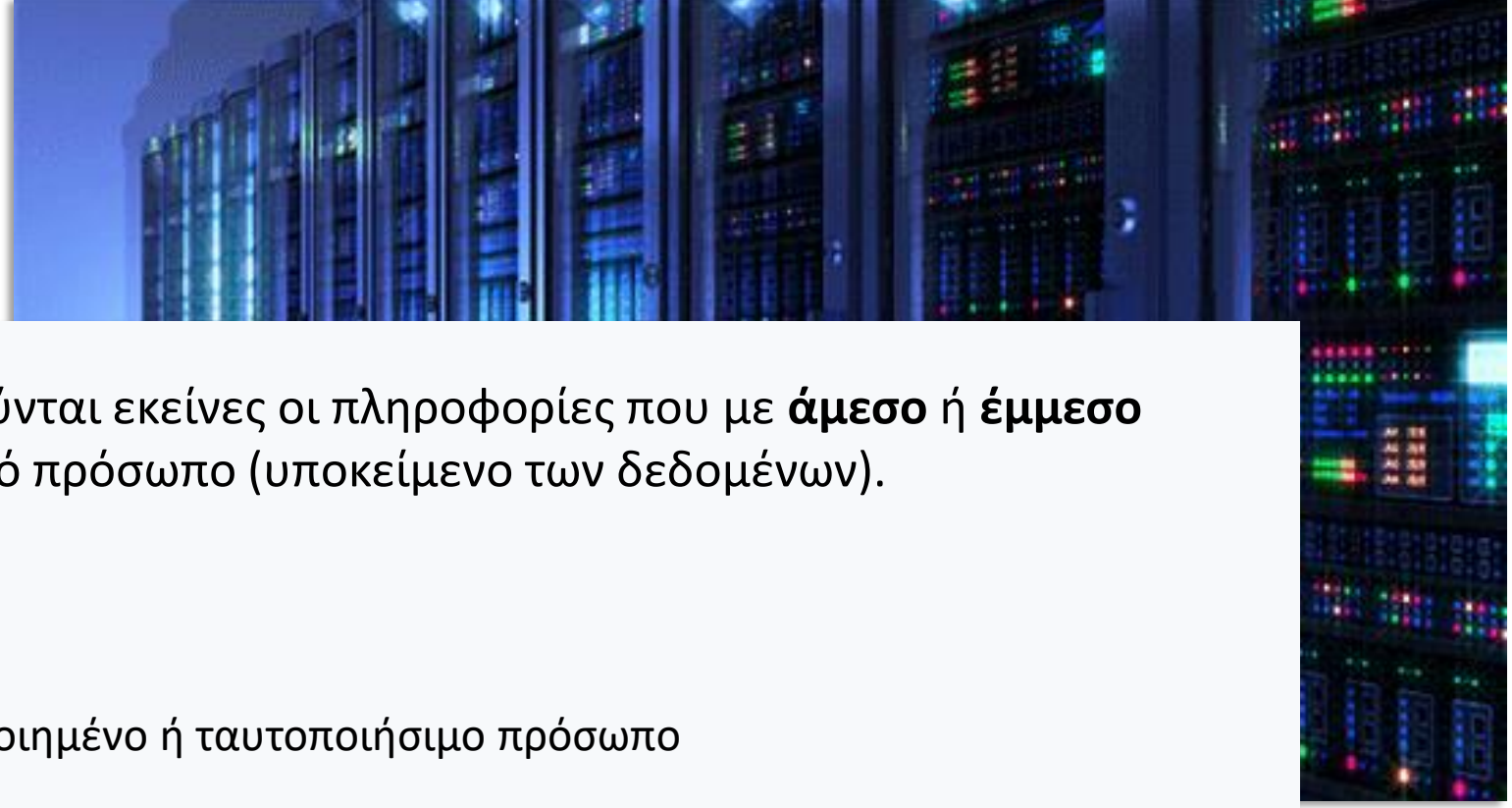
ADACOM S.A.
Ιανουάριος 2024

Σκοπός του Κανονισμού (ΕΕ) 2016/679

- Ο Κανονισμός (ΕΕ) 2016/679 θεσπίζει κανόνες που αφορούν την **προστασία** των **φυσικών προσώπων** έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα.
- Είναι σε ισχύ από τις 25/05/2018.
- Κανονισμός 679/2016 για την κατάργηση της οδηγίας 95/46/ΕΚ.
- Ο παρών κανονισμός προστατεύει θεμελιώδη **δικαιώματα** και **ελευθερίες** των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.
- Ενιαίο θεσμικό πλαίσιο όσον αφορά την επεξεργασία των Προσωπικών Δεδομένων σε όλα τα κράτη μέλη της ΕΕ.

1. Ποια στοιχεία συνιστούν Προσωπικά Δεδομένα…

Προσωπικά Δεδομένα



Ως δεδομένα προσωπικού χαρακτήρα θεωρούνται εκείνες οι πληροφορίες που με **άμεσο** ή **έμμεσο** τρόπο μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο (υποκείμενο των δεδομένων).

Παραδείγματα Προσωπικών Δεδομένων

- Οποιαδήποτε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο
- Όνομα, επώνυμο και αριθμός ταυτότητας
- Δεδομένα τοποθεσίας
- Διεύθυνση IP
- Φωτογραφίες
- Βίντεο
- Παράγοντες που αφορούν τη φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του προσώπου

Κατηγορίες Προσωπικών Δεδομένων

Οι κατηγορίες που αναφέρονται στη διπλανή εικόνα αποτελούν κατηγορίες προσωπικών πληροφοριών, που σχετίζονται με τον ιδιωτικό ή δημόσιο βίο του προσώπου. Οι συγκεκριμένες κατηγορίες αναφέρονται ενδεικτικά και δεν είναι αποκλειστικές.

Εσωτερικό – C2

Ευαίσθητα Προσωπικά Δεδομένα

01 Θρησκευτικές ή φιλοσοφικές πεποιθήσεις

02 Συμμετοχή σε συνδικαλιστικές οργανώσεις

03 Βιομετρικά δεδομένα

04 Γενετικά δεδομένα

05 Πολιτικά φρονήματα

06 Δεδομένα υγείας

07 Φυλετική ή εθνοτική καταγωγή

08 Σεξουαλικός προσανατολισμός

Δεν επιτρέπεται η επεξεργασία προσωπικών δεδομένων σχετικά με τα παραπάνω χαρακτηριστικά ενός προσώπου, εκτός εάν υπάρχει ισχυρή νομική βάση για την επεξεργασία τους.

2. Τι σημαίνει επεξεργασία Προσωπικών Δεδομένων…

Επεξεργασία Προσωπικών Δεδομένων

Επεξεργασία δεδομένων είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως:

- η συλλογή
- η καταχώριση
- η οργάνωση
- η διάρθρωση
- η αποθήκευση
- η προσαρμογή ή η μεταβολή
- η ανάκτηση
- η αναζήτηση πληροφοριών
- η χρήση
- η κοινοποίηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης
- η συσχέτιση ή ο συνδυασμός
- ο περιορισμός
- η διαγραφή ή η καταστροφή τους

Βασικές έννοιες και ορισμοί της Επεξεργασίας

Υποκείμενο των Δεδομένων	Υπεύθυνος Επεξεργασίας	Εκτελών την Επεξεργασία
Το άτομο	*Καθορίζει τους σκοπούς και τα μέσα με τα οποία γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα*	*Επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας*

Πηγή:

https://www.youtube.com/watch?v=OPWZEo1cKyA

3. Βασικές Αρχές Προστασίας Δεδομένων

Βασικές Αρχές Προστασίας Δεδομένων

ΟΙ ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Νομιμότητα, δικαιοσύνη και διαφάνεια

Τα Προσωπικά Δεδομένα θα επεξεργάζονται νόμιμα, δίκαια και με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων

Περιορισμός του σκοπού επεξεργασίας των δεδομένων

Τα προσωπικά δεδομένα συλλέγονται για συγκεκριμένους, ρητούς και νόμιμους σκοπούς χωρίς περαιτέρω επεξεργασία κατά τρόπο ασυμβίβαστο με τους σκοπούς αυτούς.

Ελαχιστοποίηση δεδομένων

Τα προσωπικά δεδομένα πρέπει να είναι επαρκή, συναφή και να περιορίζονται σε αυτά που είναι αναγκαία σε σχέση με τους σκοπούς για τους οποίους επεξεργάζονται.

Ακρίβεια

Τα Προσωπικά Δεδομένα πρέπει να είναι ακριβή και ενημερωμένα.

Περιορισμός αποθήκευσης

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρούνται υπό μορφή που επιτρέπει την αναγνώριση του υποκείμενου των δεδομένων για χρονικό διάστημα που δεν υπερβαίνει τον αναγκαίο χρόνο επίτευξης του σκοπού για τον οποίο διατηρούνται.

Ακεραιότητα και εμπιστευτικότητα

Τα προσωπικά δεδομένα πρέπει να επεξεργάζονται κατά τρόπο που να διασφαλίζει κατάλληλη ασφάλεια για αυτά, συμπεριλαμβανομένης της προστασίας κατά της μη εξουσιοδοτημένης ή παράνομης τροποποίησης τους και κατά της τυχαίας απώλειας, καταστροφής ή ζημιάς. Η επιχείρηση πρέπει να χρησιμοποιεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας.

Λογοδοσία

Ο υπεύθυνος επεξεργασίας δεδομένων είναι υπεύθυνος και πάντοτε σε θέση να αποδείξει τη συμμόρφωση της επιχείρησης με τον παρόντα κανονισμό και τη τήρηση των αρχών προστασίας δεδομένων

Πότε επιτρέπεται η Επεξεργασία Δεδομένων;

Νόμιμη Βάση Επεξεργασίας

- **Συγκατάθεση**: το άτομο (υποκείμενο) έχει δώσει τη **σαφή** συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων για συγκεκριμένο σκοπό
- **Σύμβαση**: η επεξεργασία είναι απαραίτητη για μια σύμβαση με το άτομο ή επειδή έχει ζητήσει να εκτελεστούν συγκεκριμένες ενέργειες πριν τη σύναψη της σύμβασης
- **Νομική υποχρέωση**: η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με τη νομοθεσία (χωρίς τις συμβατικές υποχρεώσεις)
- **Ζωτικά συμφέροντα**: η επεξεργασία είναι απαραίτητη για την προστασία της ζωής κάποιου
- **Δημόσιο συμφέρον**: η επεξεργασία είναι απαραίτητη για την εκτέλεση εργασίας προς το δημόσιο συμφέρον ή για τις επίσημες λειτουργίες του υπεύθυνου διαχείρισης (επιχείρησης) εφόσον οι λειτουργίες έχουν σαφή νομική βάση
- **Έννομα συμφέροντα**: η επεξεργασία είναι απαραίτητη για τα έννομα συμφέροντά του οργανισμού ή τα έννομα συμφέροντα τρίτων, εκτός εάν υπάρχει σημαντικός λόγος για την προστασία των προσωπικών δεδομένων του ατόμου που υπερισχύει αυτών των έννομων συμφερόντων

Συγκατάθεση

Πως χορηγείται η συγκατάθεση;

- Ο Οργανισμός πρέπει να διατηρεί αποδεικτικά στοιχεία της συγκατάθεσης,
- Εάν η συγκατάθεση είναι γραπτή, το κείμενο πρέπει να είναι εύκολα προσβάσιμο, κατανοητό, ευδιάκριτο, σε σαφή, απλή γλώσσα και να διαχωρίζεται από άλλα θέματα,
- Απαιτείται ρητή συγκατάθεση για την επεξεργασία ειδικών κατηγοριών δεδομένων,
- Ο Οργανισμός πρέπει να παρέχει έναν εύκολο τρόπο ανάκλησης της συγκατάθεσης ανά πάσα στιγμή και να ενημερώνει το υποκείμενο των δεδομένων σχετικά με αυτό το δικαίωμα,
- Πρέπει να δίνεται ελεύθερα. π.χ. Αποτελεί προϋπόθεση για την υπηρεσία, ενώ η αντίστοιχη επεξεργασία δεδομένων δεν είναι απαραίτητη για την υπηρεσία;
- Πρέπει να είναι σαφές για ποια επεξεργασία δίνεται η συγκατάθεση,
- Η παροχή ηλεκτρονικών υπηρεσιών σε παιδιά κάτω των 16 ετών (έως 13 ετών) απαιτεί τη συγκατάθεση του κηδεμόνα.

