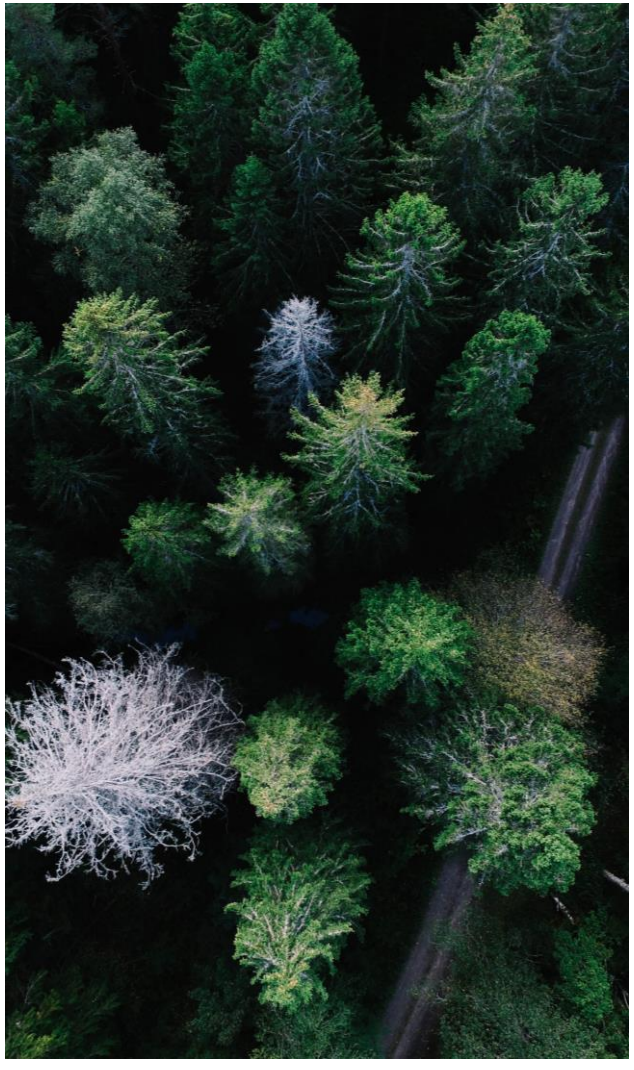
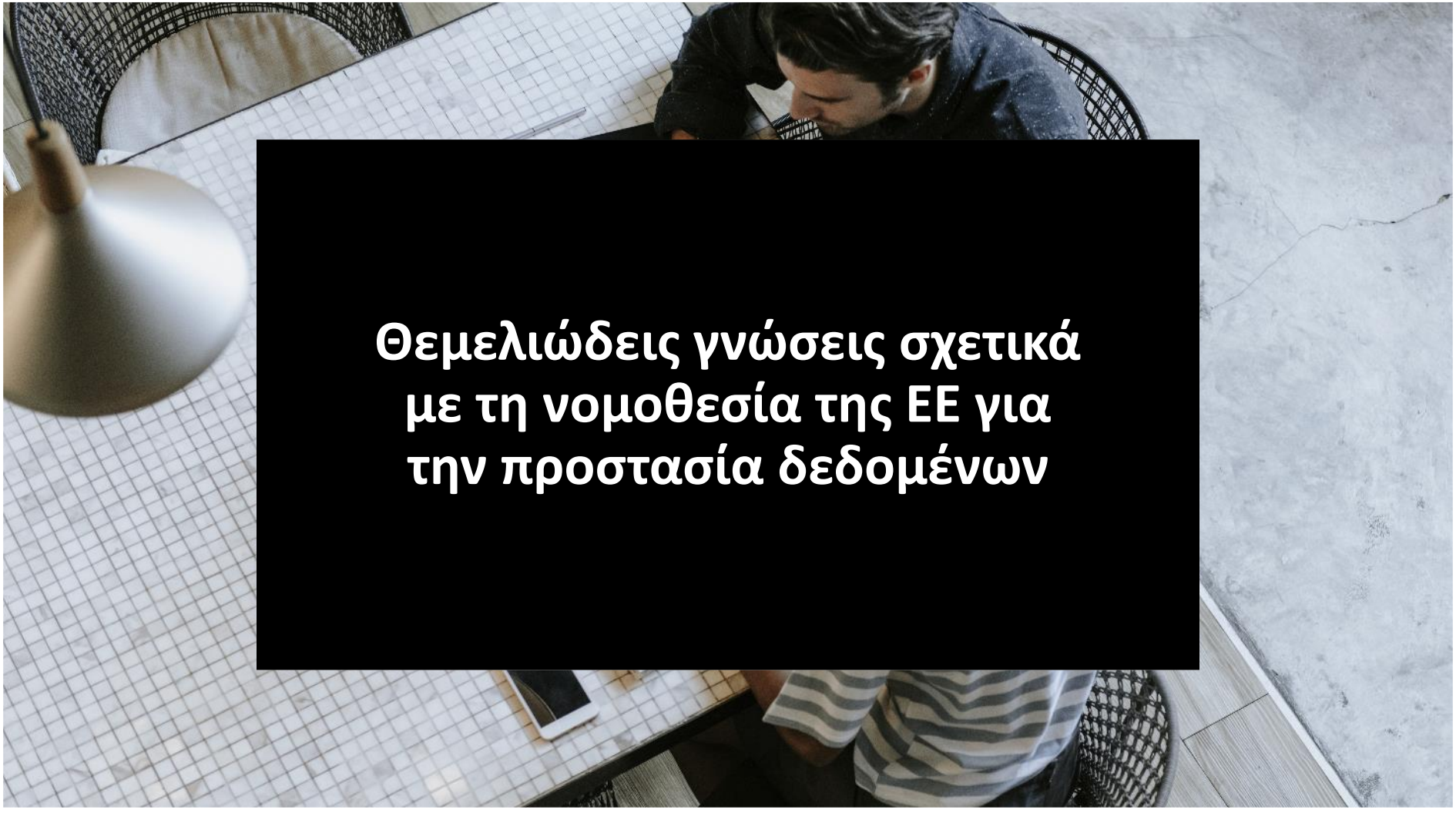
Εκπαίδευση Ευαισθητοποίησης Προσωπικών Δεδομένων

Χαροκόπειο Πανεπιστήμιο

Baker Tilly
South East Europe





Θεμελιώδεις γνώσεις σχετικά με τη νομοθεσία της ΕΕ για την προστασία δεδομένων

…πλέον θέμα συμμόρφωσης με Ευρωπαϊκή νομοθεσία

Ευρωπαϊκή Ένωση

Ισχυροποίηση νομοθεσίας και απαίτηση για ενιαία εφαρμογή σε όλα τα κράτη μέλη της ΕΕ

