Ο ΝΕΟΣ ΕΥΡΩΠΑΪΚΟΣ ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

GDPR

2016/679

GDPR GR

SFAKIANAKIS | MAKRIPOULIAS

Εισαγωγικές έννοιες και ορισμοί.....

Πεδίο Εφαρμογής

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ ή GDPR) εφαρμόζεται σε οποιοδήποτε, εγκατεστημένο εντός Ε.Ε., φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή φορέα πραγματοποιεί με αυτοματοποιημένο τρόπο επεξεργασία προσωπικών δεδομένων και με μη αυτοματοποιημένο, εφόσον τα προσωπικά δεδομένα περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης καθώς και σε οποιονδήποτε μη εγκατεστημένο εντός Ε.Ε., εφόσον προσφέρει αγαθά και υπηρεσίες σε φυσικά πρόσωπα εντός Ε.Ε. (με ή χωρίς πληρωμή) ή παρακολουθεί τη συμπεριφορά τους, που λαμβάνει χώρα εντός Ε.Ε.

Δεδομένα Προσωπικού Χαρακτήρα

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

Δεδομένα Ειδικών κατηγοριών

Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό

Επεξεργασία

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 κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Εισαγωγικές έννοιες και ορισμοί.....

Δικαίωμα Ενημέρωσης----------

Συνοπτική, σαφής και κατανοητή ενημέρωση του υποκειμένου για τη συλλογή, την επεξεργασία και το σκοπό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του καθώς και γνωστοποίηση των δικαιωμάτων του.

Δικαίωμα Πρόσβασης----------

Το υποκείμενο έχει το δικαίωμα να λαμβάνει γνώση των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται ο υπεύθυνος επεξεργασίας και το αφορούν καθώς και το δικαίωμα λήψης αντιγράφου αυτών.

Δικαίωμα Διόρθωσης----------

Το υποκείμενο έχει το δικαίωμα να ζητήσει τη συμπλήρωση ή διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Δικαίωμα Διαγραφής----------

Το υποκείμενο έχει το δικαίωμα να ζητήσει τη διαγραφή των δεδομένων που το αφορούν υπό προϋποθέσεις.

Δικαίωμα Περιορισμού της Επεξεργασίας--

Το υποκείμενο έχει το δικαίωμα να ζητήσει τον περιορισμό της επεξεργασίας των δεδομένων που το αφορούν υπό προϋποθέσεις.

Δικαίωμα στη Φορητότητα----------

Το υποκείμενο έχει το δικαίωμα να λαμβάνει τα δεδομένα του από τον υπεύθυνο επεξεργασίας ή να ζητά τη διαβίβαση αυτών σε άλλον χωρίς αντίρρηση

Δικαίωμα Εναντίωσης----------

Το υποκείμενο έχει το δικαίωμα να εναντιωθεί στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν υπό προϋποθέσεις.

Υπεύθυνος προστασίας προσωπικών δεδομένων (DPO)

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας δεδομένων σε κάθε περίπτωση στην οποία:
α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,
β) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
γ) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα.

Απαραίτητα Βήματα.....

1

Καταγραφή – Αρχείο Δραστηριοτήτων:

Καταγράψτε τις δραστηριότητες οι οποίες εμπεριέχουν επεξεργασία δεδομένων προσωπικού χαρακτήρα περιλαμβάνοντας τα δεδομένα τα οποία επεξεργάζεστε, το σκοπό της επεξεργασίας και αν περιλαμβάνονται δεδομένα ειδικών κατηγοριών δημιουργώντας ένα αρχείο δραστηριοτήτων.

