ΙΔΙΩΤΙΚΟ ΙΕΚ
eurotraining
εναλλακτική εκπαίδευση

ΜΙΝΙ ΟΔΗΓΟΣ

10 ΕΡΩΤΗΣΕΙΣ ΚΑΙ ΑΠΑΝΤΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΝΕΟ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ (GDPR)

Εισαγωγή

Τα τεχνολογικά άλματα των τελευταίων ετών τα οποία έχουν καταστήσει αναμφισβήτητη την είσοδο μας στην ψηφιακή εποχή δεν έχουν συντελεστεί χωρίς την εμφάνιση πρωτόγνωρων κινδύνων. Η δυνατότητα των οργανισμών να διατηρούν ασύλληπτο όγκο δεδομένων ψηφιακά σε συνδυασμό με την οικονομική αξία αυτών έχει πλέον δημιουργήσει κινδύνους παραβίασης από hackers με σκοπό είτε την υποκλοπή των δεδομένων και τη μετέπειτα παράνομη πώληση τους είτε την κρυπτογράφηση τους και τον εκβιασμό του οργανισμού έως ότου αποδώσει το ζητούμενο ποσό (Ransomware). Περαιτέρω, απόρροια της τεχνολογικής εξέλιξης είναι ο διαρκώς αυξανόμενος φόβος του μέτρου ελέγχου που θα μπορεί να έχει ο εργοδότης ή το κράτος στα φυσικά πρόσωπα. Κάμερες οι οποίες συλλέγουν στοιχεία, οργανισμοί που ελέγχουν τους εργαζομένους μέσω συσκευών εντοπισμού ή βιομετρικού υλικού αποτελούν μερικά μόνο παραδείγματα τα οποία αν αφεθούν ανεξέλεγκτα μπορεί να οδηγήσουν σε ένα δυστοπικό μέλλον. Ταυτόχρονα, η οικονομική αξία των προσωπικών δεδομένων ειδικά όταν τελούνται σε αυτά επεξεργασίες που οδηγούν στην εξαγωγή συμπερασμάτων για το φυσικό πρόσωπο που μπορεί να αφορούν ακόμα και το πως θα δράσει μελλοντικά δημιουργούν τον κίνδυνο της παραβίασης του δικαιώματος της προστασίας του φυσικού προσώπου έναντι της επεξεργασίας των δεδομένων του, δικαίωμα που έχει καταστεί θεμελιώδες με το άρθρο 8 παρ. 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και το άρθρο 16 παρ. 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης. Όλες οι παραπάνω σκέψεις οδήγησαν στην ανάγκη μεγαλύτερης προστασίας από αυτήν που όριζε το προηγούμενο νομοθετικό πλαίσιο και τελικά οδήγησαν στην ψήφιση του Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Με αυτόν τον Κανονισμό η Ευρωπαϊκή Ένωση θέτει το θεσμικό πλαίσιο για τη νόμιμη επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Ενδεικτικά, απαριθμεί τις αρχές που πρέπει να διέπουν κάθε επεξεργασία και συνδέει τη νομιμότητα της επεξεργασίας με το σκοπό αυτής, επιβάλει αυξημένες υποχρεώσεις στους οργανισμούς ενώ παράλληλα εμπλουτίζει τα δικαιώματα των φυσικών προσώπων και τέλος, ενισχύει το ρόλο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Σκοπός του παρόντος Οδηγού που σας προσφέρει η EUROTraining είναι να δώσει σύντομες κατανοητές και πρακτικές απαντήσεις στις βασικότερες ερωτήσεις που μπορεί να προκύψουν σε σχέση με το νέο Κανονισμό.

Απαραίτητο όμως για την κατανόηση του νέου Κανονισμού είναι αρχικά η επεξήγηση των βασικών όρων. Έτσι, δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία (Ονοματεπώνυμο, Διεύθυνση, Τηλέφωνο, ΑΦΜ) με την οποία μπορεί να γίνει η ταυτοποίηση κάποιου φυσικού προσώπου. Σε αυτό το σημείο είναι χρήσιμο να αναφερθεί ότι δεν αποτελούν δεδομένα προσωπικού χαρακτήρα για τον Κανονισμό τα στοιχεία των νομικών προσώπων. Ειδικές κατηγορίες δεδομένων είναι τα δεδομένα τα οποία θεωρούνται ευαίσθητα. Ο Κανονισμός απαγορεύει γενικά την επεξεργασία τους και την επιτρέπει μόνο υπό μορφή εξαιρέσεων και με αυξημένες εγγυήσεις προστασίας και