4. Δικαιώματα των υποκειμένων

Δικαιώματα των Υποκειμένων (Άρθρα 12-23)

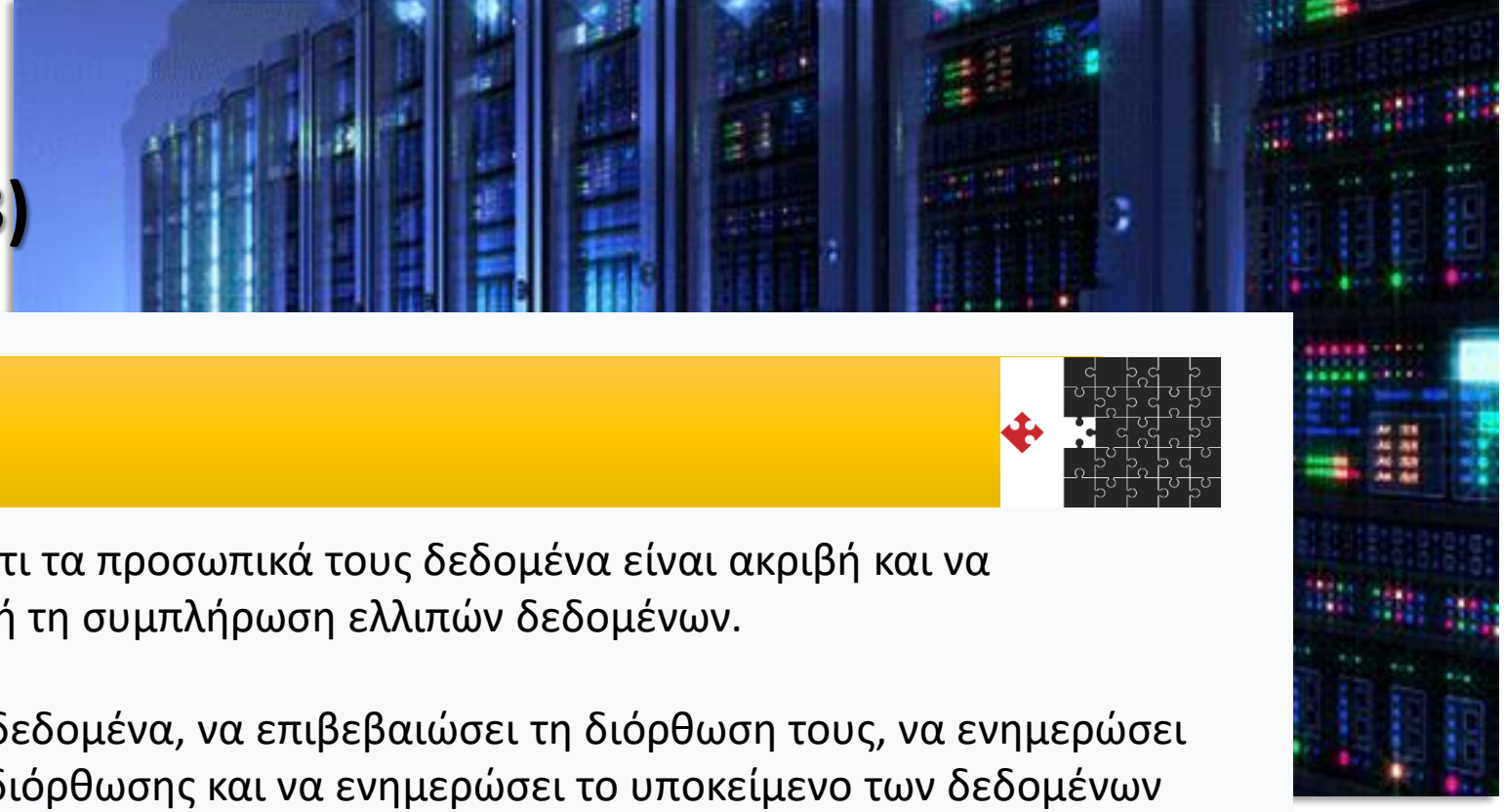
1 Δικαίωμα ενημέρωσης

Τα άτομα έχουν το δικαίωμα να λαμβάνουν πληροφορίες απορρήτου όπως: Πώς θα γίνει η επεξεργασία των δεδομένων τους, σε ποιους θα κοινοποιηθούν, ποια είναι τα δικαιώματά τους σε σχέση με αυτά. Οι πληροφορίες που παρέχονται πρέπει να είναι συνοπτικές, διαφανείς, κατανοητές και εύκολα προσβάσιμες. Γραμμένες σε σαφή και απλή γλώσσα, ειδικά αν απευθύνονται σε παιδί και παρέχονται **δωρεάν**.

2 Δικαίωμα πρόσβασης

Τα άτομα έχουν το δικαίωμα να έχουν επιβεβαίωση ότι τα δεδομένα τους υποβάλλονται σε επεξεργασία, να ενημερωθούν και να επαληθεύσουν τη νομιμότητα της επεξεργασίας και να απαιτήσουν πρόσβαση στα προσωπικά τους δεδομένα.
Στη περίπτωση αυτή η επιχείρηση μπορεί να θέσει ένα εύλογο τέλος πρόσβασης ή να αρνηθεί να απαντήσει όταν ένα αίτημα είναι προδήλως αβάσιμο ή υπερβολικό, ιδιαίτερα εάν είναι επαναλαμβανόμενο με σχετική ενημέρωση του υποκειμένου.

Δικαιώματα των Υποκειμένων (Άρθρα 12-23)



3 Δικαίωμα διόρθωσης

Τα άτομα έχουν το δικαίωμα να επιβεβαιώσουν ότι τα προσωπικά τους δεδομένα είναι ακριβή και να απαιτήσουν τη διόρθωση ανακριβών δεδομένων ή τη συμπλήρωση ελλιπών δεδομένων.

Η επιχείρηση οφείλει να διορθώσει τα ανακριβή δεδομένα, να επιβεβαιώσει τη διόρθωση τους, να ενημερώσει τους παραλήπτες για λανθασμένα δεδομένα της διόρθωσης και να ενημερώσει το υποκείμενο των δεδομένων εάν δεν είναι δυνατή η τροποποίηση και οι λόγοι αυτής.

Δικαιώματα των Υποκειμένων (Άρθρα 12-23)

4 Δικαίωμα διαγραφής

Τα άτομα έχουν το δικαίωμα να διαγράψουν τα προσωπικά τους δεδομένα εάν:

- Τα προσωπικά τους δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τον σκοπό για τον οποίο συλλέχθηκαν/επεξεργάστηκαν αρχικά
- Αποσύρουν τη συγκατάθεσή τους
- Τα δεδομένα τους έχουν υποστεί παράνομη επεξεργασία
- Υπάρχει νομική υποχρέωση διαγραφής

Η επιχείρηση οφείλει να συμμορφωθεί με το αίτημα (εκτός εάν υπάρχει νομική υποχρέωση συνέχισης της επεξεργασία των δεδομένων) και να λάβει μέτρα για την ενημέρωση τυχόν άλλων υπεύθυνων επεξεργασίας σχετικά με το αίτημα διαγραφής του υποκειμένου των δεδομένων.

Δικαιώματα των Υποκειμένων (Άρθρα 12-23)

5 Δικαίωμα περιορισμού της επεξεργασίας

Τα άτομα μπορούν να ζητήσουν:

- Περιορισμό επεξεργασίας των προσωπικών τους δεδομένων, έως ότου επαληθευτεί μια απαίτηση ακρίβειας
- Απόσυρση δεδομένων που έχουν υποστεί παράνομη επεξεργασία
- Διατήρηση δεδομένων για άσκηση ή υπεράσπιση νομικών αξιώσεων

Η επιχείρηση οφείλει να λάβει μέτρα για να διασφαλίσει τον περιορισμό όπως ζητήθηκε. Ενημερώνει το υποκείμενο των δεδομένων εάν η επεξεργασία δεδομένων θα ξαναρχίσει και γιατί.

6 Δικαίωμα μεταφοράς δεδομένων

Τα άτομα έχουν το δικαίωμα:

- Λήψης των προσωπικών τους δεδομένων σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή.
- Μεταφοράς των δεδομένων τους σε άλλον υπεύθυνο επεξεργασίας χωρίς εμπόδια.

Δικαιώματα των Υποκειμένων (Άρθρα 12-23)

7 Δικαίωμα ένστασης

Τα άτομα έχουν το δικαίωμα να αντιταχθούν σε:

- Επεξεργασία για προώθηση πωλήσεων και **direct marketing**
- Επεξεργασία εάν δεν γίνεται για το δημόσιο συμφέρον ή για τα νόμιμα συμφέροντα του Υπεύθυνου Επεξεργασίας, συμπεριλαμβανομένης της δημιουργίας προφίλ

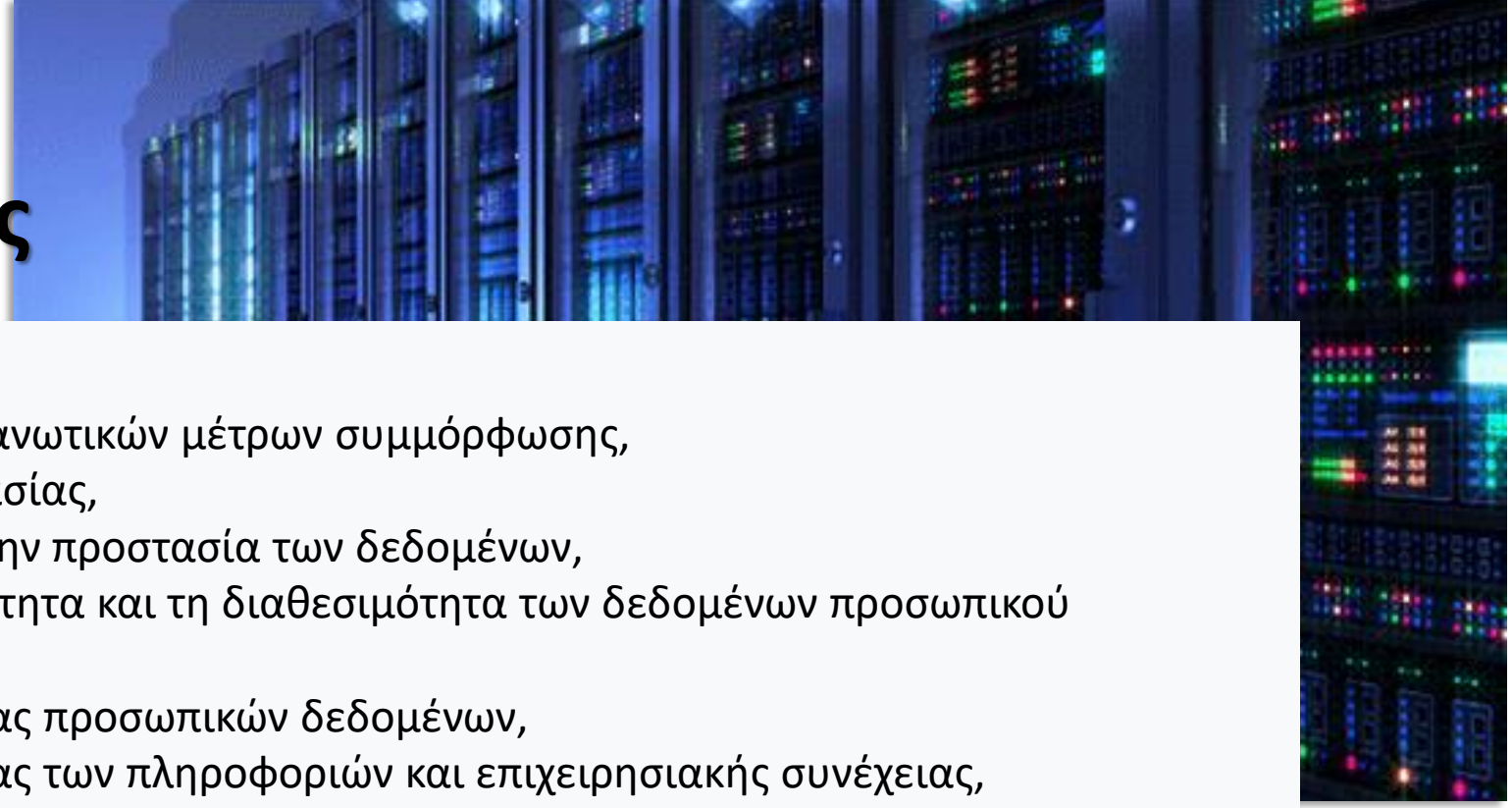
8 Δικαιώματα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ

Σύμφωνα με το άρθρο 22, τα άτομα έχουν το δικαίωμα να μην υπόκεινται σε κάποια απόφαση όταν:

- Βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της δημιουργίας προφίλ
- Παράγει νομική ή παρόμοια σημαντική επίδραση στο άτομο

5. Υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας



- Λήψη όλων των απαραίτητων τεχνικών και οργανωτικών μέτρων συμμόρφωσης,
- Τήρηση των αρχείων δραστηριοτήτων επεξεργασίας,
- Διενέργεια μελέτης εκτίμησης αντικτύπου για την προστασία των δεδομένων,
- Διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα,
- Ανάπτυξη πολιτικών και διαδικασιών προστασίας προσωπικών δεδομένων,
- Ανάπτυξη πολιτικών και διαδικασιών προστασίας των πληροφοριών και επιχειρησιακής συνέχειας,
- Ορισμός DPO (εάν απαιτείται),
- Εφαρμογή της αρχής της προστασίας της ιδιωτικότητας κατά το σχεδιασμό,
- Χρήση ψευδωνύμων ή κρυπτογράφησης (κατά περίπτωση),
- Διασφαλίζει τη συμμόρφωση των συνεργατών τους (εκτελούντες την επεξεργασία),
- Κοινοποίηση κάθε παραβίασης στην ΑΠΔΠΧ και στα υποκείμενα των δεδομένων,
- Διενέργεια τακτικών ελέγχων σχετικά με την αποτελεσματικότητα των μέτρων.

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας Ασφάλεια Πληροφοριών

Εμπιστευτικότητα (Confidentiality)

Οι πληροφορίες δεν διατίθενται ή αποκαλύπτονται σε μη **εξουσιοδοτημένα** άτομα, οντότητες ή διαδικασίες

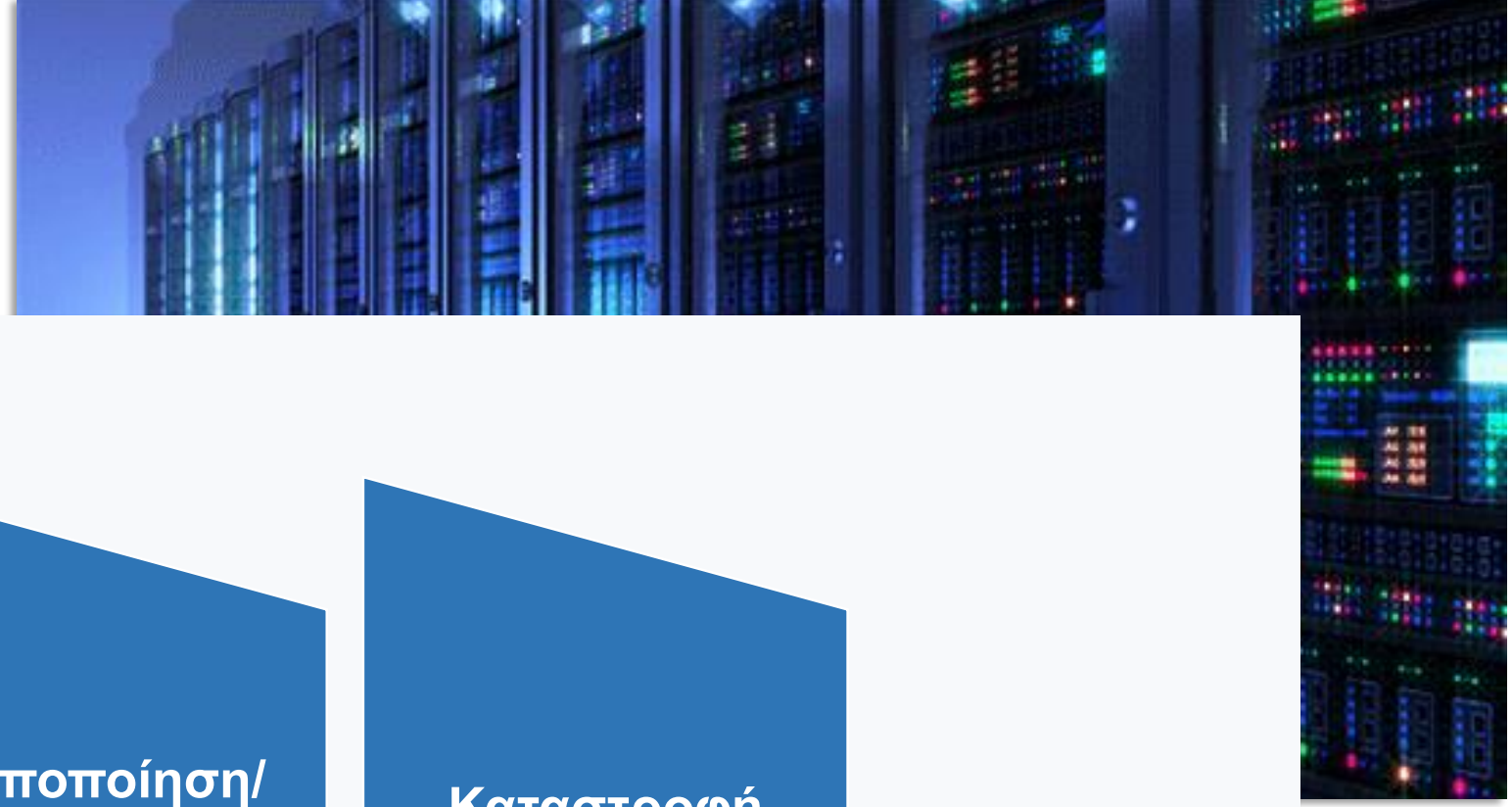
Ακεραιότητα (Integrity)

Η **ακρίβεια**, πληρότητα και **αξιοπιστία** του περιεχομένου των πληροφοριών

Διαθεσιμότητα (Availability)

Οι πληροφορίες είναι **προσβάσιμες** και **χρησιμοποιήσιμες** κατόπιν αιτήματος εξουσιοδοτημένου φορέα

Από τι θα πρέπει να προστατέψουμε τα προσωπικά δεδομένα;



- Απώλεια
- Τροποποίηση/ Αλλοίωση
- Καταστροφή

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Τεχνικά και Οργανωτικά Μέτρα

Technical Measures

Facility protection

Firewalls

VM Security

Sys Admin

and many more

Data Encryption
(at record-application level)

Auth & Access Control

Consent Tracking

Immutable audit logs

and many more

Organisational Measures

Privacy Policies

Terms & Conditions

DPA

DPIA & Risk Assess.

and many more

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Φυσική Ασφάλεια

Παραδείγματα μέτρων Φυσικής Ασφάλειας

- Ασφαλής φύλαξη, αποθηκευτικοί χώροι που κλειδώνουν, περιορισμός πρόσβασης στα γραφεία, χώροι εργασίας με ασφάλεια

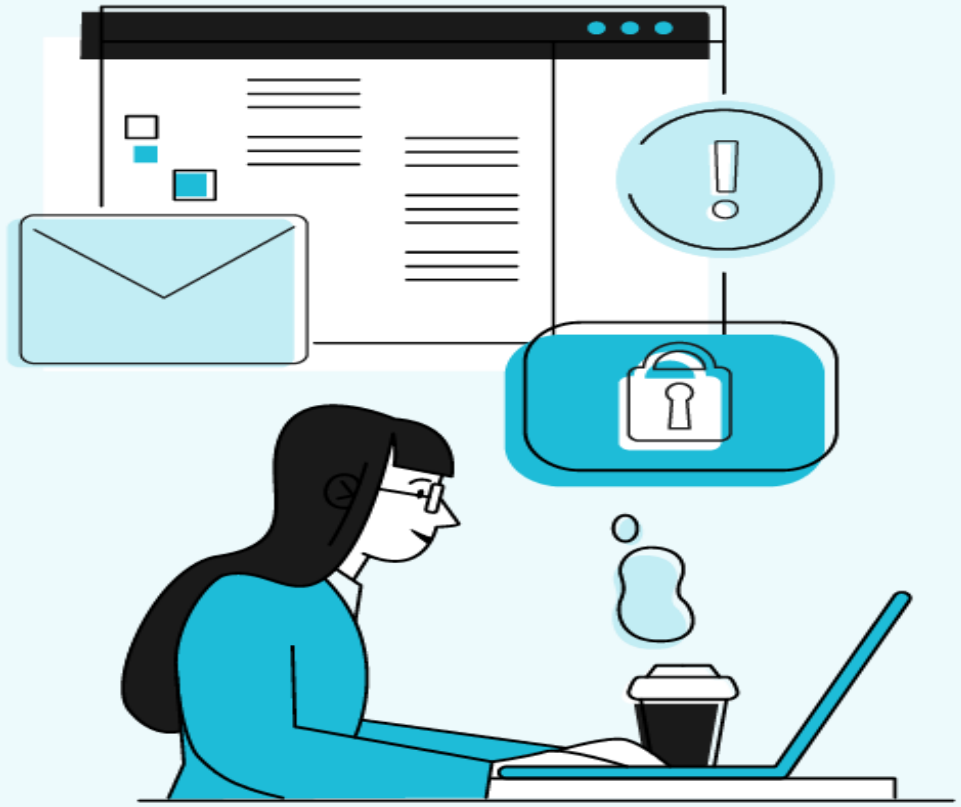
- Εγκαταστάσεις, οι οποίες είναι επαρκώς προστατευμένες έναντι φυσικών καταστροφών (πλημμύρες, σεισμοί, πυρκαγιές)

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Τεχνικά Μέτρα

ΜΕΤΡΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΠΟΥ ΜΠΟΡΕΙ ΚΑΘΕ ΕΠΙΧΕΙΡΗΣΗ ΝΑ ΛΑΒΕΙ…

Σημ.: Τα μέτρα δεν εξαντλούνται στα παρακάτω παραδείγματα



1. **Λήψη VPN** Εικονικό Ιδιωτικό Δίκτυο
2. **Εγκατάσταση** αξιόπιστου λογισμικού **Antivirus**
3. **Χρήση** σύνθετων **passwords**
4. **Χρήση** κατάλληλου **password manager**
5. **Χρήση** Κατάλληλου **Firewall**
6. **Εγκατάσταση** λογισμικού **κρυπτογράφησης**
7. Αγνόηση **ύποπτων emails**
8. Περιορισμός **πρόσβασης σε κρίσιμα δεδομένα**
9. Τακτική λήψη αντιγράφων ασφαλείας **Backups**
10. Προστασία του δικτύου **Wi-Fi**
11. Προστασία **Laptops** και **Smartphones**
12. Επικοινωνία μέτρων κυβερνοασφάλειας στο **προσωπικό**

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Τεχνικά Μέτρα

Ασφάλεια Δικτύου

Προστασία δικτύου από επιθέσεις. Ασφάλεια περιμέτρου δικτύου, απαγόρευση μη εξουσιοδοτημένης πρόσβασης και κακόβουλου λογισμικού. Παρακολούθηση και έλεγχος μέτρων ασφαλείας.

Αποσπώμενα μέσα αποθήκευσης

Εφαρμογή πολιτικής για τον έλεγχο πρόσβασης των αποσπώμενων μέσων. Περιορισμός τύπων και χρήσης των μέσων. Έλεγχος πριν την είσοδο τους στο δίκτυο.