Ισχυροποίηση Δικαιωμάτων Υποκειμένων Δεδομένων

Ο νέος Κανονισμός (GDPR) ενισχύει τα δικαιώματα των φυσικών προσώπων και τον έλεγχο των ΔΠΧ που τους αφορούν

Δεδομένα Προσωπικού Χαρακτήρα (ΔΠΧ)

Αφορά

- Κάθε οργανισμό που επεξεργάζεται ΔΠΧ Ευρωπαίων πολιτών
- Κάθε φυσικό πρόσωπο, πολίτη ΕΕ (υποκείμενα των δεδομένων)
- Κάθε συνεργαζόμενη, τρίτη, εταιρία ενός οργανισμού στον ιδιωτικό και δημόσιο τομέα

Σε ισχύ από 25/5/2018

Πολύ υψηλά πρόστιμα και ποινές μη συμμόρφωσης

GDPR: ένας Κανονισμός που επηρεάζει οριζόντια όλες τις αγορές

Επεξεργασία Βάσει Κανόνων & Αρχών

Νομιμότητα, Αντικειμενικότητα Διαφάνεια

- Συλλογή & επεξεργασία ΔΠΧ μόνο στο πλαίσιο συμβατής νομικής βάσης (π.χ. συγκατάθεση, έννομο συμφέρον, νομική υποχρέωση κ.α.)
- Παροχή πλήρους ενημέρωσης κατά την συλλογή ΔΠΧ

Δικαιώματα Υποκειμένων

- Λήθη / Διαγραφή ΔΠΧ
- Πρόσβαση/Ενημέρωση
- Διόρθωση ΔΠΧ
- Εναντίωση ή / και παύση περαιτέρω Επεξεργασίας ΔΠΧ
- Άρση αρχικής συγκατάθεσης
- Ενημέρωση για κάθε επεξεργασία που οδηγεί σε αυτοματοποιημένη λήψη αποφάσεων (συμπεριλαμβανομένης της κατάρτισης προφίλ)

Ελαχιστοποίηση ΔΠΧ

Τα ΔΠΧ είναι κατάλληλα, συναφή και περιορίζονται στο απολύτως αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

Περιορισμός Σκοπού

Συλλογή μόνο των αναγκαίων ΔΠΧ για τους σκοπούς της επεξεργασίας

Ακρίβεια

Επεξεργασία ΔΠΧ που εξασφαλίζουν την ακρίβεια και ακεραιότητα αυτών

Εμπιστευτικότητα & Ακεραιότητα

Αποτελεσματικά τεχνικά & οργανωτικά μέτρα προστασίας και ασφάλειας ΔΠΧ

Διατήρηση / Διαγραφή ΔΠΧ

Διαγραφή ΔΠΧ όταν παύει να ισχύει πλέον ο σκοπός για τον οποίο αρχικά συλλέχθηκαν

Απαίτηση Συμμόρφωσης Με Αποδείξεις

DPO

- DPO
- Ανάθεση ρόλου Υπεύθυνου Προστασίας ΔΠΧ
- Εξασφάλιση ανεξαρτησίας αναφορών

Διακυβέρνηση

- Λογοδοσία & Υπευθυνότητα
- Έλεγχος Συμμόρφωσης
- Πολιτικές & Διαδικασίες προστασίας
- Εκπαίδευση Υπαλλήλων
- Οργανωτική Δομή Προστασίας ΔΠΧ

Μητρώα Επεξεργασίας

Ανάπτυξη μητρώων:

- Επεξεργασίας ΔΠΧ
- Διαβίβασης ΔΠΧ
- Συνεργαζόμενων 3ΩΝ
- Τεχνολογιών Επεξεργασίας

ΕΑΠΔ / DPIAs

Μελέτες Εκτίμησης Αντικτύπου σε κάθε νέα, σημαντική / κρίσιμη επεξεργασία ΔΠΧ

Διαχείριση 72 ωρών

Άμεση διαχείριση σε περίπτωση περιστατικού διαρροής ΔΠΧ, Ενημέρωση, Γνωστοποίηση εντός 72 ωρών από την εκδήλωση

Διαχείριση Κινδύνων

- Έλεγχος & Αξιολόγηση Κινδύνων, Αναφορές
- Μηχανισμοί Προστασίας
- Διαχείριση Παραπόνων

Σχέσεις με Τρίτους

- Συμβατικό πλαίσιο μεταξύ Υπεύθυνων / Εκτελούντων την Επεξεργασία
- Παρακολούθηση Προστασίας ΔΠΧ Τρίτων

Εμπιστοσύνη

Ανάπτυξη πλαισίου εμπιστοσύνης & συνεργασίας με την Αρχή και τα Υποκείμενα Δεδομένων:

- Διαβουλεύσεις με την Αρχή για κρίσιμες επεξεργασίες ΔΠΧ
- Ικανοποίηση αιτημάτων Υποκειμένων και παροχή πληροφοριών για τα ΔΠΧ τους
- Ανάπτυξη και Δημοσίευση Πολιτικών Απορρήτου

Εισαγωγή

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) (ΕΕ) 2016/679 εγκρίθηκε από την Ευρωπαϊκή Επιτροπή τον Απρίλιο του 2016 και εφαρμόζεται σε όλα τα κράτη μέλη της ΕΕ από τις 25 Μαΐου 2018. Ως «κανονισμός» και όχι ως «οδηγία», οι απαιτήσεις του ισχύουν άμεσα για όλα τα κράτη μέλη, αντικαθιστώντας τους ισχύοντες τοπικούς νόμους για την προστασία των δεδομένων και καταργώντας ή / και αντικαθιστώντας την οδηγία 95/46 / ΕΚ και τη νομοθεσία εφαρμογής των κρατών μελών.

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) δημιουργήθηκε για να προσδώσει μια ενιαία και συνεπή προσέγγιση στην προστασία προσωπικών πληροφοριών και την ανταλλαγή δεδομένων σε όλη την ΕΕ, να αντιμετωπίσει την πρόοδο της τεχνολογίας και των κοινωνικών μέσων ενημέρωσης και να βελτιώσει και ενισχύσει τη συναίνεση και την πρόσβαση των φυσικών προσώπων στα δεδομένα τους.