ασφάλειας. Τέτοια είναι τα ιατρικά, γενετικά ή βιομετρικά δεδομένα, οι πολιτικές και θρησκευτικές πεποιθήσεις κ.α. Υποκείμενο των δεδομένων είναι κάθε φυσικό πρόσωπο ανεξάρτητα από την ιδιότητα του. Υπεύθυνος επεξεργασίας είναι ο οργανισμός υπό τις υποδείξεις και τις οδηγίες του οποίου γίνεται η επεξεργασία των δεδομένων και εκτελών την επεξεργασία είναι ο οργανισμός που εκτελεί μία ή περισσότερες εργασίες για λογαριασμό του υπευθύνου. Ο υπεύθυνος μπορεί να είναι και εκτελών ή να συνεργάζεται με κάποιον εκτελών την επεξεργασία ή με άλλο υπεύθυνο. Η απόδοση του όρου εξαρτάται από την εξουσία που έχει να διευθύνει την επεξεργασία ή όχι. Επεξεργασία αποτελεί κάθε ενέργεια αυτοματοποιημένη ή μη, που πραγματοποιείται πάνω στα δεδομένα, όπως ενδεικτικά: συλλογή, αποθήκευση, αρχειοθέτηση, διαγραφή, διαβίβαση κ.α. και υπεύθυνος προστασίας δεδομένων είναι ένα πρόσωπο το οποίο έχει χαρακτήρα συμβούλου στον οργανισμό σχετικά με την προστασία των δεδομένων και πρέπει να είναι πρόσωπο αποδεδειγμένα ανεξάρτητο με νομικές γνώσεις, γνώσεις πληροφορικής και οργανωτικές και διευθυντικές δεξιότητες.

1. Με αφορά ο Κανονισμός;

Ο Κανονισμός αφορά κάθε φυσικό ή νομικό πρόσωπο το οποίο προβαίνει σε επεξεργασία δεδομένων προσωπικού χαρακτήρα για οποιοδήποτε σκοπό πλην της ιδιωτικής χρήσης. Επεξεργασία σε δεδομένα προσωπικού χαρακτήρα μπορεί να συντελεστεί σε πελάτες, συνεργάτες ή εργαζομένους. Επίσης είναι άνευ σημασίας αν η επεξεργασία γίνεται με ψηφιακά μέσα (π.χ. μία βάση δεδομένων) ή σε φυσικό αρχείο. Νομικό πρόσωπο δε, είναι εκείνο που ασκεί οικονομική δραστηριότητα ανεξάρτητα από το αν είναι οντότητα ιδιωτικού ή δημοσίου δικαίου ή της εταιρικής του μορφής. Επίσης ο Κανονισμός αυτός εφαρμόζεται σε φυσικά ή νομικά πρόσωπα που είναι εγκατεστημένα στην Ευρωπαϊκή Ένωση ανεξάρτητα αν η επεξεργασία εκτελείται στην Ένωση αλλά και σε πρόσωπα εγκατεστημένα εκτός Ένωσης τα οποία όμως πραγματοποιούν ενέργειες επεξεργασίας εντός της Ένωσης. Επομένως αν είστε φυσικό ή νομικό πρόσωπο που τελείτε οποιαδήποτε ενέργεια επεξεργασίας, αυτοματοποιημένη ή μη, σε προσωπικά δεδομένα πελατών, εργαζομένων ή συνεργατών σας και είστε εγκατεστημένος στην Ευρωπαϊκή Ένωση ή δεν είστε εγκατεστημένος στην Ένωση η επεξεργασία όμως συντελείτε στην Ένωση ή αφορά Ευρωπαίους πολίτες τότε ναι πρέπει σας αφορά ο Κανονισμός και πρέπει να συμμορφωθείτε με αυτόν.