Προστασία διαμόρφωσης

(Configuration)
Εφαρμογή ενημερώσεων ασφαλείας (security patch) και έλεγχος ότι η διαμόρφωση των συστημάτων τηρείται. Δημιουργία βάσης μέσων δικτύου και ορισμός βασικών ρυθμίσεων για όλες τις συσκευές

Διαχείριση Περιστατικών

Προσδιορισμός ικανότητας ανταπόκρισης και αποκατάστασης σε έκτακτα περιστατικά. Έλεγχος σχεδίων ανταπόκρισης.

Παρακολούθηση

Ανάπτυξη στρατηγικής παρακολούθησης και επί μέρους πολιτικών. Συνεχής παρακολούθηση όλων των συστημάτων και των δικτύων. Ανάλυση περιστατικών ασυνήθιστης δραστηριότητας που ίσως συνιστά κυβερνοεπίθεση.

Έλεγχος δικαιωμάτων πρόσβασης

Εφαρμογή αποτελεσματικών διαδικασιών απόδοσης δικαιωμάτων πρόσβασης και περιορισμός χρηστών με προνομιακά δικαιώματα. **Παρακολούθηση** εργασιών χρηστών. Έλεγχος προσβάσεων και **Audit Logs**.

Απομακρυσμένη εργασία

Ανάπτυξη πολιτικής απομακρυσμένης εργασίας. Προσδιορισμός ρυθμίσεων ασφαλείας και εφαρμογή σε όλες τις συσκευές.

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας
Οργανωτικά Μέτρα

Security Tests	Δοκιμές ασφαλείας. Διάγνωση πραγματικών τρωτών σημείων μέσω δοκιμών σε συγκεκριμένες περιοχές της υποδομής ασφαλείας σας.
Network Vulnerability Tests: **Εσωτερικά & Εξωτερικά**	Η αξιολόγηση **τρωτότητας** δικτύου είναι μια διαδικασία που βοηθά στην ανασκόπηση και ανάλυση των δικτύων τελικών σημείων και συσκευών για θέματα ασφάλειας. Η αξιολόγηση μπορεί να εντοπίσει ελαττώματα και κενά στο δίκτυο που θα μπορούσαν να αφήσουν μια ευκαιρία για εκμετάλλευση από hackers. **Απαιτείται ειδικό λογισμικό**
Network Penetration Tests: **Εσωτερικά & Εξωτερικά**	Οι δοκιμές **διείσδυσης** προσομοιώνουν επιθέσεις στον κυβερνοχώρο, εστιάζοντας στην ανακάλυψη τυχόν αδύναμων σημείων στις άμυνες ενός συστήματος υπολογιστών, τα οποία οι εγκληματίες του κυβερνοχώρου μπορούν να χρησιμοποιήσουν για να εισέλθουν και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες. **Απαιτούνται εξειδικευμένες γνώσεις**.
Web Application Penetration	Έλεγχος Ευπαθειών δικτύου, Ιστοσελίδας ή e-shop Από Επιθέσεις & Κακόβουλες Ενέργειες. Έλεγχος Τρωτών Σημείων Δικτύου για Αποφυγή Κακόβουλων Ενεργειών.
Social Engineering Tests	Η δοκιμή διείσδυσης **κοινωνικής μηχανικής (phising)** είναι η πρακτική της απόπειρας τυπικών μορφών απάτης κοινωνικής μηχανικής στους υπαλλήλους μιας εταιρείας για να διαπιστωθεί το επίπεδο ευπάθειας του οργανισμού σε αυτόν τον τύπο εκμετάλλευσης. **Απαιτούνται εξειδικευμένες γνώσεις**.
Wi-Fi Review & Testing	Εξέταση και δοκιμές της τοπολογίας ασύρματου δικτύου όσον αφορά τη τήρηση κατάλληλων μέτρων ασφαλείας.
VOIP Testing	Δοκιμές συστημάτων τηλεφωνίας μέσω διαδικτύου (**VOIP**) για τρωτότητες και ασφαλή παραμετροποίηση. **Απαιτούνται εξειδικευμένες γνώσεις**.
Security Configuration	Δοκιμές και βελτιστοποίηση ρυθμίσεων συσκευών ασφαλείας (Intrusion Detection System, Intrusion Prevention System, UTM Firewall) και συναφών λύσεων.
Operational Tests	Δοκιμές συστημάτων για ρυθμίσεις ασφαλείας όπως δοκιμές λογισμικού εφαρμογών.
Threat Assessment	Η αξιολόγηση απειλών είναι μια διαδικασία για την αξιολόγηση και την επαλήθευση των αντιληπτών απειλών, συμπεριλαμβανομένης της αξιολόγησης της πιθανότητάς τους.

Υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Οργανωτικά Μέτρα

Πολιτικές και Διαδικασίες Προστασίας Προσωπικών Δεδομένων

Συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας ή/και πιστοποιήσεις

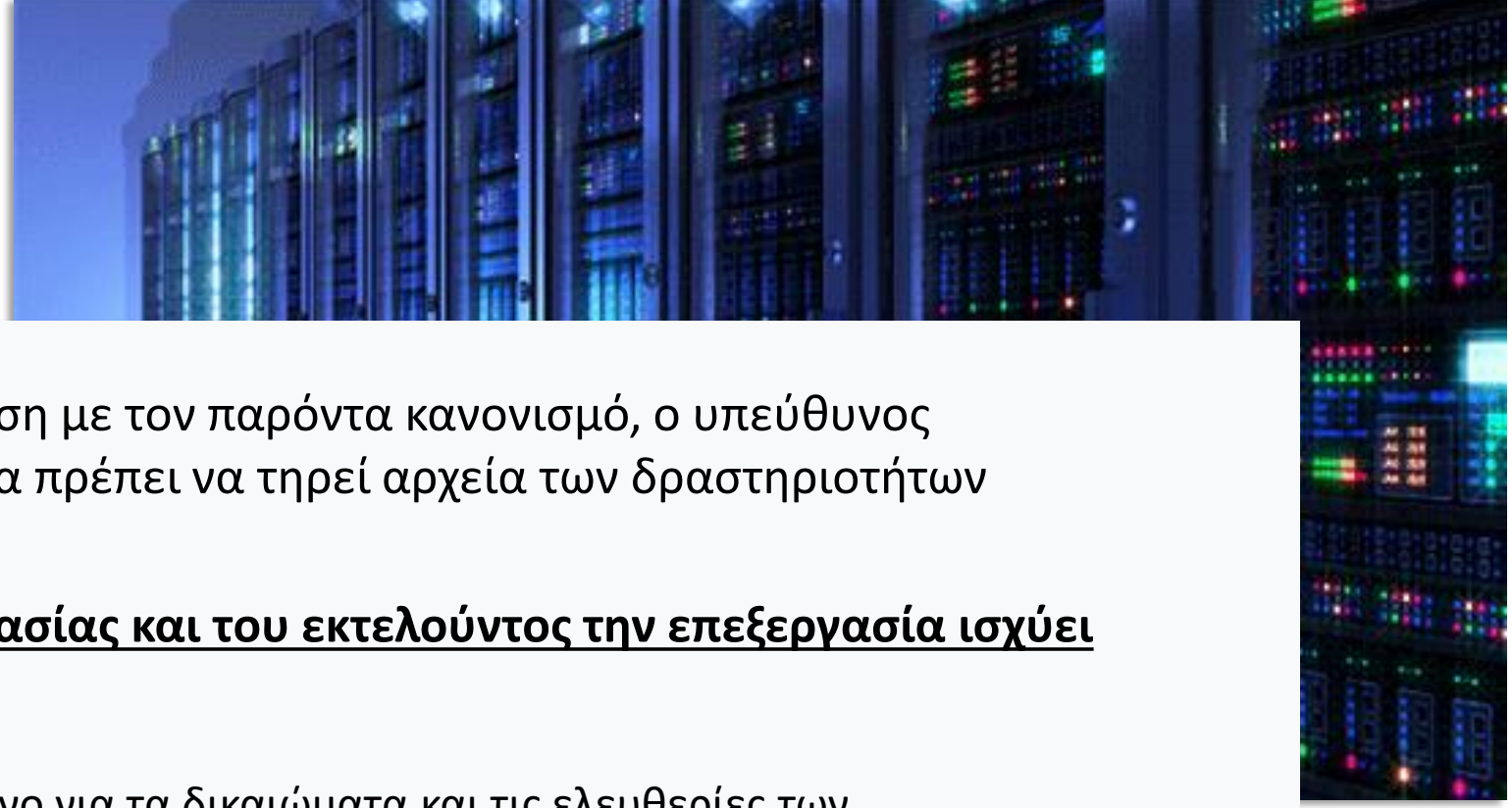
Εσωτερικοί έλεγχοι των ενεργειών επεξεργασίας προσωπικών δεδομένων

Περιοδική ανασκόπηση των Πολιτικών και Διαδικασιών

Εκπαίδευση

6. Αρχείο Δραστηριοτήτων

Αρχείο Δραστηριοτήτων



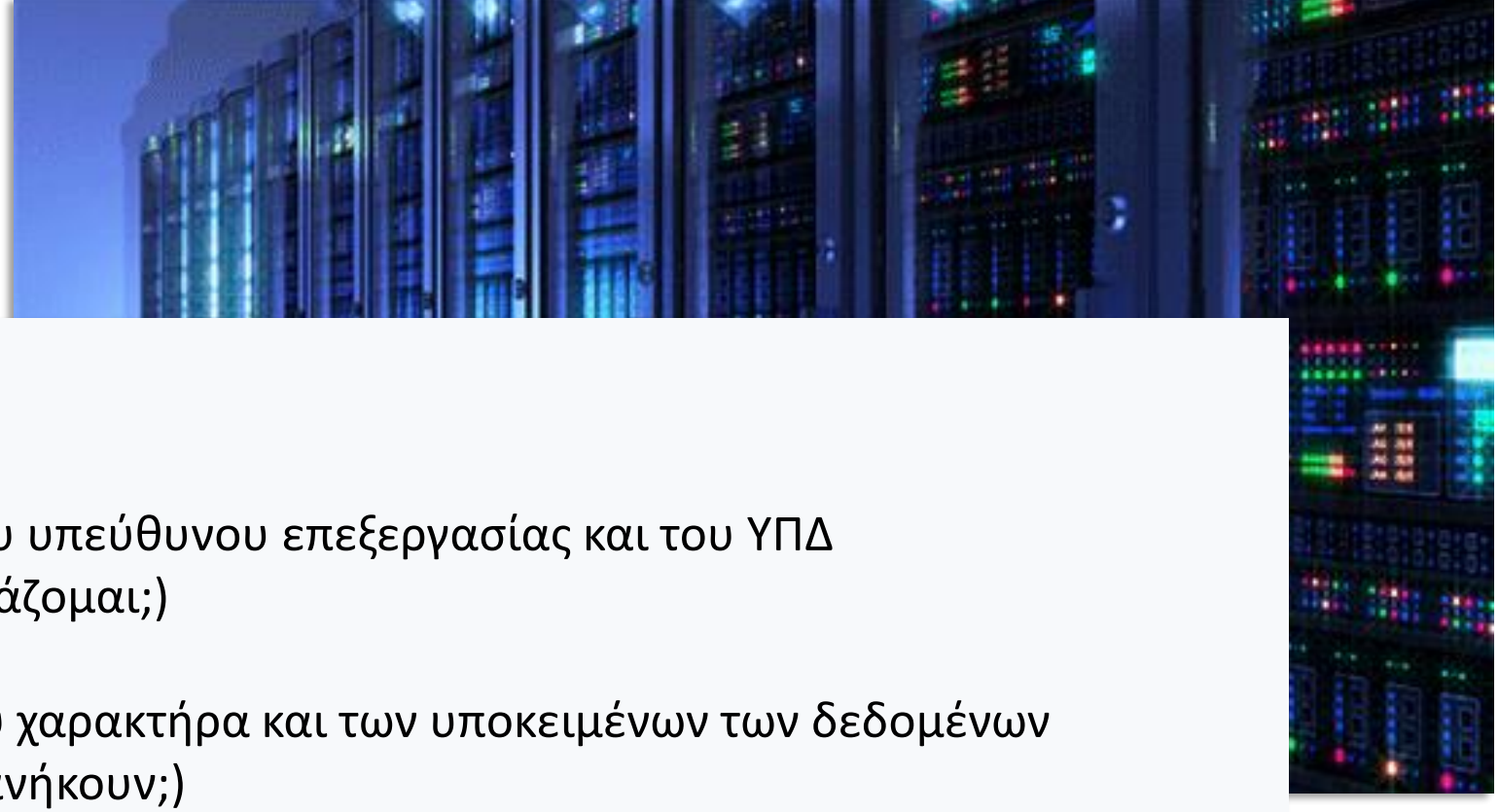
Προκειμένου να αποδεικνύεται η συμμόρφωση με τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να τηρεί αρχεία των δραστηριοτήτων επεξεργασίας υπό την ευθύνη του.

