Ο ΝΕΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ο ΝΕΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Με τον νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679, που τίθεται σε εφαρμογή στις 25 Μαΐου 2018, καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ.

ΒΑΣΙΚΑ ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΠΟΛΙΤΩΝ

1. Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα: Έχετε περισσότερη και σαφέστερη ενημέρωση κατά τη συλλογή των δεδομένων για την επεξεργασία τους και το δικαίωμα πρόσβασης σε αυτά.

2. Δικαίωμα διόρθωσης: Έχετε το δικαίωμα να απαιτήσετε από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών δεδομένων καθώς και τη συμπλήρωση ελλιπών δεδομένων που σας αφορούν.

3. Δικαίωμα περιορισμού της επεξεργασίας: Δικαιούστε να εξασφαλίζετε από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας υπό συγκεκριμένες προϋποθέσεις.

4. Δικαίωμα εναντίωσης στην επεξεργασία: Έχετε το δικαίωμα να αντιταχθείτε στην επεξεργασία των δεδομένων σας υπό συγκεκριμένες προϋποθέσεις, ιδίως όταν πρόκειται για κατάρτιση «προφίλ» ή για σκοπούς απευθείας εμπορικής προώθησης.

5. Δικαίωμα στη λήθη: Όταν δεν επιθυμείτε πλέον την επεξεργασία και διατήρηση προσωπικών σας δεδομένων, έχετε το δικαίωμα να ζητήσετε τη διαγραφή τους, υπό την προϋπόθεση ότι τα δεδομένα δεν τηρούνται για κάποιο συγκεκριμένο νόμιμο και δηλωμένο σκοπό.

6. Δικαίωμα στη φορητότητα των δεδομένων: Δικαιούστε να λάβετε ή να ζητήσετε τη μεταφορά των δεδομένων σας, σε μηχαναγνώσιμη μορφή, από έναν υπεύθυνο επεξεργασίας σε άλλον υπό συγκεκριμένες προϋποθέσεις, εφόσον το επιθυμείτε.

ΒΑΣΙΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΓΙΑ ΤΟΥΣ ΥΠΕΥΘΥΝΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Ο Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στους υπευθύνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη **αρχή της διαφάνειας** στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα **αρχή της λογοδοσίας**, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων:

- **Ευθύνη:** Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδεικνύει ότι λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και ότι συμμορφώνεται με τον Κανονισμό.
- **Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design»):** Ο Κανονισμός επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων σας. Για παράδειγμα, στις υπηρεσίες ηλεκτρονικής κοινωνικής δικτύωσης πρέπει να σας δίνεται η δυνατότητα να επιλέγετε ρυθμίσεις που θα προστατεύουν περισσότερο τα προσωπικά σας δεδομένα.

• **Προστασία δεδομένων εξ ορισμού («Data protection by default»):** Ο Κανονισμός επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, *εξ ορισμού*, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.

• **Ασφάλεια επεξεργασίας:** Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.

• **Γνωστοποίηση παραβιάσεων δεδομένων:** Ο υπεύθυνος επεξεργασίας έχει υποχρέωση, μόλις αντιληφθεί παραβίαση, να ενημερώσει τις αρμόδιες εποπτικές Αρχές και εσάς, εφ' όσον η παραβίαση σάς θέτει σε σοβαρό κίνδυνο.

• **Εκτίμηση επιπτώσεων και προηγούμενη διαβούλευση:** Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων («Data protection impact assessment»). Όταν βάσει της διενεργηθείσας εκτίμησης επιπτώσεων και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εποπτική Αρχή.

• **Υπεύθυνος προστασίας δεδομένων:** Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική Αρχή.

• **Κώδικες δεοντολογίας:** Ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας από τους υπευθύνους επεξεργασίας, οι οποίοι υποβάλλονται προς έγκριση στην εποπτική Αρχή. Σε περίπτωση διευρωπαϊκής δραστηριότητας ζητείται και η γνώμη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

• **Πιστοποίηση:** Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων για την απόδειξη της συμμόρφωσης προς τον Κανονισμό ή για την απόδειξη παροχής κατάλληλων εγγυήσεων κατά την επεξεργασία. Η πιστοποίηση είναι εθελοντική και μπορεί να παρέχεται και από την εποπτική Αρχή.