Αφορά στην προστασία και νομιμότητα επεξεργασίας των προσωπικών δεδομένων των Ευρωπαίων Πολιτών από κάθε εταιρία ή οργανισμό που επεξεργάζεται τα δεδομένα αυτά τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα

Βασικές Έννοιες & Ορισμοί

Προσωπικά Δεδομένα σημαίνει οποιαδήποτε πληροφορία σχετικά με αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο («υποκείμενο δεδομένων»). Ένα αναγνωρίσιμο φυσικό πρόσωπο είναι ένα πρόσωπο το οποίο μπορεί να αναγνωριστεί άμεσα ή έμμεσα, ιδίως με αναφορά σε αναγνωριστικό στοιχείο όπως όνομα, αριθμό ταυτότητας, δεδομένα τοποθεσίας, ηλεκτρονικό αναγνωριστικό ή σε ένα ή περισσότερα στοιχεία που είναι συγκεκριμένα για την φυσική, φυσιολογική, γενετική, πνευματική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του φυσικού προσώπου

Ειδικές Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα (Ευαίσθητα Δεδομένα), περιλαμβάνουν τα προσωπικά δεδομένα που αποκαλύπτουν φυλετική ή εθνική καταγωγή πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συνδικαλιστική δράση, σεξουαλικό προσανατολισμό, ασθένεια ή κατάσταση σωματικής ή / και ψυχικής υγείας, γενετικά ή βιομετρικά δεδομένα για τον μοναδικό προσδιορισμό ενός ατόμου

Υποκείμενο Δεδομένων: το φυσικό πρόσωπο που αποτελεί το υποκείμενο προσωπικών δεδομένων.

Επεξεργασία Δεδομένων: κάθε εργασία ή σύνολο εργασιών που εκτελείται σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε αυτοματοποιημένα είτε όχι, όπως συλλογή, καταγραφή, οργάνωση, διαμόρφωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, διαβούλευση, χρήση γνωστοποίηση μέσω μετάδοσης, διάδοσης ή άλλης διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής

Βασικές Έννοιες & Ορισμοί

Υπεύθυνος Επεξεργασίας, είναι το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, οργανισμός ή άλλος φορέας ο οποίος, από μόνος του ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα (ΔΠΧ).

Εκτελών την Επεξεργασία, είναι το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας και κατόπιν ρητών, καταγεγραμμένων εντολών του.

Κάθε ρόλος έχει διαφορετικές υποχρεώσεις συμμόρφωσης ως προς τον νέο Γενικό Κανονισμό Προστασίας ΔΠΧ

Η *Εποπτική Αρχή ή Αρχή Προστασίας Δεδομένων* (DPA) στο πλαίσιο του GDPR είναι μια ανεξάρτητη δημόσια αρχή που έχει συσταθεί από κάθε κράτος μέλος για την επίβλεψη, την υποστήριξη και την επιβολή του κανονισμού. Η αρμόδια Αρχή στην Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr)

Κατάρτιση Προφίλ είναι κάθε μορφή, αυτοματοποιημένης ή μη, επεξεργασίας δεδομένων προσωπικού χαρακτήρα που αποτελείται από την χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση και κατηγοριοποίηση ορισμένων προσωπικών δεδομένων που αφορούν τα φυσικά πρόσωπα, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση των φυσικών προσώπων στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα συμφέροντα, την αξιοπιστία, τη συμπεριφορά, τη τοποθεσία ή τις κινήσεις αυτών

Εφαρμοστικό Πλαίσιο & Ποινές

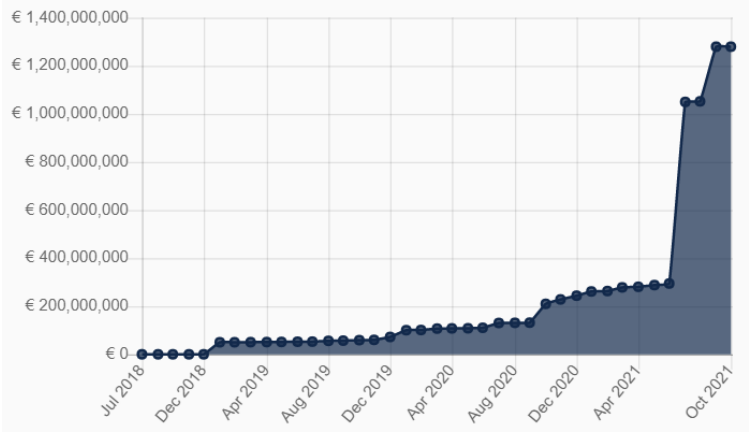
Στόχος του νέου Κανονισμού (GDPR) - είναι να προστατεύσει όλους τους πολίτες της ΕΕ από παραβάσεις απορρήτου δεδομένων προσωπικού χαρακτήρα. Τα βασικά σημεία και χαρακτηριστικά του GDPR καθώς και πληροφορίες για τις επιπτώσεις που επιφέρει στους οργανισμούς περιγράφονται πιο κάτω.

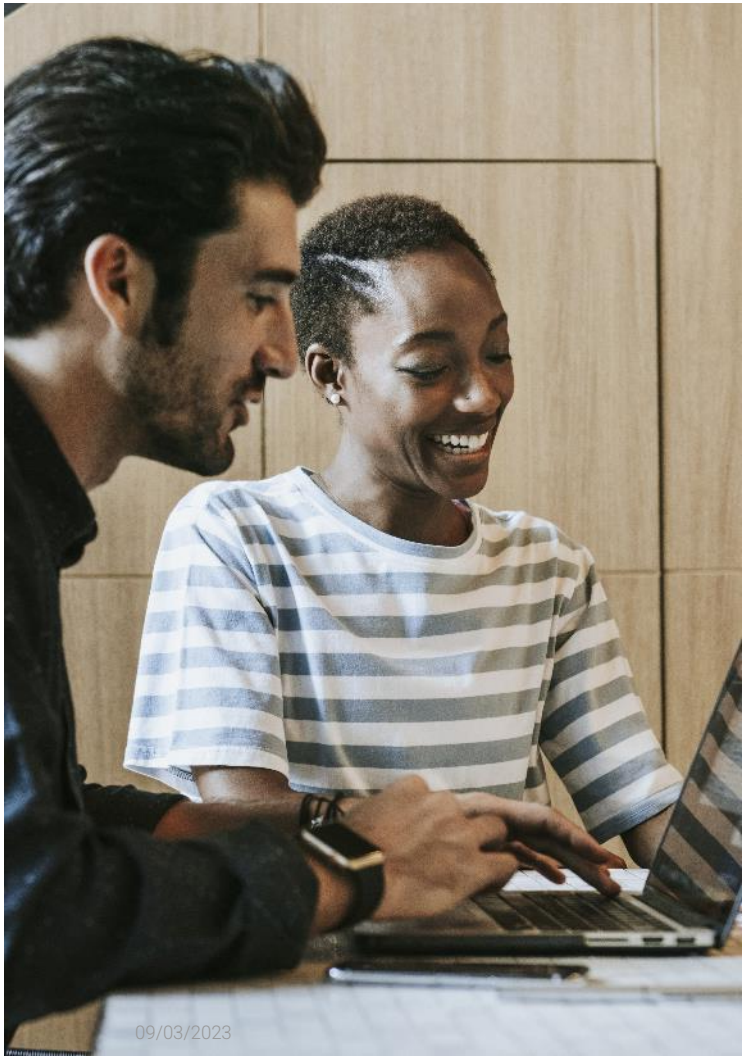
Εμβέλεια Εφαρμογής - Αναμφισβήτητα η μεγαλύτερη αλλαγή στο ρυθμιστικό περιβάλλον αναφορικά με την προστασία των προσωπικών δεδομένων έχει να κάνει με την εκτεταμένη εφαρμογή του GDPR, καθώς ισχύει για όλες τις εταιρείες και οργανισμούς που επεξεργάζονται προσωπικά δεδομένα φυσικών προσώπων στην ΕΕ ανεξαρτήτως της τοποθεσίας και του είδους δραστηριοποίησης της εταιρείας/οργανισμού.