Αυτή η υποχρέωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία ισχύει όταν:

- η επεξεργασία ενδέχεται να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
- Η επεξεργασία δεν είναι περιστασιακή
- Η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων

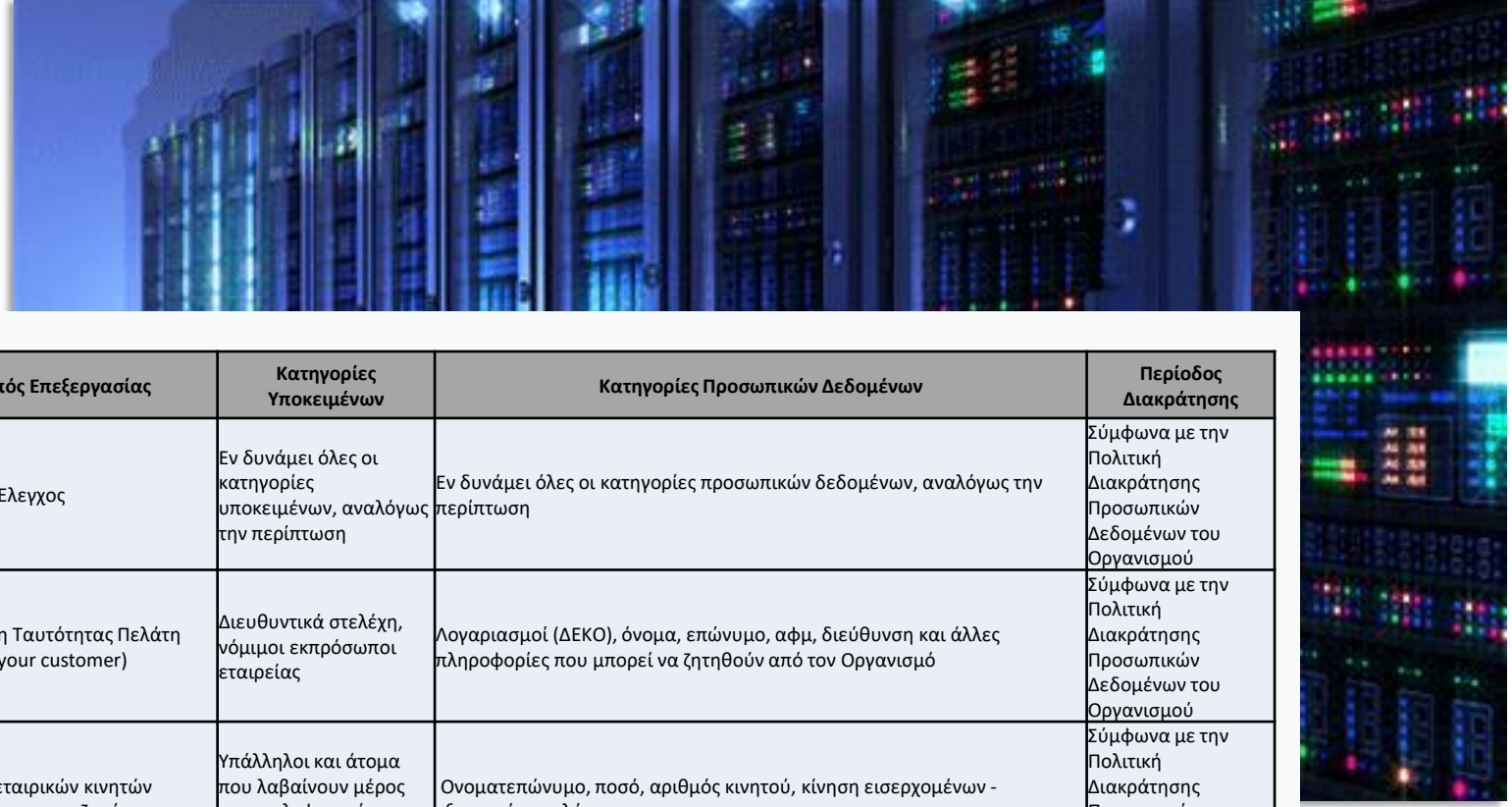
Τα αρχεία πρέπει να είναι γραπτά, μεταξύ άλλων και σε ηλεκτρονική μορφή, και να τίθενται στη διάθεση της εποπτικής αρχής (κατόπιν αιτήματος).

Περιεχόμενα Αρχείου Δραστηριοτήτων



- Στοιχεία επικοινωνίας του εκπροσώπου του υπεύθυνου επεξεργασίας και του ΥΠΔ
- Σκοπός της επεξεργασίας (γιατί τα επεξεργάζομαι;)
- Πού αποθηκεύονται τα δεδομένα
- Οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα και των υποκειμένων των δεδομένων (ποια δεδομένα επεξεργάζομαι; σε ποιον ανήκουν;)
- Οι κατηγορίες των αποδεκτών των δεδομένων (πού τα αποστέλλω;)
- Οι διαβιβάσεις δεδομένων σε τρίτες χώρες
- Οι προβλεπόμενες προθεσμίες για τη διαγραφή των δεδομένων (πόσο καιρό θα τα διατηρήσω;)
- Γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας

Υπόδειγμα Αρχείου Δραστηριοτήτων



Υπεύθυνο Τμήμα	Δραστηριότητα Επεξεργασίας	Σκοπός Επεξεργασίας	Κατηγορίες Υποκειμένων	Κατηγορίες Προσωπικών Δεδομένων	Περίοδος Διακράτησης
Λογιστήριο & Τμήμα Διαχείρισης Ανθρώπινου Δυναμικού	Πρόσβαση σε προσωπικά δεδομένα στο πλαίσιο της διεξαγωγής των εξωτερικών ελέγχων	Εξωτερικός Έλεγχος	Εν δυνάμει όλες οι κατηγορίες υποκειμένων, αναλόγως την περίπτωση	Εν δυνάμει όλες οι κατηγορίες προσωπικών δεδομένων, αναλόγως την περίπτωση	Σύμφωνα με την Πολιτική Διακράτησης Προσωπικών Δεδομένων του Οργανισμού
Λογιστήριο & Τμήμα Διαχείρισης Ανθρώπινου Δυναμικού	Διαβίβαση προσωπικών δεδομένων σε τρίτα μέρα κατόπιν αιτήματος για τη διεξαγωγή της διαδικασίας Πιστοποίησης Ταυτότητας Πελάτη (KYC, Know your customer)	Πιστοποίηση Ταυτότητας Πελάτη (KYC, Know your customer)	Διευθυντικά στελέχη, νόμιμοι εκπρόσωποι εταιρείας	Λογαριασμοί (ΔΕΚΟ), όνομα, επώνυμο, αφμ, διεύθυνση και άλλες πληροφορίες που μπορεί να ζητηθούν από τον Οργανισμό	Σύμφωνα με την Πολιτική Διακράτησης Προσωπικών Δεδομένων του Οργανισμού
Λογιστήριο & Τμήμα Διαχείρισης Ανθρώπινου Δυναμικού	Συλλογή και χρήση προσωπικών δεδομένων για την πληρωμή των λογαριασμών των εταιρικών κινητών τηλεφώνων των εργαζομένων	Διαχείριση εταιρικών κινητών τηλεφώνων των εργαζομένων	Υπάλληλοι και άτομα που λαβαίνουν μέρος στην τηλεφωνική συνομιλία	Ονοματεπώνυμο, ποσό, αριθμός κινητού, κίνηση εισερχομένων - εξερχομένων κλήσεων	Σύμφωνα με την Πολιτική Διακράτησης Προσωπικών Δεδομένων του Οργανισμού
Λογιστήριο & Τμήμα Διαχείρισης Ανθρώπινου Δυναμικού	Πρόσβαση σε προσωπικά δεδομένα στο πλαίσιο της διατήρησης του τηλεφωνικού καταλόγου των εργαζομένων	Διατήρησης του τηλεφωνικού καταλόγου	Εργαζόμενοι	Ονοματεπώνυμο, αριθμός εσωτερικού τηλεφώνου, αριθμός κινητού τηλεφώνου, διεύθυνση email	Σύμφωνα με την Πολιτική Διακράτησης Προσωπικών Δεδομένων του Οργανισμού
Λογιστήριο & Τμήμα Διαχείρισης Ανθρώπινου Δυναμικού	Συλλογή και χρήση προσωπικών δεδομένων για την κάλυψη εξόδων των υπαλλήλων	Διαχείριση εξόδων των εργαζομένων	Εργαζόμενοι	Ονοματεπώνυμο, τμήμα εργαζόμενου, ποσό εξόδων, είδος εξόδου, περιγραφή εξόδου, ημερομηνία απόδειξης	Σύμφωνα με την Πολιτική Διακράτησης Προσωπικών Δεδομένων του Οργανισμού
Λογιστήριο & Τμήμα Διαχείρισης Ανθρώπινου Δυναμικού	Συλλογή, χρήση και αποθήκευση προσωπικών δεδομένων για τη διαχείριση των πληρωμών	Εκτέλεση πληρωμών	Συνεργάτες, πελάτες και άλλα τρίτα μέρη στα οποία γίνονται πληρωμές	Ονοματεπώνυμο, ΑΦΜ, ημερομηνία γέννησης, τραπεζικά στοιχεία, αριθμός ταυτότητας ή διαβατηρίου, email	Σύμφωνα με την Πολιτική Διακράτησης Προσωπικών Δεδομένων του Οργανισμού

Υπόδειγμα Αρχείου Δραστηριοτήτων

Τεχνικά και Οργανωτικά μέτρα	Αποδέκτες/Διαβίβαση σε Τρίτα Μέρη	Από Κοινού Υπεύθυνοι Επεξεργασίας	Κατάλληλες Εγγυήσεις σε περίπτωση διαβιβάσεων σε τρίτες χώρες	Εκτίμηση Αντικτύπου	Προηγούμενη Διαβούλευση
Πολιτική Ασφάλειας Πληροφοριών, Πολιτική Διακράτησης Προσωπικών Δεδομένων, Πολιτική Ιδιωτικότητας από το σχεδιασμό και εξ ορισμού, Διαδικασία Απόκρισης και Ειδοποίησης για την Παραβίαση Προσωπικών Δεδομένων, Πολιτική Απορρήτου, Πολιτική Προστασίας Προσωπικών Δεδομένων, Διαδικασία Διαχείρισης Δικαιωμάτων των Υποκειμένων των Δεδομένων, Ρήτρες σχετικά με την προστασία προσωπικών δεδομένων σε συμβάσεις με τρίτα μέρη, Ειδοποιήσεις Απορρήτου, Παροχή Συγκατάθεσης υποκειμένων των δεδομένων, Επίβλεψη Νομικής και Κανονιστικής Συμμόρφωσης, Προσωπικοί Λογαριασμοί, Εφαρμογή διαχωρισμού Καθηκόντων, Χρήση Κωδικών , Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network, VPN) για απομακρυσμένη πρόσβαση, Ασύρματο Δίκτυο (WiFi) προστατευμένο με κωδικό, Εκπαιδεύσεις αναφορικά με την ασφάλεια των προσωπικών δεδομένων, Μέτρα Φυσικής Ασφάλειας - Κλειδωμένα γραφεία, Μέτρα Φυσικής Ασφάλειας - Ντουλάπια, Μέτρα Φυσικής Ασφάλειας στο Κέντρο Δικτύου (Data Center) - Ανιχνευτής φωτιάς & και μηχανισμοί προστασίας, Μέτρα Φυσικής Ασφάλειας στο Κέντρο Δικτύου (Data Center) - Επίβλεψη θερμοκρασίας , Μέτρα Φυσικής Ασφάλειας στο Κέντρο Δικτύου (Data Center) - Ασφαλής Καλωδίωση, Εφεδρικά αρχεία (Backups), Αντιικό λογισμικό (Antivirus), Συγχρονισμός Ρολογιού (Clock Synchronization)	Ελεγκτική Εταιρία που διενεργεί τον Οικονομικό έλεγχο, Δημόσιες Αρχές	Μ/Ε	Μ/Ε	Μ/Ε	Μ/Ε

7. Υπεύθυνος Προστασίας Δεδομένων (DPO)

Υπεύθυνος Προστασίας Δεδομένων (Άρθρο 39)

Υπεύθυνος Προστασίας Δεδομένων ορίζεται όταν:

α) η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (ανεξάρτητα από το είδος των δεδομένων που υφίστανται επεξεργασία), ή
β) εάν οι βασικές δραστηριότητες του οργανισμού συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
γ) εάν οι βασικές δραστηριότητες του οργανισμού συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.