2. Ποιες είναι οι αρχές και οι νομικές βάσεις προστασίας των δεδομένων;

Ο Κανονισμός επιβάλει 6 αρχές με τις οποίες πρέπει να είναι σύμφωνη κάθε επεξεργασία που πραγματοποιείται από έναν οργανισμό. Αυτές είναι: Νομιμότητα, αντικειμενικότητα και διαφάνεια. Πρακτικά τα δεδομένα πρέπει να συλλέγονται σύμφωνα με μία από τις νόμιμες βάσεις που ορίζει ο Κανονισμός και να ενημερώνεται το υποκείμενο σχετικά. Περιορισμός του σκοπού. Τα δεδομένα πρέπει να συλλέγονται για συγκεκριμένο και καθορισμένο σκοπό και όχι για κρυφούς σκοπούς που δεν αναφέρονται. Ελαχιστοποίηση των δεδομένων. Να συλλέγονται παραπάνω δεδομένα από τα αναγκαία για την επίτευξη του σκοπού. Ακρίβεια και Επικαιροποίηση. Να ελέγχονται τακτικά και να διορθώνονται ή να επικαιροποιούνται κατά το αναγκαίο. Διαγραφή. Τα δεδομένα δεν πρέπει να διατηρούνται για αόριστο χρόνο και πρέπει να υπάρχουν προβλέψεις για τη διαγραφή τους.

Προστασία και Ασφάλεια. Να έχουν ληφθεί προληπτικά μέτρα (τεχνικά) ασφαλείας από μη εξουσιοδοτημένη ή παράνομη ενέργεια, τυχαία απώλεια ή καταστροφή τόσο για το ψηφιακό όσο και για το φυσικό αρχείο. Από την άλλη, οι νομικές βάσεις προστασίας είναι οι ακόλουθες και κάθε διαφορετική επεξεργασία που πραγματοποιείται πρέπει να στηρίζεται σε μία από αυτές: Να υπάρχει σχετική πρόβλεψη νόμου (π.χ. Στοιχεία που συλλέγει η φορολογική αρχή) Το υποκείμενο να έχει δώσει ρητή και ελεύθερη συγκατάθεση. Αυτή η νομική βάση χρήζει ιδιαίτερης προσοχής γιατί πρέπει η συγκατάθεση να είναι όντως ελεύθερη καθώς δεν επιτρέπεται πλέον μία άρνηση συγκατάθεσης να επιφέρει δυσμενείς συνέπειες για το υποκείμενο. (π.χ. Διαφήμιση. Δεν γίνεται πλέον να στηρίζεται η σύμβαση στη θετική δήλωση εγγραφής στο Newsletter) Η επεξεργασία να είναι απαραίτητη για την εκτέλεση σύμβασης (π.χ. Άνοιγμα τραπεζικού λογαριασμού) Η επεξεργασία να είναι απαραίτητη για την ικανοποίηση δημόσιου συμφέροντος (π.χ. το δαχτυλικό αποτύπωμα στις ταυτότητες) Να σχετίζεται με τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου (π.χ. αναίσθητο υποκείμενο που έχει τρακάρει εισάγεται στο νοσοκομείο) Να στηρίζεται σε συμφέρον του υπευθύνου (αφορά ερευνητικούς, στατιστικούς και επιστημονικούς σκοπούς)

3. Ποια είναι τα τεχνικά μέτρα που πρέπει να λάβω;

Τα τεχνικά μέτρα που καλείτε να λάβει ο οργανισμός αφορούν το σύστημα προστασίας τόσο του ψηφιακού εργασιακού περιβάλλοντος όσο και του φυσικού ώστε να εξασφαλιστεί σε πρώτο επίπεδο η πρόληψη και σε δεύτερο επίπεδο η ανάκαμψη από την καταστροφή και η επιχειρησιακή συνέχεια. Ο Κανονισμός θέλοντας να παραμείνει τεχνολογικά ουδέτερος δεν κατονομάζει τα απαραίτητα μέτρα και αναφέρει μόνο σαν παραδείγματα την ψευδωνυμοποίηση και την κρυπτογράφηση. Περαιτέρω μέτρα που πρέπει να ληφθούν αφού πρώτα εντοπιστούν όλες οι ευπάθειες και οι κίνδυνοι έχουν να κάνουν με την προστασία των συσκευών και των συστημάτων, του εταιρικού δικτύου, του φυσικού αρχείου, προστασία και ασφάλεια από κλοπή από μη εξουσιοδοτημένη πρόσβαση και υποκλοπή και από εγκλήματα του Διαδικτύου. Πρέπει τα μέτρα να είναι κατάλληλα με την έννοια ότι προσφέρουν ουσιαστική προστασία αλλά πάντα λαμβάνονται υπόψιν οι ανάγκες και οι δυνατότητες του κάθε οργανισμού ώστε να μην χρειαστεί να λάβει δυσανάλογα για το μέγεθος και τον κύκλο εργασιών του μέτρα.