Ποινές και Πρόστιμα - Οι οργανισμοί που παραβιάζουν τον Κανονισμό μπορούν να υποστούν ποινές και πρόστιμα έως 4% του ετήσιου συνολικού κύκλου εργασιών ή € 20 εκατ. (όποιο είναι μεγαλύτερο). Αυτό είναι το μέγιστο πρόστιμο που μπορεί να επιβληθεί για τις πολύ σοβαρές παραβάσεις (π.χ. συνεχής επεξεργασία χωρίς τη συγκατάθεση των υποκειμένων, εκτεταμένη διαρροή δεδομένων προσωπικού χαρακτήρα λόγω πλημμελούς πλαισίου ασφάλειας κλπ.). Είναι σημαντικό να σημειωθεί ότι αυτοί οι κανόνες ισχύουν τόσο για τους υπεύθυνους επεξεργασίας όσο και για τους εκτελούντες την επεξεργασία.

Εφαρμοστικό Πλαίσιο & Ποινές

Τα διοικητικά πρόστιμα που απορρέουν από τον GDPR και έχουν επιβληθεί από τις Αρχές Προστασίας Δεδομένων των κρατών μελών της ΕΕ ανέρχονται σε σχεδόν 1,3 δισ. €. Η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από την ημερομηνία ισχύος του Κανονισμού μέχρι σήμερα έχει επιβάλει διοικητικά πρόστιμα ύψους 864.000 €





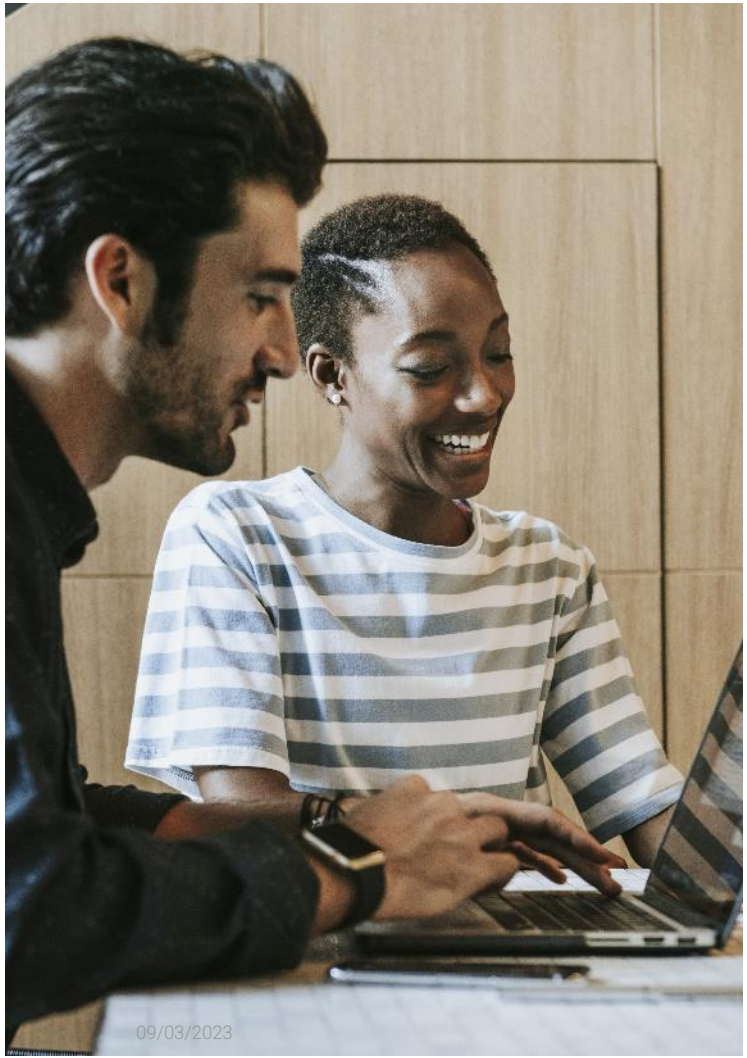
Αρχές / Κανόνες Επεξεργασίας ΔΠΧ

Αρχές / Κανόνες Επεξεργασίας ΔΠΧ

- Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας. Σύμφωνα με τη συγκεκριμένη αυτή αρχή, τα δεδομένα θα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η διαφάνεια απαιτεί η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση.
- Η αρχή του περιορισμού του σκοπού, σύμφωνα με την οποία, τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.
- Η αρχή της αναλογικότητας «ελαχιστοποίηση των δεδομένων», σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι πρόσφορα, συναφή και αναγκαία για τους επιδιωκόμενους σκοπούς επεξεργασίας.
- Η αρχή της ακρίβειας των δεδομένων, σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή, να επικαιροποιούνται και να λαμβάνονται τα κατάλληλα μέτρα για την άμεση διόρθωση ή διαγραφή ανακριβών σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας δεδομένων.
- Η αρχή της «ακεραιότητας και εμπιστευτικότητας», σύμφωνα με την οποία τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους.