Βασικές δραστηριότητες είναι οι σημαντικές δραστηριότητες για την επίτευξη των στόχων του οργανισμού και όλες οι δραστηριότητες για τις οποίες η επεξεργασία δεδομένων είναι απαραίτητη ώστε να πραγματοποιηθούν

Καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων (Άρθρο 39)

Ο DPO έχει τα ακόλουθα καθήκοντα:

- ✓ Να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελών την επεξεργασία καθώς και τους υπαλλήλους
- ✓ Να παρακολουθεί την συμμόρφωση με τους νόμους περί προστασίας των δεδομένων
- ✓ Να συνεργάζεται και να ενεργεί ως η επαφή για τις εποπτικές αρχές

8. Παραβίαση των Προσωπικών Δεδομένων

Τι είναι η παραβίαση 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, **”**

- Δεν συσχετίζεται με το επίπεδο ή την ποιότητα των μηχανισμών ελέγχου
- Παράμετροι Ασφάλειας: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα

Αναφορά στην Εποπτική Αρχή (Άρθρο 33)

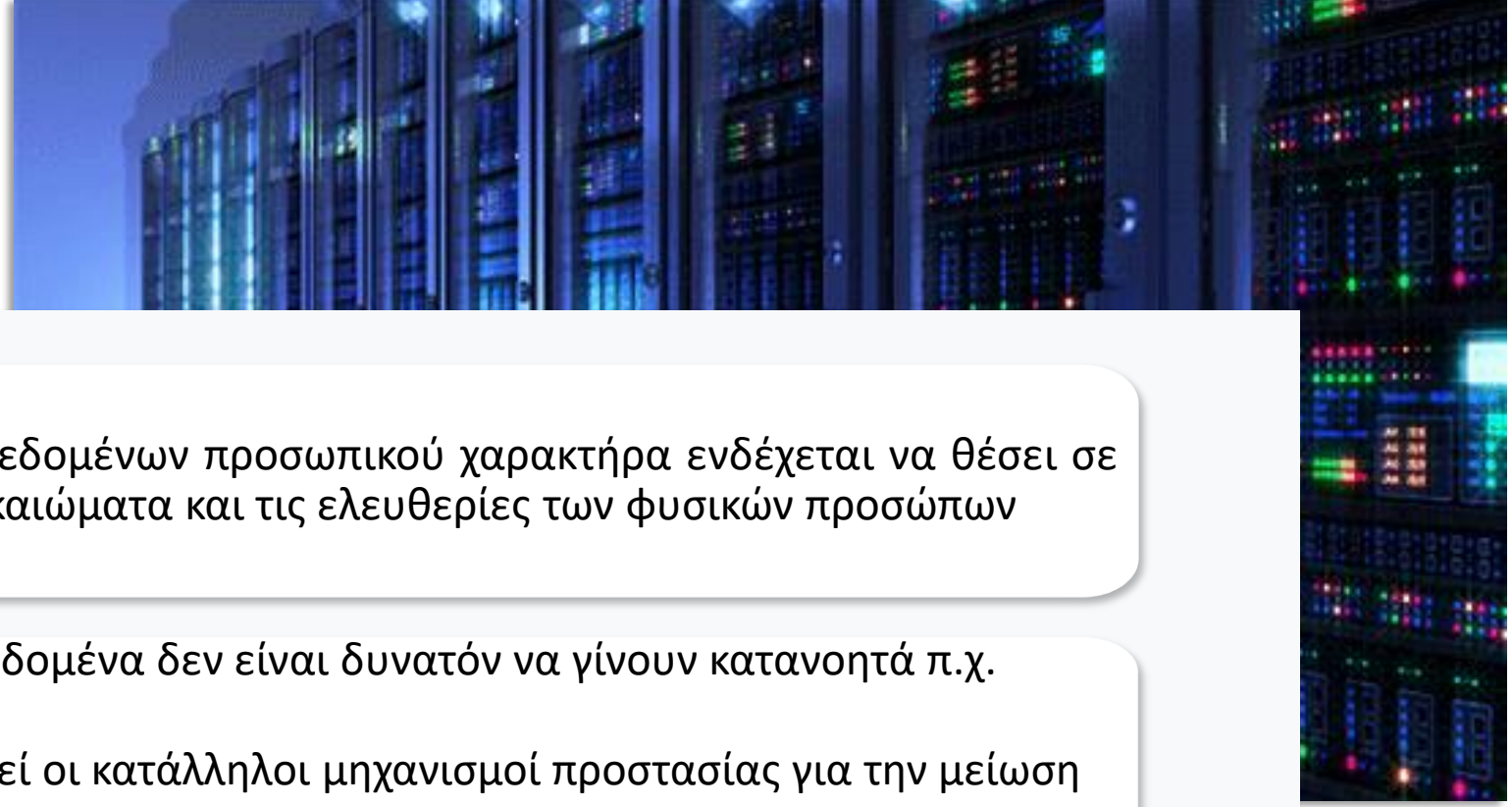
Πότε

- Χωρίς καμία καθυστέρηση
- εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος της παραβίασης των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή
- Εάν η ενημέρωση είναι > 72 ώρες: απαιτείται αιτιολόγηση

Τι περιλαμβάνεται στην αναφορά

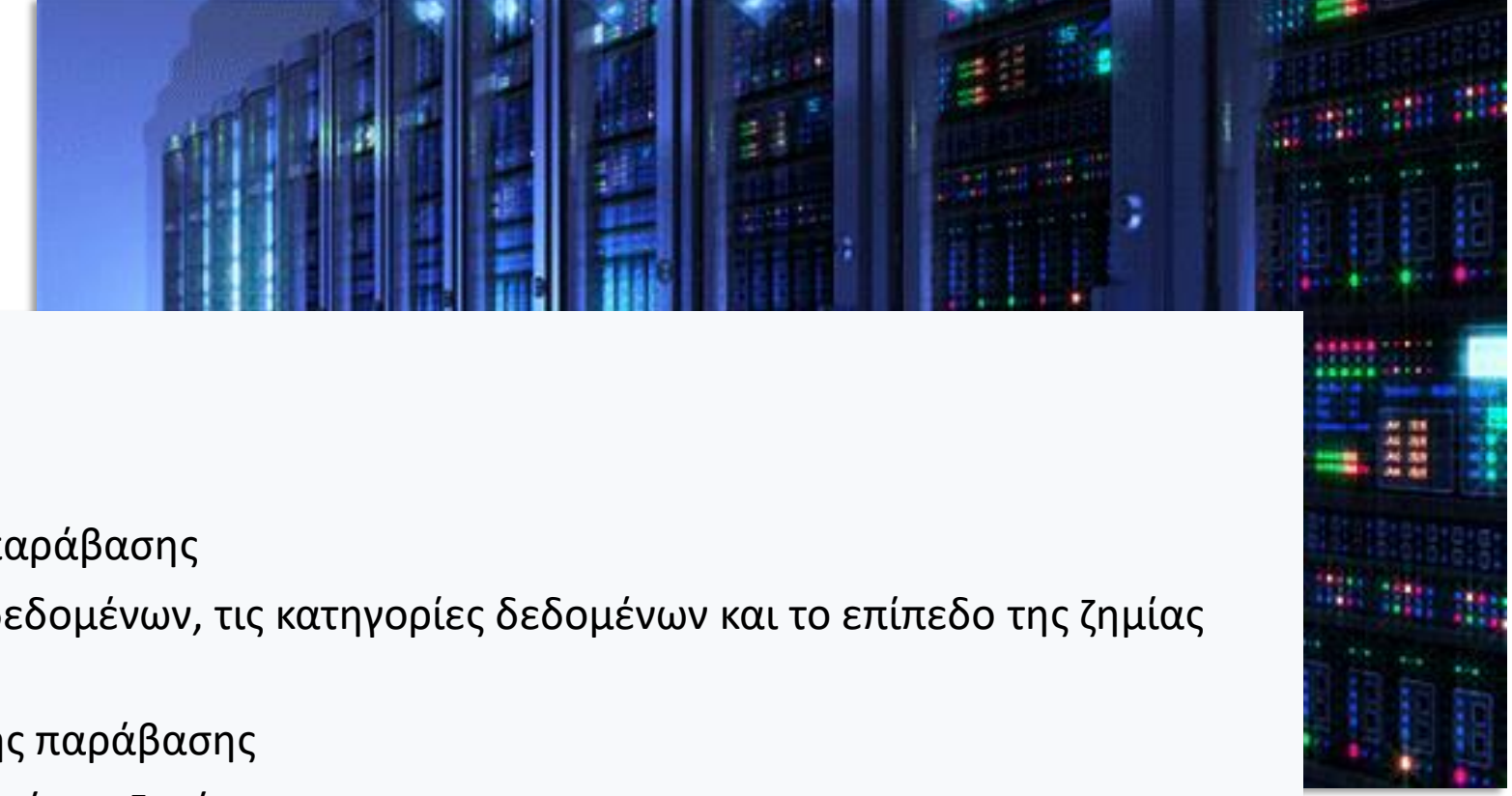
- περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα
- ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων
- περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα

Ενημέρωση των Υποκειμένων (Άρθρο 34)



Πότε;	• Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων
Εξαιρέσεις	• Εάν τα προσωπικά δεδομένα δεν είναι δυνατόν να γίνουν κατανοητά π.χ. κρυπτογραφημένα • Εάν έχουν εφαρμοσθεί οι κατάλληλοι μηχανισμοί προστασίας για την μείωση του κινδύνου
Τι;	• Οι ίδιες πληροφορίες όπως και στην γνωστοποίηση στην Εποπτική Αρχή
Πως;	• Εξ ορισμού: Κατευθείαν επικοινωνία με τα υποκείμενα • Δημόσια ανακοίνωση εάν η κατευθείαν επικοινωνία προϋποθέτει δυσανάλογες προσπάθειες

Πρόστιμα από Παραβιάσεις



Το ποσό του προστίμου εξαρτάται από:

- Τη φύση, τη σοβαρότητα και τη διάρκεια της παράβασης
- Τον αριθμό των θιγόμενων υποκειμένων των δεδομένων, τις κατηγορίες δεδομένων και το επίπεδο της ζημίας που υπέστησαν
- Τον εκ προθέσεως ή εξ αμελείας χαρακτήρα της παράβασης
- Τυχόν μέτρα που ελήφθησαν για τον περιορισμό της ζημίας
- Τα τεχνικά και οργανωτικά μέτρα
- Τυχόν προηγούμενες παραβάσεις
- Τον τρόπο με τον οποίο έγινε γνωστή η παράβαση
- Πιστοποιήσεις