2

Βασικές Αρχές – Νομική Βάση

Ελέγξτε και καταγράψτε τη νομική βάση της επεξεργασίας για κάθε μία από τις παραπάνω δραστηριότητες.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι νόμιμη εάν στηρίζεται σε μία από τις παρακάτω νόμιμες βάσεις:

1. Συγκατάθεση του υποκειμένου
2. Εκτέλεση σύμβασης
3. Συμμόρφωση με έννομη υποχρέωση
4. Διαφύλαξη ζωτικού συμφέροντος
5. Εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας
6. Απαραίτητη επεξεργασία 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

** **Η επεξεργασία δεδομένων προσωπικού χαρακτήρα ειδικών κατηγοριών εν γένει απαγορεύεται εκτός και αν πληρείται μία από τις προϋποθέσεις που ορίζονται στο άρ.9 του ΓΚΠΔ.**

Βασικές Αρχές – Τρόποι Επεξεργασίας

3

1. Διαγράψτε προσωπικά δεδομένα, που δεν έχουν αποκτηθεί νόμιμα ή δεν είναι απαραίτητα για τη δραστηριότητά σας.
2. Περιορίστε την επεξεργασία που πραγματοποιείται στο βασικό σκοπό για τον οποίο έχουν συλλεχθεί τα δεδομένα.
3. Ελαχιστοποιήστε τα δεδομένα που επεξεργάζεστε σε κάθε δραστηριότητα στα απολύτως απαραίτητα και διαγράψτε τυχόν πλεονάζοντα δεδομένα.
4. Επικαιροποιήστε τα δεδομένα και δημιουργήστε διαδικασίες τακτικής επικαιροποίησης τους
5. Δημιουργήστε πολιτική διατήρησης και διαγραφής των δεδομένων σύμφωνα με την οποία τα δεδομένα διατηρούνται για το διάστημα που απαιτείται από το σκοπό της επεξεργασίας και τις έννομες υποχρεώσεις.

Συγκατάθεση

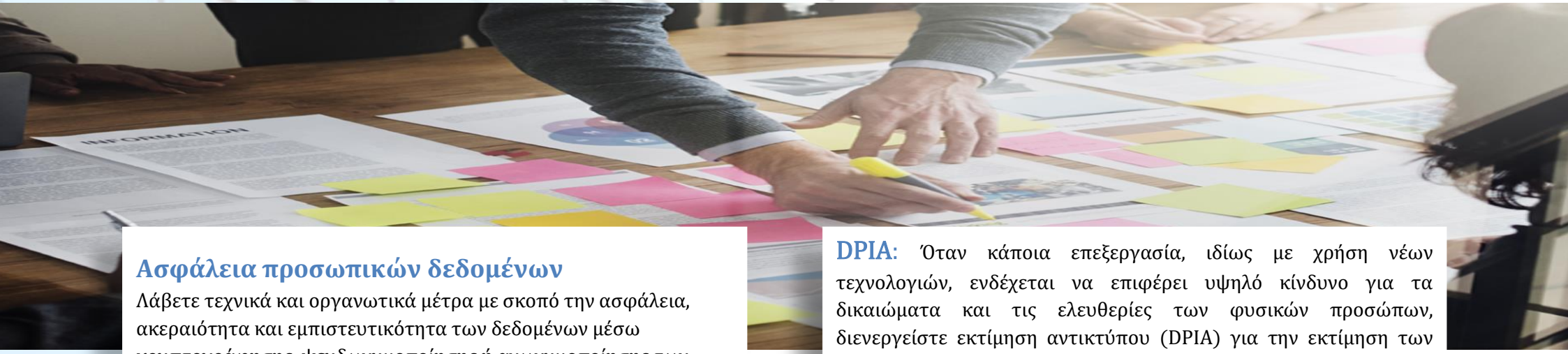
4

1. Για τις επεξεργασίες οι οποίες βασίζονται στη συγκατάθεση του υποκειμένου ελέγξτε αν η συγκατάθεση έχει ληφθεί με σαφή και κατανοητό τρόπο, με ξεκάθαρη ενέργεια από την πλευρά του υποκειμένου και αν διατηρείτε αρχείο των συγκαταθέσεων. Αν όχι τότε αναδιαμορφώστε τις διαδικασίες συγκατάθεσης και ανανεώστε τις συγκαταθέσεις για τα υπάρχοντα δεδομένα.
2. Αν επεξεργάζεστε στοιχεία ανηλίκων κάτω των 16 ετών ζητήστε τη συγκατάθεση των γονέων.