4. Ποια είναι τα οργανωτικά μέτρα που πρέπει να λάβω;

Από τα οργανωτικά μέτρα που καλείται να λάβει ο οργανισμός κάποια ορίζονται ρητά από τον Κανονισμό και κάποια αφήνονται στη διακριτική του ευχέρεια ενώ κάποια είναι υποχρεωτικά υπό προϋποθέσεις. Στα υποχρεωτικά μέτρα περιλαμβάνονται τα εξής:

• Αρχεία Δραστηριοτήτων: Αρχείο το οποίο καλείται να τηρεί ο οργανισμός το οποίο προκύπτει μετά από χαρτογράφηση όλων των δεδομένων και των επεξεργασιών του οργανισμού και το οποίο περιγράφει λεπτομερώς τη ροή της πληροφορίας καθ' όλο τον κύκλο ζωής της. Πρέπει να διατηρείται επικαιροποιημένο.

• Αν υπάρχουν κάμερες πρέπει να υπάρχει σχετική ενημέρωση (με κάποιο αυτοκόλλητο σε εμφανές σημείο), ένας υπεύθυνος για τις κάμερες (μπορεί να είναι και ο επιχειρηματίας απλά πρέπει να μπορεί να αποδειχθεί ότι δεν έχει όλο το προσωπικό πρόσβαση στο υλικό) και τα δεδομένα να διαγράφονται ανά 15ήμερο.

• Πρέπει να προβλεφθεί τρόπος ενημέρωσης των υποκειμένων για το ποια δεδομένα τους συλλέγονται, τι επεξεργασία/ες θα τελεστούν, ποια είναι η νομική βάση συλλογής και επεξεργασίας όσο και για τα υπόλοιπα δικαιώματα τους καθώς και για τους τρόπους που μπορούν να τα ασκήσουν κατά το στάδιο της συλλογής των δεδομένων τους (κυρίως όταν η νομική βάση είναι η συγκατάθεση αν είναι νόμος/σύμβαση είναι λίγο αυτονόητο και ίσως αρκεί μία απλή αναφορά και μία εγγύηση ότι κάθε επεξεργασία θα είναι σύμφωνη με το θεσμικό πλαίσιο όπως κάθε φορά ισχύει).

• Να υπάρχει εσωτερική πρόβλεψη για την τήρηση αρχείου παραβιάσεων καθώς και γνωστοποίησης της παραβίασης στην Αρχή και ανακοίνωση της στα υποκείμενα εντός 72 ωρών. Αν αποφασιστεί να μην γίνει γνωστοποίηση και ανακοίνωση πρέπει το σχετικό αρχείο παραβιάσεων να αναφέρει επιπλέον γιατί αυτή δεν συντελέστηκε.

• Στη διακριτική ευχέρεια του οργανισμού ο Κανονισμός αφήνει τις εξής ενέργειες οι οποίες όμως σε κάθε περίπτωση συστήνονται έντονα:

• Την τροποποίηση των συμβάσεων να περιλαμβάνουν διασφαλίσεις απορρήτου και σύννομης και θεμιτής επεξεργασίας.

• Να συνταχθεί μία εσωτερική πολιτική στην οποία να περιλαμβάνονται όλα τα μέτρα και οι διαδικασίες καθώς και οι κυρώσεις σε περίπτωση κακόβουλης παραβίασης των διατάξεων από εργαζόμενο, που έχει λάβει ο οργανισμός για τη συμμόρφωση του με τον Κανονισμό.

• Να πραγματοποιηθεί εκπαίδευση της διοίκησης και του προσωπικού για την εξοικείωση και την ευαισθητοποίηση του με την προστασία των δεδομένων προσωπικού χαρακτήρα και την παρουσίαση της νέας πολιτικής της εταιρείας για να εξασφαλιστεί η εύρυθμη μεταβολή στη νέα φιλοσοφία.