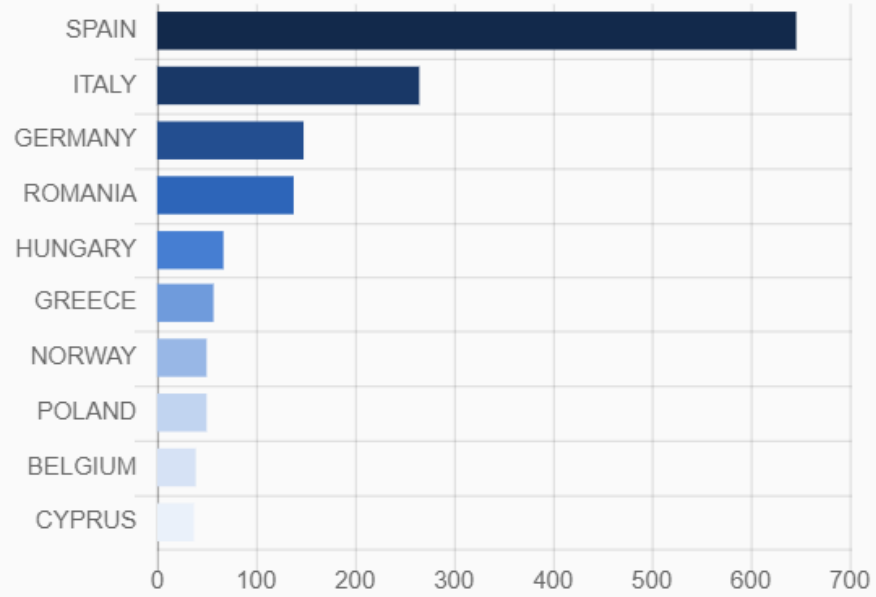
Πρόστιμα από Παραβιάσεις

Πηγή: *www.enforcementtraccker.com*

Statistics: Countries with highest fines (Top 10)

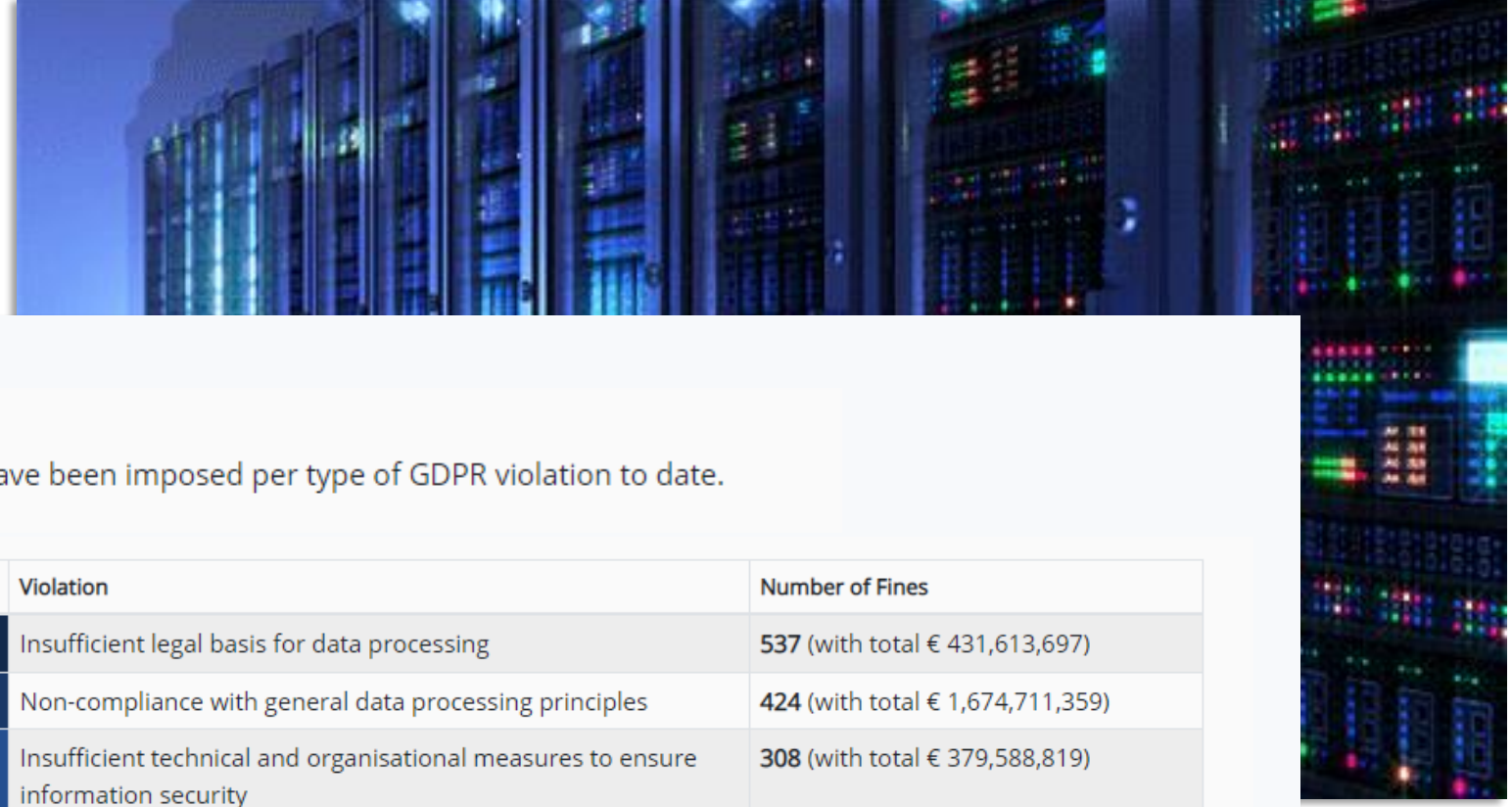
The following statistics show how many fines and what sum of fines have been imposed per country to date (only top 10 countries).

2. By total number of fines:



Country	Number of Fines
SPAIN	**646** (with total € 59,560,050)
ITALY	**265** (with total € 123,369,596)
GERMANY	**148** (with total € 54,810,633)
ROMANIA	**138** (with total € 749,250)
HUNGARY	**67** (with total € 2,313,861)
GREECE	**57** (with total € 30,601,000)
NORWAY	**50** (with total € 10,417,950)
POLAND	**50** (with total € 3,440,669)
BELGIUM	**39** (with total € 1,822,000)
CYPRUS	**37** (with total € 1,363,500)

Πρόστιμα από Παραβιάσεις

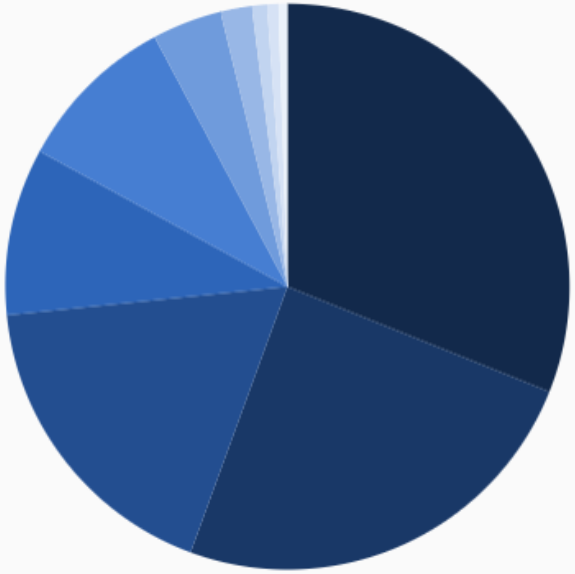


Πηγή: *www.enforcementtraccker.com*

Statistics: Fines by type of violation

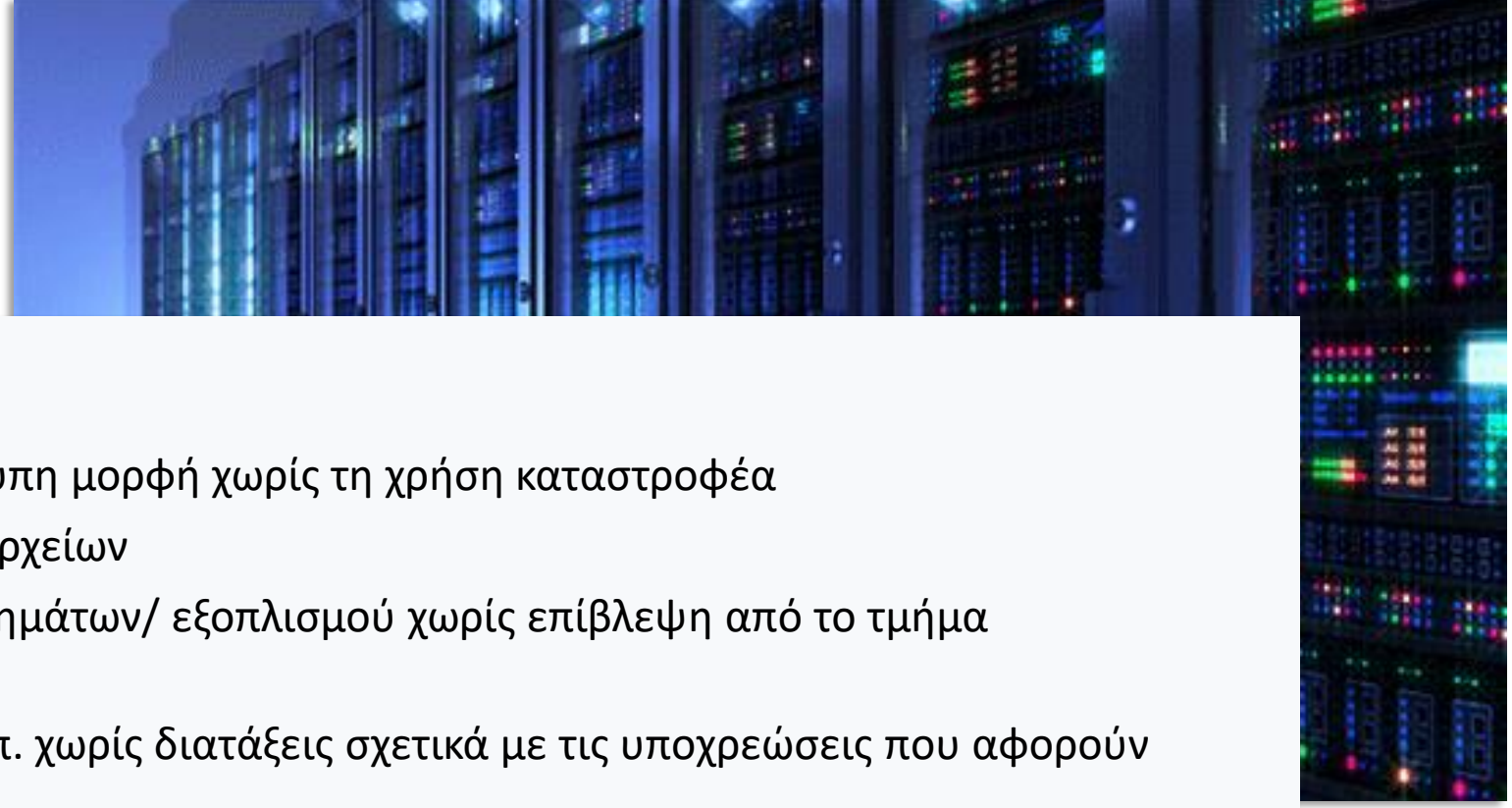
The following statistics show how many fines and what sum of fines have been imposed per type of GDPR violation to date.