Ενημερώσεις και δικαιώματα:

5

1. Αναθεωρήστε την πολιτική προστασίας δεδομένων ώστε να περιλαμβάνει τις απαραίτητες γνωστοποιήσεις (άρ. 13 και 14 ΓΚΠΔ και δικαιώματα υποκειμένου) και δημοσιοποιήστε τη σε απλή και κατανοητή γλώσσα.
2. Δημιουργήστε διαδικασίες εξυπηρέτησης των δικαιωμάτων των πολιτών οι οποίες θα υποδέχονται και θα εξυπηρετούν τα αιτήματα εντός 1 μηνός.



Ασφάλεια προσωπικών δεδομένων

Λάβετε τεχνικά και οργανωτικά μέτρα με σκοπό την ασφάλεια, ακεραιότητα και εμπιστευτικότητα των δεδομένων μέσω κρυπτογράφησης, ψευδωνυμοποίησης ή ανωνυμοποίησης των δεδομένων και των βάσεων που τηρείτε. Ισχυροποιείστε τους κωδικούς πρόσβασης και την ασφάλεια των πληροφοριακών συστημάτων σας και ορίστε κατάλληλα δικαιώματα πρόσβασης για το προσωπικό.

Χρησιμοποιείτε αποθηκευτικούς χώρους για τα φυσικά αρχεία με επαρκή και κατάλληλη φύλαξη και εξουσιοδοτείστε συγκεκριμένα πρόσωπα, που θα έχουν πρόσβαση στο φυσικό αρχείο.

Χρησιμοποιείτε καταστροφείς εγγράφων για την καταστροφή των φυσικών αρχείων.

DPIA: Όταν κάποια επεξεργασία, ιδίως με χρήση νέων τεχνολογιών, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, διενεργείστε εκτίμηση αντικτύπου (DPIA) για την εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

DPO: Αν πληροίτε τις προϋποθέσεις για ορισμό Υπεύθυνου Προστασίας Προσωπικών Δεδομένων (D.P.O.) ορίστε μέλος του προσωπικού σας ή τρίτο, ανακοινώστε τα στοιχεία του στην Α.Π.Δ.Π.Χ. και δημοσιεύστε τα. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων θα πρέπει να μην έχει αντικρουόμενα συμφέροντα (π.χ. νομικός σύμβουλος, υπεύθυνος μηχανογράφησης κ.λπ.) και να μην είναι μέλος της διοίκησης.

Διαδικασίες ανίχνευσης παραβιάσεων και πολιτική παραβίασης: Δημιουργήστε μεθόδους ανίχνευσης και αντίδρασης σε περιστατικά παραβίασης καθώς και διαδικασία γνωστοποίησης στην Αρχή και στο υποκείμενο στις περιπτώσεις που απαιτείται.

Συμβάσεις:

Αναθεωρήστε τις συμβάσεις με το προσωπικό, τυχόν προμηθευτές και συνεργαζόμενες εταιρείες και τους πελάτες σας συμπεριλαμβάνοντας όρους και ρήτρες σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

8

Διαβιβάσεις:

Εξετάστε αν πραγματοποιείτε διαβίβαση των δεδομένων σε χώρες εκτός Ε.Ε. και αν ναι επιλέξτε ένα νόμιμο μηχανισμό διαβίβασης όπως: διαβίβαση βάσει απόφασης επάρκειας από την Επιτροπή, διαβίβαση βάσει δεσμευτικών εταιρικών κανόνων BCRs, διαβίβαση βάσει εγκεκριμένου κώδικα κ.λπ.

9

Εκπαίδευση

Ενημερώστε το προσωπικό σας για τις απαιτήσεις του GDPR και τις αλλαγές που επιφέρει δίνοντας έμφαση στις επιπτώσεις από μία πιθανή παραβίαση.

10

Thank you

GDPR GR
SFAKIANAKIS | MAKRIPOULIAS

Συμβουλές και λύσεις τεχνικού, εκπαιδευτικού, στρατηγικού και οργανωτικού χαρακτήρα σε θέματα πληροφορικής και ασφάλειας πληροφοριακών συστημάτων.

Αιγαίου πελάγους 1-3, Αγία Παρασκευή
Τηλ: (30) 210 6090059
Mail: info@gdprgreece.com