Αρχές / Κανόνες Επεξεργασίας ΔΠΧ

- Η αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας «περιορισμός της περιόδου αποθήκευσης», σύμφωνα με την οποία τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας.
- Η αρχή της λογοδοσίας του υπευθύνου επεξεργασίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και θα πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή με τον Κανονισμό ενώπιον των εποπτικών αρχών και των δικαστηρίων.
- Ακεραιότητα και Εμπιστευτικότητα. Τα δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία με τρόπο που εξασφαλίζει την κατάλληλη ασφάλεια, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, από τυχαία απώλεια, καταστροφή χρησιμοποιώντας κατάλληλα τεχνικά ή οργανωτικά μέτρα



Πότε επιτρέπεται να επεξεργάζεστε προσωπικά δεδομένα;

- Το άρθρο 6 του GDPR απαριθμεί περιπτώσεις κατά τις οποίες είναι νόμιμη η επεξεργασία δεδομένων προσωπικού χαρακτήρα
  - Συγκατάθεση
  - Σύναψη σύμβασης
  - Συμμόρφωση με νομική υποχρέωση
  - Ζωτικό συμφέρον
  - Εκτέλεση έργου προς το δημόσιο συμφέρον
  - Έννομο συμφέρον

Νομικές Βάσεις Συλλογής & Επεξεργασίας ΔΠΧ

Η συλλογή και επεξεργασία των ΔΠΧ από μια εταιρία είναι σύννομη και επιτρέπεται μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις (νομικές βάσεις συλλογής και επεξεργασίας):

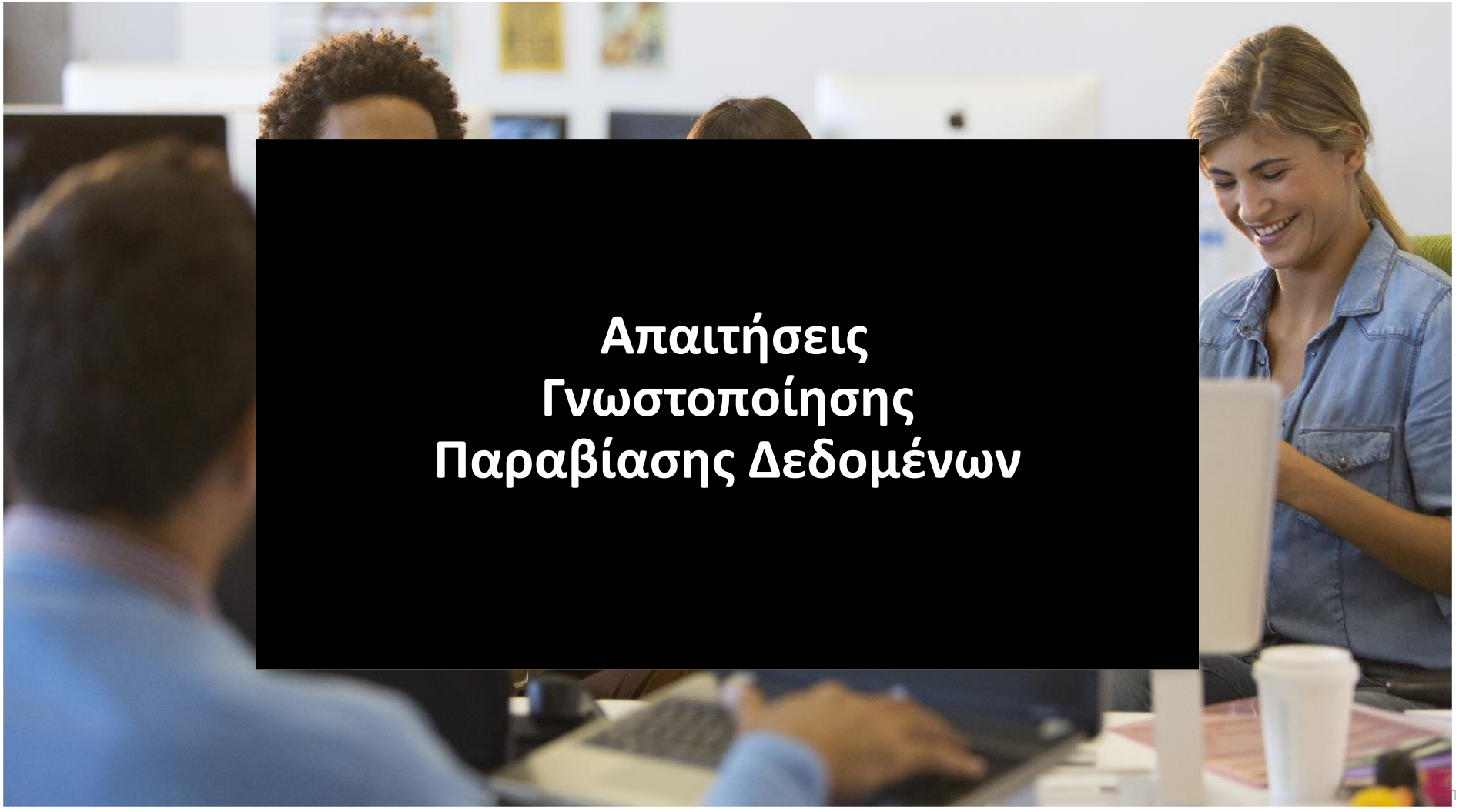
- Συναίνεση / Συγκατάθεση: το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς (πχ συγκατάθεση για επικοινωνία για προωθητικές ενέργειες, συγκατάθεση για διατήρηση βιογραφικών υποψηφίων)
- Εκτέλεση Σύμβασης: η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης (πχ. φορολογικά στοιχεία πελατών, προμηθευτών κλπ.)
- Νομική Υποχρέωση: η επεξεργασία είναι απαραίτητη για τη συμμόρφωση του Υπεύθυνου ή/και Εκτελούντα την Επεξεργασία με συγκεκριμένη νομική υποχρέωση (πχ επεξεργασία δεδομένων υπαλλήλων στη βάση της εργατικής νομοθεσίας)

Νομικές Βάσεις Συλλογής & Επεξεργασίας ΔΠΧ

- Ζωτικό Συμφέρον: η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων / φυσικού προσώπου (πχ επεξεργασία δεδομένων υγείας ασθενών για την σωστή περίθαλψή τους)
- Δημόσιο Συμφέρον: 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 (πχ επεξεργασία δεδομένων εγκληματικής συμπεριφοράς ή απάτης)
- Έννομο Συμφέρον: η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί (πχ επεξεργασία δυσμενών δεδομένων φυσικών προσώπων)