• Κάθε άλλο μέτρο κριθεί σκόπιμο ότι θα συντελέσει αποτελεσματική προστασία και ασφάλεια.

• Τα μέτρα που τίθενται ως απαραίτητα υπό προϋποθέσεις αλλά σε κάθε περίπτωση ενθαρρύνονται να υιοθετηθούν είναι τα εξής:

• Πρόσληψη Υπεύθυνου Προστασίας Δεδομένων

• Μελέτη Αντικτύπου

5. Πρέπει να προσλάβω Υπεύθυνο Προστασίας Δεδομένων;

Ο διορισμός Υπεύθυνου Προστασίας Δεδομένων είναι απαραίτητος όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή οι βασικές δραστηριότητες συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Σε κάθε άλλη περίπτωση δεν είναι απαραίτητη η πρόσληψη του σε κάθε περίπτωση όμως το να προσλάβει ένας οργανισμός Υπεύθυνο Προστασίας Δεδομένων αποτελεί ισχυρή ένδειξη της συμμόρφωσης του με τον Κανονισμό. Σχετικά με την πρόσληψη του θα ήταν σκόπιμο να γίνουν κάποιες διευκρινίσεις. Μπορεί να προσληφθεί ως μισθωτός στον οργανισμό ή να δρα σαν εξωτερικός συνεργάτης (π.χ. συμβουλευτική εταιρεία). Προσλαμβάνεται για ορισμένο χρόνο και πρέπει να υπάρχουν εγγυήσεις για την ανεξαρτησία του, ενώ η πρόσληψη του ανακοινώνεται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Είναι υπόλογος μόνο στα ανώτερα κλιμάκια της Διοίκησης και δεν μπορεί να προέρχεται από τη Διοίκηση γιατί θα υπάρχει σύγκρουση συμφερόντων ή να είναι απλός υπάλληλος γιατί δεν θα είναι ανεξάρτητος.

6. Ποια είναι τα καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων;

Ο υπεύθυνος προστασίας δεδομένων έχει τουλάχιστον τα ακόλουθα καθήκοντα: ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται σχετικά με την προστασία δεδομένων, παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του οργανισμού σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της συνεργάζεται με την εποπτική αρχή και ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

7. Πρέπει να πραγματοποιήσω Εκτίμηση Αντικτύπου;

Η εκτίμηση αντικτύπου πραγματοποιείται για πράξεις επεξεργασίας που ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους. Αυτά τα είδη ενεργειών επεξεργασίας ενδέχεται να είναι εκείνα που, ιδίως, περιλαμβάνουν τη χρήση νέων τεχνολογιών ή που είναι νέου τύπου και όταν δεν έχει διενεργηθεί προηγουμένως εκτίμηση αντικτύπου όσον αφορά την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας ή όταν καθίστανται αναγκαία λόγω του χρόνου που έχει παρέλθει από την αρχική επεξεργασία. Σε αυτές τις περιπτώσεις, ο υπεύθυνος επεξεργασίας, πριν από την επεξεργασία, θα πρέπει να διενεργεί εκτίμηση αντικτύπου όσον αφορά την προστασία των δεδομένων, ώστε να εκτιμήσει την ιδιαίτερη πιθανότητα και τη σοβαρότητα του υψηλού κινδύνου, λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας και τις πηγές του κινδύνου. Η εν λόγω εκτίμηση αντικτύπου θα πρέπει να περιλαμβάνει, ιδίως, τα προβλεπόμενα μέτρα, εγγυήσεις και μηχανισμούς που μετριάζουν αυτόν τον κίνδυνο, διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα και αποδεικνύουν τη συμμόρφωση προς τον παρόντα κανονισμό. Συνεπώς δεν είναι απαραίτητη για κάθε επεξεργασία αλλά επιβάλλεται όταν πρόκειται να υιοθετηθεί μία νέα επεξεργασία που μπορεί να οδηγήσει σε περιορισμό δικαιωμάτων των υποκειμένων.