2. By total number of fines:



	Violation	Number of Fines
	Insufficient legal basis for data processing	**537** (with total € 431,613,697)
	Non-compliance with general data processing principles	**424** (with total € 1,674,711,359)
	Insufficient technical and organisational measures to ensure information security	**308** (with total € 379,588,819)
	Insufficient fulfilment of information obligations	**165** (with total € 237,251,580)
	Insufficient fulfilment of data subjects rights	**160** (with total € 51,889,270)
	Insufficient cooperation with supervisory authority	**69** (with total € 840,529)
	Insufficient fulfilment of data breach notification obligations	**31** (with total € 1,778,582)
	Insufficient involvement of data protection officer	**15** (with total € 919,300)
	Insufficient data processing agreement	**11** (with total € 1,057,110)
	Unknown	**9** (with total € 9,250,000)

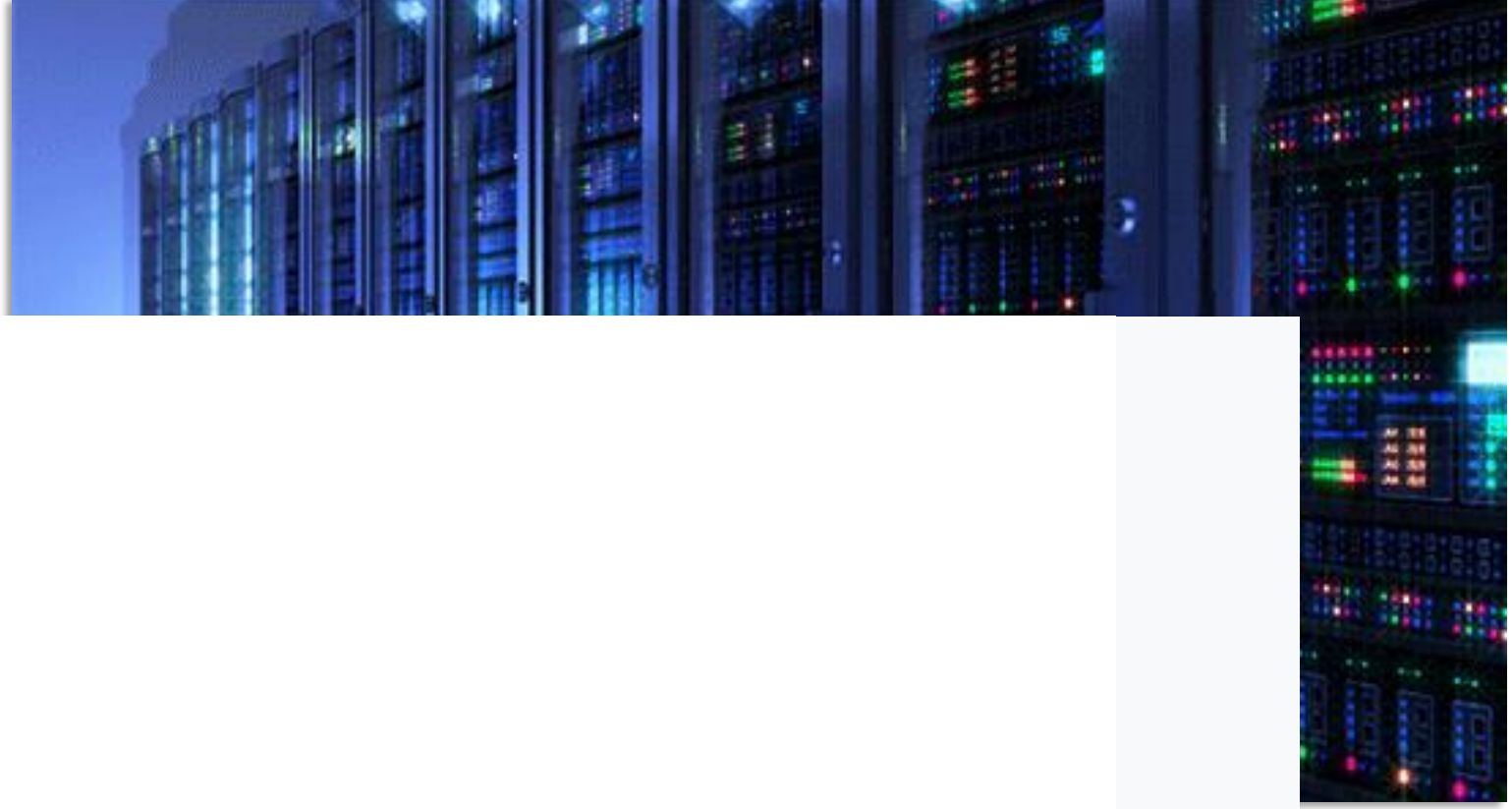
Συνήθεις αποκλίσεις



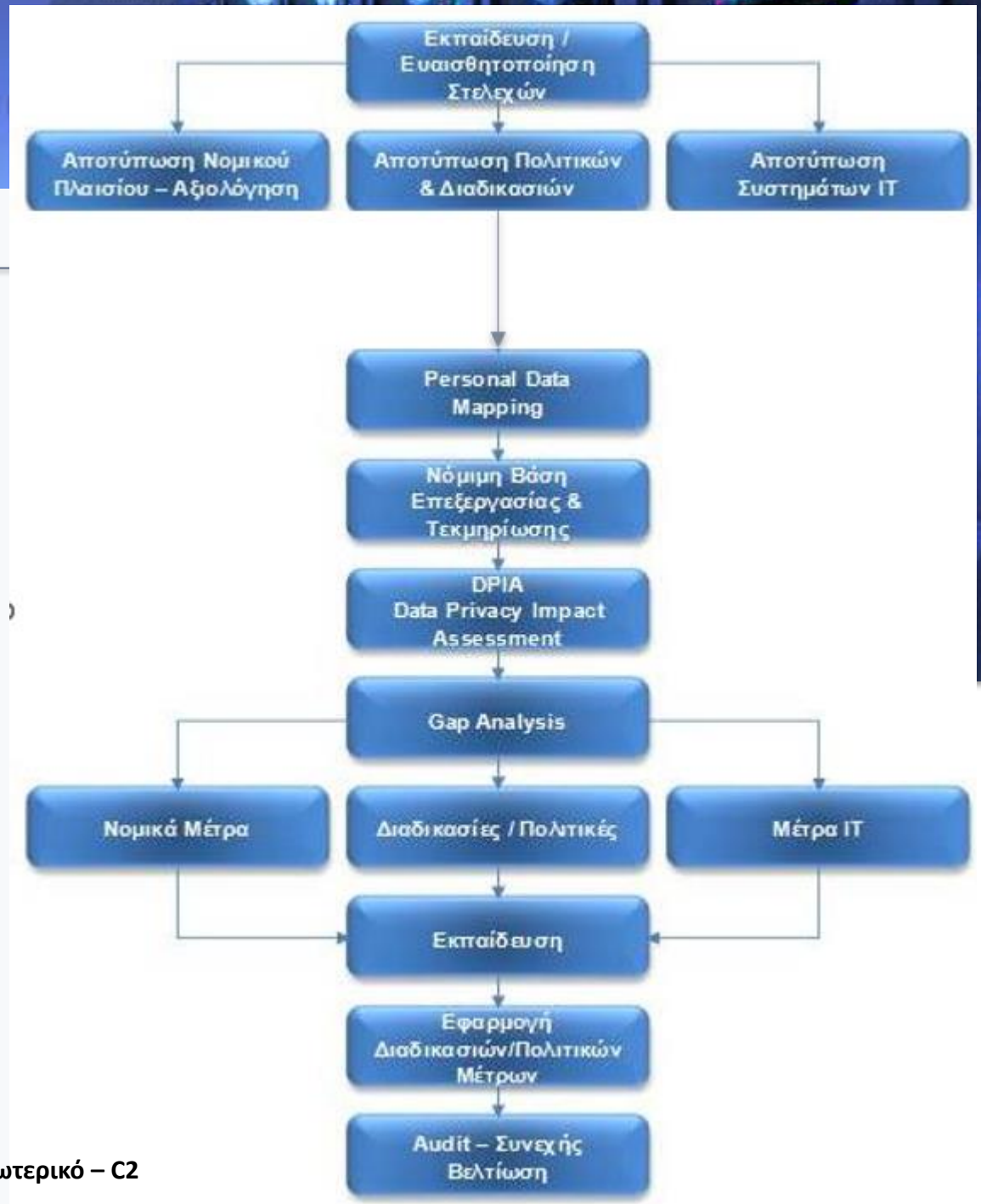
- Απόρριψη εμπιστευτικών πληροφοριών σε έντυπη μορφή χωρίς τη χρήση καταστροφέα
- Εκτεθειμένοι φάκελοι σε γραφεία, ντουλάπια αρχείων
- Πρόσβαση συνεργατών για τη συντήρηση συστημάτων/ εξοπλισμού χωρίς επίβλεψη από το τμήμα πληροφορικής
- Συμβάσεις με υπεργολάβους, προμηθευτές κ.λπ. χωρίς διατάξεις σχετικά με τις υποχρεώσεις που αφορούν θέματα διαχείρισης προσωπικών δεδομένων
- Αποθήκευση αρχείων προσωπικών δεδομένων τοπικά στον Η/Υ
- Αποκάλυψη κωδικών πρόσβασης σε εφαρμογές
- Αποθήκευση προσωπικών δεδομένων σε μονάδες USB, εξωτερικούς σκληρούς δίσκους κ.λπ. με μη ελεγχόμενο τρόπο
- Αποστολή προσωπικών δεδομένων μέσω μη κρυπτογραφημένου ηλεκτρονικού ταχυδρομείου

Πηγή:

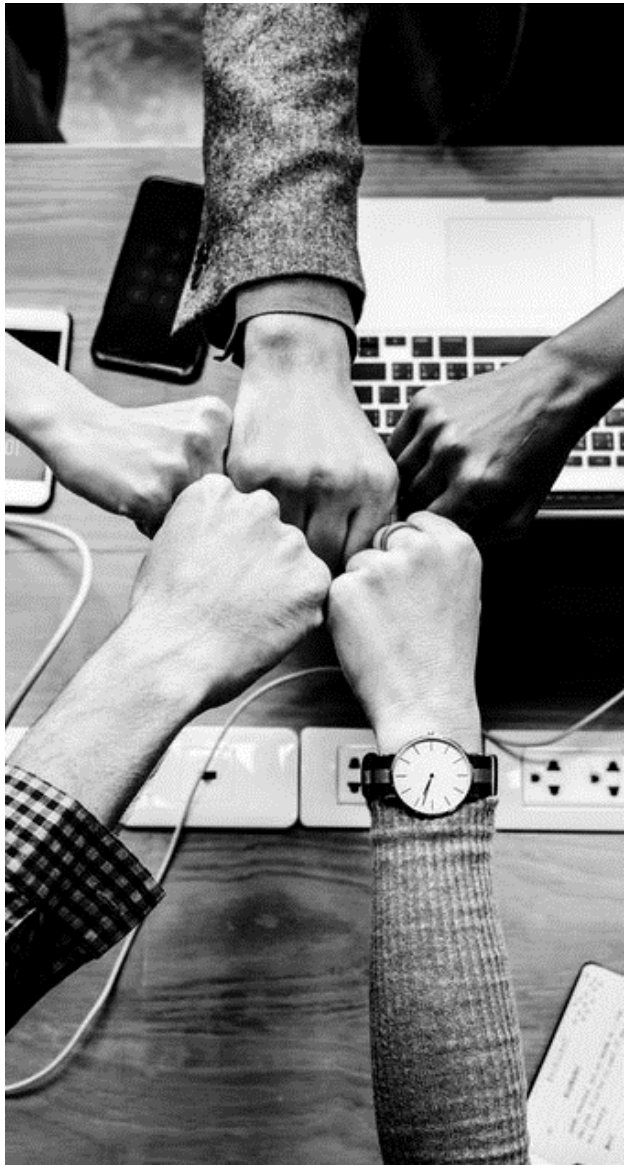
https://www.youtube.com/watch?v=iH8rj0oezu8



Τα βήματα εφαρμογής του κανονισμού



ΕΡΩΤΗΣΕΙΣ



ADACOM

SECURITY
BUILT ON TRUST

www.adacom.com

Ευχαριστώ!

GREECE

25 Kreontos Str.,
104 42, Athens
+30 210 5193740

UNITED KINGDOM

8950 Fitness Lane,
Suite 100 Fishers, IN 46037
+44(0) 317 588 3131

CYPRUS

10 Katsoni Str.,
1082, Nicosia
+357 22 444 071

KINGDOM OF BAHRAIN

Manama Center, Blog: 316
Road: 383, Building: 128
Flat/Office: 2030