Η Έννοια Της Συγκατάθεσης

- Όταν η ζητούμενη επεξεργασία στηρίζεται στην νομική βάση της Συγκατάθεσης του υποκειμένου, δηλαδή στην συμφωνία του για την επιδιωκόμενη ενέργεια, τότε οι όροι και προϋποθέσεις της επεξεργασίας θα πρέπει να είναι απλοί, κατανοητοί και να μην αφήνουν καμία αμφιβολία ως προς το νόημα και τον σκοπό εκτέλεσης.
- Τα υποκείμενα των δεδομένων έχουν το δικαίωμα να άρουν την Συγκατάθεσή τους οποιαδήποτε στιγμή το επιθυμήσουν και πρέπει να σεβαστείτε την απόφασή τους. Για αυτόν τον σκοπό οι Υπεύθυνοι Επεξεργασίας θα πρέπει να παρέχουν τα κατάλληλα εργαλεία και υποδομές ώστε ή άρση αυτή να πραγματοποιείται το ίδιο εύκολα όπως η αρχική συλλογή της. Δεν μπορείτε απλώς να αλλάξετε τη νομική βάση της επεξεργασίας σε μία από τις άλλες αιτιολογήσεις.
- Τα παιδιά κάτω των 13 ετών μπορούν να δώσουν τη συγκατάθεσή τους μόνο με την άδεια του γονέα τους.
- Πρέπει να κρατάτε αποδεικτικά έγγραφα συγκατάθεσης.
- Εδώ θα πρέπει να υπενθυμίσουμε ότι η Συγκατάθεση δεν είναι η μοναδική νομική βάση επεξεργασίας δεδομένων αλλά μια από τις έξι κύριες νομικές βάσεις που δικαιολογούν συλλογή και επεξεργασία ΔΠΧ.


Απαιτήσεις
Γνωστοποίησης
Παραβίασης Δεδομένων

Απαιτήσεις Γνωστοποίησης Παραβίασης Δεδομένων

Σύμφωνα με τον νέο Κανονισμό (GDPR), η κοινοποίηση – γνωστοποίηση ενός **σοβαρού περιστατικού διαρροής ΔΠΧ** προς την αρμόδια Αρχή, αλλά και προς τα υποκείμενα που ζημιώθηκαν είναι επιτακτική και υποχρεωτική (ειδικά όταν το περιστατικό μπορεί να οδηγήσει σε κίνδυνο των δικαιωμάτων και ελευθεριών των ατόμων). **Για αυτόν τον λόγο κάθε περιστατικό διαρροής ΔΠΧ (ακόμα και υπόνοιας διαρροής) θα πρέπει να αναφέρεται άμεσα στα αρμόδια εταιρικά τμήματα για την έγκαιρη και αποτελεσματική διαχείριση της υπόθεσης)**

Απαιτήσεις Γνωστοποίησης Παραβίασης Δεδομένων

Η γνωστοποίηση του περιστατικού θα πρέπει να πραγματοποιηθεί χωρίς καθυστέρηση και **εντός 72 ωρών** από την στιγμή που θα γίνει αντιληπτό. Συμμετοχή σε αυτήν την υποχρέωση έχουν και οι συνεργαζόμενες τρίτες εταιρίες (εκτελούντες την επεξεργασία) οι οποίες θα πρέπει επίσης άμεσα να ενημερώσουν τους πελάτες τους για τυχόν εκδήλωση ενός περιστατικού διαρροής ΔΠΧ.

Οι εταιρίες και οργανισμοί θα πρέπει να θεσπίζουν κατάλληλες διαδικασίες και μηχανισμούς έγκαιρης εξακρίβωσης και διαχείρισης περιστατικών ασφάλειας που δύναται να οδηγήσουν σε διαρροή ή απώλεια ΔΠΧ

Δικαιώματα Φυσικών Προσώπων

Στο πλαίσιο των απαιτήσεων του Νέου Γενικού Κανονισμού (GDPR), τα υποκείμενα δεδομένων έχουν πολύ ισχυρά δικαιώματα αναφορικά με την συλλογή και επεξεργασία των δεδομένων τους. Οι εταιρίες (Υπεύθυνοι Επεξεργασίας και οι Εκτελούντες την Επεξεργασία) θα πρέπει να ανταποκρίνονται εγκαίρως στα τυχόν αιτήματα των υποκειμένων αναφορικά με τα δικαιώματά τους

Δικαιώματα Φυσικών Προσώπων

– **Δικαίωμα διόρθωσης:** Ο GDPR περιλαμβάνει το δικαίωμα των ατόμων να διορθώνουν ή να συμπληρώνουν ανακριβή προσωπικά δεδομένα εάν είναι ελλιπή. Ένα άτομο μπορεί να υποβάλει αίτημα διόρθωσης προφορικά ή γραπτά. Ωστόσο, οι εταιρείες θα πρέπει να είναι σε θέση να ταυτοποιήσουν το φυσικό πρόσωπο που ζητά τη διόρθωση.
– **Δικαίωμα αντίρρησης:** Ο GDPR δίνει στα άτομα το δικαίωμα να αντιταχθούν στην επεξεργασία των προσωπικών τους δεδομένων σε ορισμένες περιπτώσεις. (ειδικά όταν η επεξεργασία βασίζεται στη νομική βάση της Συναίνεσης)

Δικαιώματα Φυσικών Προσώπων

– **Δικαίωμα πρόσβασης:** Μέρος των διευρυμένων δικαιωμάτων των υποκειμένων των δεδομένων που περιγράφονται από τον GDPR είναι το δικαίωμα των υποκειμένων των δεδομένων να έχουν πρόσβαση και να λαμβάνουν επιβεβαίωση από τον υπεύθυνο επεξεργασίας για το εάν τα προσωπικά δεδομένα που τα αφορούν υποβάλλονται σε επεξεργασία, πού και για ποιο σκοπό. Επιπλέον, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να παρέχει δωρεάν αντίγραφο των δεδομένων προσωπικού χαρακτήρα σε ηλεκτρονική μορφή.Το συγκεκριμένο δικαίωμα αποτελεί μια πολύ σημαντική προσθήκη στο πλαίσιο της επιδιωκόμενης διαφάνειας