ΕΠΟΠΤΙΚΕΣ ΑΡΧΕΣ – ΣΥΝΕΡΓΑΣΙΑ ΚΑΙ ΣΥΝΕΚΤΙΚΟΤΗΤΑ

Όταν κάποιος υπεύθυνος επεξεργασίας είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη και προβαίνει σε διασυνοριακή επεξεργασία δεδομένων εντός ΕΕ, είναι σκόπιμο να καθορίσει το κράτος μέλος της κύριας εγκατάστασής του στην ΕΕ, ώστε να μπορεί να απευθύνεται στην εποπτική Αρχή του κράτους αυτού –η οποία θεωρείται η επικεφαλής εποπτική Αρχή– σε σχέση με τις διάφορες υποχρεώσεις συμμόρφωσης που πηγάζουν από τον Κανονισμό. Αυτό αποτελεί τον λεγόμενο μηχανισμό μίας στάσης («One stop shop»), σύμφωνα με τον οποίο προβλέπεται συνεργασία μεταξύ της επικεφαλής εποπτικής Αρχής και των ενδιαφερόμενων εθνικών Αρχών στην αρμοδιότητα των οποίων μπορεί να εμπίπτει μια υπόθεση ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου τόσο για τους υπευθύνους επεξεργασίας όσο και για τους πολίτες της Ένωσης.

Περαιτέρω, προκειμένου να υπάρχει συνεκτική εφαρμογή του σχετικού νομικού πλαισίου στο πλαίσιο της Ένωσης, προβλέπεται ο λεγόμενος «μηχανισμός συνεκτικότητας», σημαντικό ρόλο στον οποίο διαδραματίζει το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων όπου εκπροσωπούνται όλες οι εθνικές εποπτικές Αρχές και το οποίο έχει δεσμευτικές αποφασιστικές αρμοδιότητες.

ΠΡΟΕΤΟΙΜΑΣΤΕΙΤΕ ΣΕ 10 ΒΗΜΑΤΑ

1. ΕΝΗΜΕΡΩΣΗ - ΕΤΟΙΜΟΤΗΤΑ: Ενημερώστε το ανθρώπινο δυναμικό του οργανισμού σας για τις επερχόμενες μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων. Αξιολογήστε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που συλλέγετε και επεξεργάζεστε. Διαμορφώστε στρατηγική αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα.

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

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

4. ΕΛΕΓΧΟΣ ΣΥΓΚΑΤΑΘΕΣΗΣ: Εξετάστε τις μεθόδους για εξασφάλιση συγκατάθεσης για κάθε επιδιωκόμενο σκοπό επεξεργασίας.

5. ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ: Επικαιροποιήστε τις διαδικασίες για τον χειρισμό των αιτημάτων και την ικανοποίηση των δικαιωμάτων των πολιτών, ιδίως ως προς τη διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα δεδομένων).

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

7. ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: Ανάλογα με τη δραστηριότητα που ασκείτε, εξετάστε αν χρειάζεται να ορίσετε «υπεύθυνο προστασίας δεδομένων».

8. ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ: Υιοθετήστε μεθόδους για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων. Διαθέτετε διαδικασία για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα υποκείμενα;

9. ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΣΕ ΠΕΡΙΣΣΟΤΕΡΑ ΚΡΑΤΗ ΜΕΛΗ: Στην περίπτωση αυτή πρέπει να προτείνετε το κράτος της κύριας εγκατάστασής σας.

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

Περισσότερες πληροφορίες για τη νομοθεσία προστασίας προσωπικών δεδομένων στο

www.dpa.gr

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα

Tel:+30 210 6475600 Fax: +30 210 6475628

www.dpa.gr email: contact@dpa.gr