8. Ποια είναι η Ευθύνη του Υπεύθυνου Επεξεργασίας;

Κάθε υπεύθυνος επεξεργασίας που συμμετέχει στην επεξεργασία είναι υπεύθυνος για τη ζημία που προκάλεσε η εκ μέρους του επεξεργασία που παραβαίνει τον παρόντα κανονισμό. Ο εκτελών την επεξεργασία ευθύνεται για τη ζημία που προκάλεσε η επεξεργασία μόνο εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του παρόντος κανονισμού που αφορούν ειδικότερα τους εκτελούντες την επεξεργασία ή υπερέβη ή ενήργησε αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας. Κάθε πρόσωπο το οποίο υπέστη υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του παρόντος κανονισμού δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για τη ζημία που υπέστη.

9. Ποιες είναι οι εξουσίες της Αρχής;

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαθέτει μεταξύ άλλων τις ακόλουθες εξουσίες έρευνας:
• Να δίνει εντολή στον οργανισμό να παράσχει κάθε πληροφορία την οποία απαιτεί για την εκτέλεση των καθηκόντων της
• Να διεξάγει έρευνες με τη μορφή ελέγχων για την προστασία των δεδομένων
• Να ειδοποιεί τον οργανισμό για εικαζόμενη παράβαση του παρόντος κανονισμού
• Να αποκτά πρόσβαση σε όλα τα δεδομένα προσωπικού χαρακτήρα και όλες τις πληροφορίες που απαιτούνται για την εκτέλεση των καθηκόντων της
• Να έχει πρόσβαση στις εγκαταστάσεις περιλαμβανομένων κάθε εξοπλισμού και μέσου επεξεργασίας δεδομένων
• Να απευθύνει προειδοποιήσεις στον οργανισμό σχετικά με πράξεις επεξεργασίας που είναι πιθανόν να παραβαίνουν διατάξεις του παρόντος κανονισμού
• Να απευθύνει επιπλήξεις
• Να δίνει εντολή στον οργανισμό να συμμορφώνεται προς τα αιτήματα του υποκειμένου των δεδομένων για την άσκηση των δικαιωμάτων του σύμφωνα με τον παρόντα κανονισμό
• Να δίνει εντολή στον υπεύθυνο επεξεργασίας να ανακοινώνει την παραβίαση δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων
• Να επιβάλλει προσωρινό ή οριστικό περιορισμό, περιλαμβανομένης της απαγόρευσης της επεξεργασίας
• Να δίνει εντολή διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας
• Να αποσύρει την πιστοποίηση ή να διατάξει τον οργανισμό πιστοποίησης να αποσύρει ένα πιστοποιητικό εφόσον διαπιστωθεί ότι οι απαιτήσεις πιστοποίησης δεν πληρούνται ή δεν πληρούνται πλέον
• Να δίνει εντολή για αναστολή της κυκλοφορίας δεδομένων σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό.
• Να παρέχει συμβουλές στον υπεύθυνο επεξεργασίας
• Να εκδίδει γνώμες για σχέδια κωδίκων δεοντολογίας και να εγκρίνει τα σχέδια αυτά
• Να παρέχει διαπίστευση σε φορείς πιστοποίησης
• Να εκδίδει πιστοποιητικά και να εγκρίνει κριτήρια πιστοποίησης σύμφωνα με το άρθρο
• Να εγκρίνει δεσμευτικούς εταιρικούς κανόνες δυνάμει του άρθρου

10. Τι συμβαίνει με τα πρόστιμα;

Τα διοικητικά πρόστιμα, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιβάλλονται επιπρόσθετα ή αντί των άλλων κυρώσεων που έχει την εξουσία να επιβάλει η Αρχή. Φυσικά για την επιβολή ενός προστίμου λαμβάνονται υπόψη μία σειρά από παράγοντες όπως το μέγεθος και οι δυνατότητες του οργανισμού και δεν επιβάλλονται αυθαίρετα αλλά μπορούν να φτάσουν έως τις 20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο:

ιδιωτικό IEK
eurotraining
εναλλακτική εκπαίδευση

ΑΘΗΝΑ
Βερανζέρου 1, ΤΚ 106 77
T 210 3306086
E iek@eurotraining.gr

ΘΕΣΣΑΛΟΝΙΚΗ
Χ. Πίψου 9, ΤΚ 546 27
T 2310 508410
E thessaloniki@eurotraining.gr

ΒΟΛΟΣ
Στρ. Καλλέργη 26, ΤΚ 383 34
T 24210 91390
E volos@eurotraining.gr

www.eurotraining.gr