Δικαιώματα Φυσικών Προσώπων

– Δικαίωμα στη Λήθη («Διαγραφή Δεδομένων»): γνωστό ως Data Erasure, είναι το δικαίωμα των υποκειμένων να αιτούνται διαγραφή των δεδομένων τους και να σταματήσει η περαιτέρω επεξεργασία αυτών ή / και διαβίβασή τους σε τρίτους. Παρόλα αυτά, η ικανοποίηση του δικαιώματος αυτού δεν είναι πάντα υποχρεωτικό για τους υπεύθυνους επεξεργασίας και πρέπει να εξετάζεται προσεκτικά. Για παράδειγμα ένα υποκείμενο δεδομένων μπορεί να ζητήσει την διαγραφή των δεδομένων του εφόσον η νομική βάση συλλογής και επεξεργασίας στηρίζεται μόνο στην συγκατάθεση. Όταν όμως η συλλογή και επεξεργασία αφορά στην εκτέλεση μιας συμβατικής υποχρέωσης, ο υπεύθυνος επεξεργασίας δύναται να αρνηθεί την υλοποίηση του σχετικού αιτήματος εξηγώντας τους λόγους αυτής της άρνησης

Δικαιώματα Φυσικών Προσώπων

– **Δικαίωμα Φορητότητας:** Ο Νέος Γενικός Κανονισμός προβλέπει την δυνατότητα φορητότητας των δεδομένων. Δηλαδή την δυνατότητα των υποκειμένων να αιτηθούν την διαβίβαση των δεδομένων τους σε μια «ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή» σε άλλον υπεύθυνο επεξεργασίας της αρεσκείας τους.
– **Δικαίωμα Περιορισμού Επεξεργασίας:** Σύμφωνα με το Δικαίωμα του Περιορισμού της Επεξεργασίας, τα υποκείμενα των δεδομένων έχουν το δικαίωμα να ζητήσουν τον περιορισμό μέρους της επεξεργασίας κάτω από συγκεκριμένες προϋποθέσεις. Για παράδειγμα η υλοποίηση ενός τέτοιου αιτήματος μπορεί να οδηγήσει στην δυνατότητα αποθήκευσης αλλά όχι στην διαβίβαση αυτών.

Δικαιώματα Φυσικών Προσώπων

– Ενημέρωση Αυτοματοποιημένης Λήψης Αποφάσεων και Κατάρτισης Προφίλ: Τα φυσικά πρόσωπα έχουν το δικαίωμα να ενημερωθούν για οποιαδήποτε επεξεργασία τους κατατάσσει σε συγκεκριμένες κατηγορίες (προφίλ) σύμφωνα με τις οποίες λαμβάνονται αποφάσεις για αυτά. Όταν αυτή η διαδικασία είναι αυτοματοποιημένη και χωρίς ανθρώπινη παρέμβαση, τα υποκείμενα έχουν το δικαίωμα της εναντίωσης

Σημείωση:

Η διαχείριση των αιτημάτων των φυσικών προσώπων – υποκειμένων είναι ευθύνη των Υπεύθυνων Επεξεργασίας. Οι οργανισμοί που λειτουργούν ως Εκτελούντες την Επεξεργασία θα πρέπει να συνδράμουν τους πελάτες τους στη διαχείριση των αιτημάτων (ενημέρωση, προώθηση αιτήματος κλπ.) και δεν απαντούν απευθείας στα υποκείμενα των δεδομένων

Προστασία ΔΠΧ Από Τον Σχεδιασμό Και Εξ Ορισμού

Προστασία ΔΠΧ Από Τον Σχεδιασμό Και Εξ Ορισμού

Η έννοια της προστασίας από τον σχεδιασμό και εξ ορισμού (Privacy by Design & Default) υπάρχει εδώ και αρκετό καιρό, αλλά πλέον γίνεται μέρος μιας νομικής απαίτησης του νέου Κανονισμού GDPR. Στον πυρήνα του, το Privacy by Design απαιτεί την ενσωμάτωση της έννοιας της προστασίας των δεδομένων από τον αρχικό σχεδιασμό των νέων έργων, συστημάτων ή υποδομών παρά στην μεταγενέστερη και περιστασιακή προσθήκη που συνήθως δημιουργεί περισσότερα προβλήματα.

Κατά συνέπεια, σε κάθε νέο έργο, σχεδιασμό προϊόντος ή υπηρεσίας, αγορά ή ανάπτυξης συστημάτων και εφαρμογών, σύμβασης με πελάτες και προμηθευτές θα πρέπει (απαιτείται) να προβλέπονται και αξιολογούνται τα κατάλληλα και επαρκή μέτρα που θα επιτρέπουν την σύννομη επεξεργασία των ΔΠΧ

Ειδικότερα, «Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα με αποτελεσματικό τρόπο προκειμένου να ανταποκριθεί στις απαιτήσεις του παρόντος κανονισμού και να προστατεύσει τα δικαιώματα των υποκειμένων των δεδομένων». Το άρθρο 23 απαιτεί από τους υπεύθυνους επεξεργασίας να διατηρούν και να επεξεργάζονται μόνο τα δεδομένα που είναι απολύτως απαραίτητα για την εκπλήρωση των καθηκόντων τους (ελαχιστοποίηση των δεδομένων), καθώς και τον περιορισμό της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε όσους χρειάζονται τη διεξαγωγή της επεξεργασίας.

Μελέτη Εκτίμησης Αντικτύπου (DPIA)

Μελέτη Εκτίμησης Αντικτύπου (DPIA)

Η Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ) ή αλλιώς Data Privacy Impact Assessment (DPIA) είναι μια διαδικασία που βοηθά τους οργανισμούς να εντοπίζουν και να ελαχιστοποιούν τους κινδύνους προστασίας δεδομένων ενός έργου ή μιας επεξεργασίας όταν η επεξεργασία αυτή είναι πιθανό να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων. ΕΑΠΔ απαιτείται οπωσδήποτε στις ακόλουθες περιπτώσεις:

– Επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων («ευαίσθητα ή ειδικής κατηγορίας»)

Μελέτη Εκτίμησης Αντικτύπου (DPIA)

– Συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομες αποφάσεις σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο.
– Επεξεργασία σε μεγάλη κλίμακα δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα

Μελέτη Εκτίμησης Αντικτύπου (DPIA)

– Συστηματική παρακολούθηση δεδομένων σε δημοσία προσβάσιμες πηγές σε μεγάλη κλίμακα. (π.χ. CCTV Monitoring)
– Επεξεργασία που είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες ενός ατόμου
– Επεξεργασία που ενέχει τη χρήση νέων τεχνολογιών ή χρήση νέων πρωτοπόρων δραστηριοτήτων επεξεργασίας που δεν έχουν χρησιμοποιηθεί προηγουμένως (processing over cloud)

Μελέτη Εκτίμησης Αντικτύπου (DPIA)

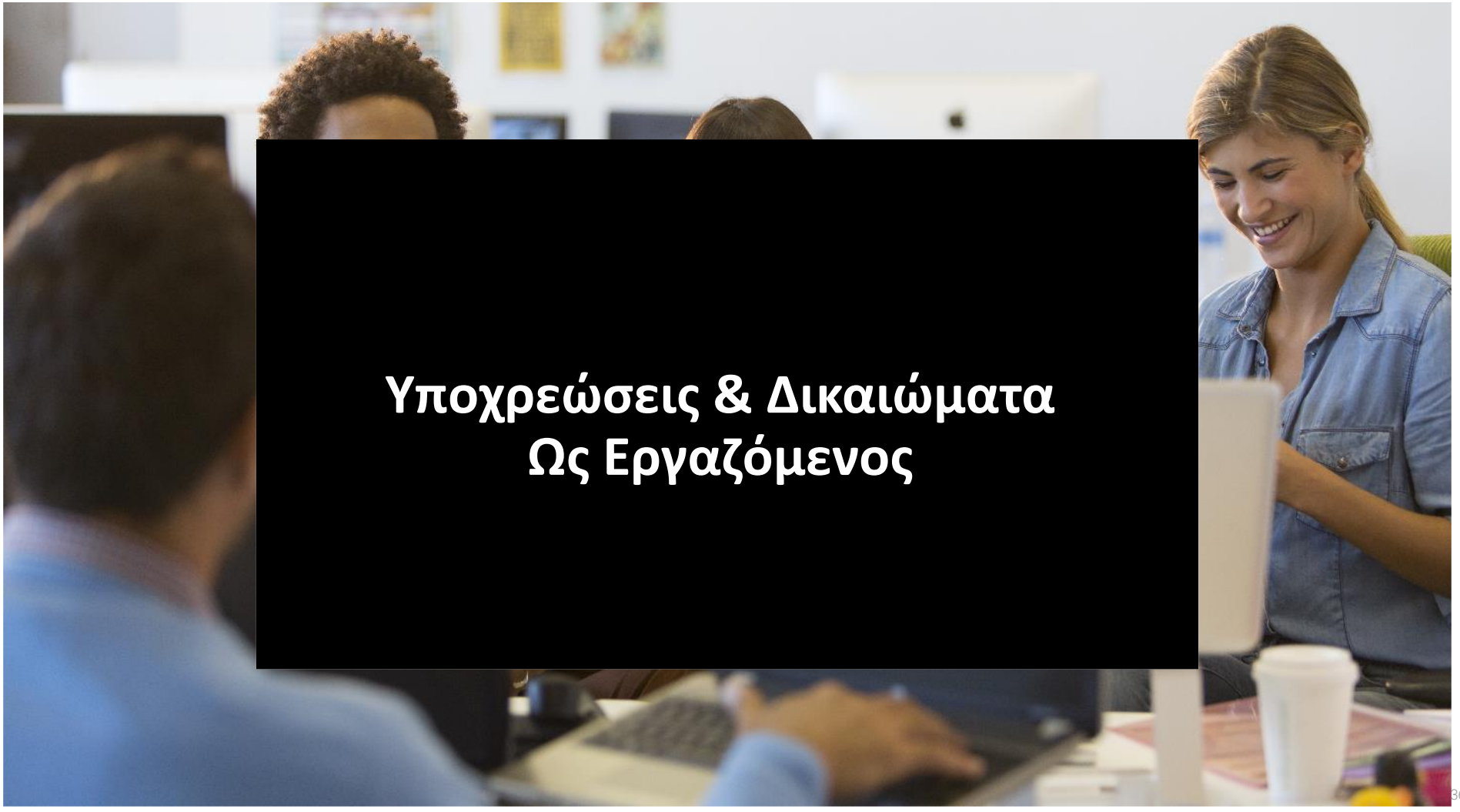
– Επεξεργασία σημαντικού όγκου δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, τα οποία θα μπορούσαν να επηρεάσουν πολλά υποκείμενα των δεδομένων.
– Επεξεργασία που καθιστά δύσκολη την άσκηση των δικαιωμάτων των υποκειμένων στα οποία αναφέρονται

Μελέτη Εκτίμησης Αντικτύπου (DPIA)

– Η μελέτη DPIA σχεδιάζεται και εκτελείται από τους υπεύθυνους επεξεργασίας του κάθε οργανισμού με την αρωγή του καθορισμένου υπεύθυνου προστασίας δεδομένων (DPO) ή άλλου καθορισμένου εμπειρογνώμονα. Μια τέτοια ειδική μελέτη θα πρέπει να περιέχει τουλάχιστον τα ακόλουθα:
– Την συστηματική περιγραφή των πράξεων επεξεργασίας και των σκοπών της επεξεργασίας
– την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς

Μελέτη Εκτίμησης Αντικτύπου (DPIA)

– την εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
– τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων συμπεριλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφαλείας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς τον ΓΚΠΔ.



Υποχρεώσεις & Δικαιώματα
Ως Εργαζόμενος

Υποχρεώσεις & Δικαιώματα Ως Εργαζόμενος

Υποχρεώσεις Εργαζόμενου

- Προστασία προσωπικών δεδομένων με κάθε τρόπο, πολιτική και διαδικασία που έχει γνωστοποιηθεί
- Επεξεργασία μόνο στο πλαίσιο εταιρικών επιχειρηματικών σκοπών
- Άμεση ειδοποίηση σε περίπτωση σοβαρού περιστατικού στους καθορισμένους φορείς (ασφάλεια, προστασία δεδομένων)
- Συμμόρφωση με τις πολιτικές της εταιρείας, τις διαδικασίες ασφάλειας και προστασίας δεδομένων

Δικαιώματα Εργαζόμενου

- Ως φυσικά πρόσωπα, οι εργαζόμενοι έχουν κάθε δικαίωμα που ορίζει και παρέχει τη σχετική νομοθεσία (δικαίωμα πρόσβασης, ενημέρωση, ανάκληση συγκατάθεσης, κατά περίπτωση, αντίρρηση κ.λπ.)
- Οι εργαζόμενοι μπορούν να παραπέμψουν, θέματα που σχετίζονται με την επεξεργασία των προσωπικών τους δεδομένων, στον υπεύθυνο και καθορισμένο ΥΠΔ που ορίζεται από την ΠΝ Πέττας

Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού,
Εκπαίδευση και Διά Βίου Μάθηση

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης