GDPR
EXPERTS TEAM
are you compliance?

Οδηγός
με 7 βήματα
για μικρές επιχειρήσεις

για να είστε έτοιμοι
με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων

BML SECURITY
Συστήματα Ασφαλείας
www.bmlsecurity.gr

Ποιους αφορά;

Σκοπός του οδηγού αυτού είναι να βοηθήσει τις εταιρίες που δεν διαχειρίζονται προσωπικά δεδομένα ως βασική επιχειρηματική δραστηριότητα, όπως είναι οι μικρομεσαίες επιχειρήσεις που κυρίως διαχειρίζονται προσωπικά δεδομένα των υπαλλήλων τους ή έχουν λίστες με πελάτες και αγοραστές.

Πρόκειται, ενδεικτικά, για εμπόρους ή μαγαζιά, όπως αρτοποιεία ή κρεοπωλεία, ή παρόχους υπηρεσιών, όπως αρχιτέκτονες. Αυτός ο οδηγός τονίζει τα λίγα βήματα που πρέπει να γίνουν, για να ετοιμαστείτε για τον ΓΚΠΔ.

Προσωπικά δεδομένα είναι κάθε πληροφορία που σχετίζεται με ζωντανό άτομο (όχι νομικές οντότητες). Αυτά περιλαμβάνουν, για παράδειγμα: όνομα, επίθετο, διεύθυνση κατοικίας, διεύθυνση ηλεκτρονικού ταχυδρομείου ή τοποθεσία από τον χάρτη του κινητού σας.

Συνήθως, πρόκειται για δεδομένα που ενδέχεται να διαθέτετε για τους υπαλλήλους σας, τους πελάτες σας ή του προμηθευτές σας.

Εφαρμόζετε βασικές αρχές:

συλλέγετε προσωπικά δεδομένα με σαφώς προσδιορισμένο σκοπό και μην τα χρησιμοποιείτε για κάτι άλλο (αν πείτε στους πελάτες σας να σας δώσουν τις διευθύνσεις ηλεκτρονικών ταχυδρομείων τους, για να τους στέλνετε νέες προσφορές ή διαφημίσεις, δεν μπορείτε να τις χρησιμοποιείτε για άλλον σκοπό ή να τις πουλήσετε σε άλλη επιχείρηση).

μην συλλέγετε περισσότερα δεδομένα από όσα χρειάζεστε (για παράδειγμα, αν κάνετε παράδοση κατ' οίκον, χρειάζεστε διεύθυνση, όνομα στο κουδούνι, αλλά δεν χρειάζεται να γνωρίζετε την οικογενειακή κατάσταση του πελάτη) -

να δίνετε ιδιαίτερη βάση στα προσωπικά δεδομένα που ελέγχετε.

Δείτε τι πρέπει να κάνετε σε 7 βήματα

ακολουθήστε τα παρακάτω απλά βήματα

1 ΒΗΜΑ

Διαθέτετε **υπαλλήλους**: επεξεργάζεστε τα προσωπικά τους δεδομένα με βάση τη σύμβαση εργασίας και τις νομικές υποχρεώσεις (π.χ. αναφορά στις φορολογικές αρχές / ασφαλιστικά συστήματα).

Μπορείτε να διαχειρίζεστε λίστα **ατομικών πελατών**, για παράδειγμα για να τους στέλνετε ειδοποιήσεις σχετικά με ειδικές προσφορές/ διαφημίσεις, αν έχετε λάβει τη συναίνεσή τους. Δεν χρειάζεστε όμως πάντα συναίνεση. Υπάρχουν περιπτώσεις όπου τα άτομα περιμένουν να επεξεργαστείτε τα δεδομένα τους. Για παράδειγμα, ως έμπορος πίτσας μπορείτε να επεξεργάζεστε τη διεύθυνση παράδοσης, για να διαφημίσετε ένα από τα καινούρια σας προϊόντα. Αυτό ονομάζεται έννομο συμφέρον.

Πρέπει να ενημερώνετε τα άτομα για τη χρήση που σκοπεύετε να κάνετε και να σταματάτε την επεξεργασία τέτοιων δεδομένων, αν σας ζητήσουν να το κάνετε.
Αν διαχειρίζεστε λίστα **προμηθευτών** ή **εταιρικών πελατών**, να το κάνετε βάσει των συμβάσεων που έχετε συνάψει μαζί τους. Οι συμβάσεις δεν είναι απαραίτητο να είναι σε γραπτή μορφή, θα ήταν όμως ιδανικό για το τυπικό να τις διατηρείτε και σε γραπτή μορφή.

ΕΛΕΓΞΤΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΠΟΥ ΣΥΛΛΕΓΕΤΕ ΚΑΙ ΕΠΕΞΕΡΓΑΖΕΣΤΕ,ΤΟΝ ΣΚΟΠΟ ΓΙΑ ΤΟΝ ΟΠΟΙΟΝ ΤΟ ΚΑΝΕΤΕ ΚΑΙ ΠΑΝΩ ΣΕ ΠΟΙΑ ΝΟΜΙΚΗ ΒΑΣΗ

2 ΒΗΜΑ

Τα άτομα πρέπει να γνωρίζουν ότι επεξεργάζεστε τα προσωπικά τους δεδομένα και για ποιο σκοπό.

Δεν είναι ανάγκη να τους ενημερώνετε όταν ήδη γνωρίζουν πως θα χρησιμοποιήσετε τα δεδομένα τους, για παράδειγμα όταν πελάτης σας ζητεί κατ' οίκων παράδοση.

Να ενημερώνετε, επίσης τους ενδιαφερόμενους για αιτήματα σχετικά με τα προσωπικά δεδομένα που διαθέτετε και να τους δίνετε πρόσβαση στα δικά τους προσωπικά δεδομένα.

Να τηρείτε σε τάξη τα δεδομένα ώστε όταν ένας υπάλληλος σας ρωτήσει τι είδους προσωπικά δεδομένα διαθέτετε , να μπορείτε να τα παρέχετε με ευκολία και χωρίς κόπο.

ΕΝΗΜΕΡΩΝΕΤΕ ΤΟΥΣ ΠΕΛΑΤΕΣ ΣΑΣ, ΤΟΥΣ ΥΠΑΛΛΗΛΟΥΣ ΣΑΣ ΚΑΙ ΑΛΛΟΥΣ, ΟΤΑΝ ΣΥΛΛΕΓΕΤΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΤΟΥΣ ΔΕΔΟΜΕΝΑ

3 ΒΗΜΑ

Δεδομένα των υπαλλήλων σας:
για όσο διαρκεί η σύμβαση εργασίας και οι σχετικές νομικές υποχρεώσεις

Δεδομένα των πελατών σας:
για όσο διαρκεί η σχέση με τον πελάτη και οι σχετικές νομικές υποχρεώσεις (για παράδειγμα για φορολογικούς σκοπούς)

Διαγράφετε τα δεδομένα, αν δεν είναι πλεόν απαραίτητα για τους σκοπούς για τους οποίους τα συλλέξατε

ΤΗΡΕΙΤΑΙ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΜΟΝΟ ΓΙΑ ΟΣΟ ΧΡΕΙΑΖΕΤΑΙ

4 ΒΗΜΑ

Αν αποθηκεύετε τα δεδομένα αυτά σε Πληροφοριακό Σύστημα να περιορίζετε την πρόσβαση στα αρχεία που τα περιέχουν, π.χ. με κωδικό πρόσβασης.
Να φροντίζετε να ενημερώνετε τακτικά τις ρυθμίσεις ασφαλείας του συστήματος σας.

Αν δεν έχετε αποθηκευμένα φυσικά έγγραφα με προσωπικά δεδομένα, βεβαιωθείτε ότι δεν έχουν πρόσβαση σε αυτά μη εξουσιοδοτημένα άτομα. Κλειδώστε τα σε ερμάριο ή χρηματοκιβώτιο.

Να θυμάστε: Ο Κανονισμός GDPR δεν υπαγορεύει τη χρήση κάποιου συγκεκριμένου συστήματος ERP

ΑΣΦΑΛΙΣΤΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΠΟΥ ΕΠΕΞΕΡΓΑΖΕΣΤΕ

5 ΒΗΜΑ

Αν διατηρείτε συμβόλαια υπεργολαβίας ή συμβάσεις συνεργασίας με άλλη εταιρεία στην οποία περιλαμβάνεται επεξεργασία προσωπικών δεδομένων, χρησιμοποιήστε μόνο πάροχο υπηρεσιών που εγγυάται τη συμμόρφωση της επεξεργασίας με τις απαιτήσεις του ΓΚΠΔ (π.χ. μέτρα ασφάλειας)

Πριν από την υπογραφή της σύμβασης, ελέγξτε αν έχουν γίνει οι αλλαγές και η προσαρμογή με τον ΓΚΠΔ. Αυτό θα πρέπει να τεθεί στη σύμβαση

ΒΕΒΑΙΩΘΕΙΤΕ ΟΤΙ Ο ΥΠΕΡΓΟΛΑΒΟΣ/ΣΥΝΕΡΓΑΤΗΣ ΣΑΣ, ΤΗΡΕΙ ΤΟΥΣ ΙΔΙΟΥΣ ΚΑΝΟΝΕΣ

6 ΒΗΜΑ

Ετοιμάστε ένα μικρό έγγραφο όπου εξηγείτε τι προσωπικά δεδομένα συλλέγετε ή έχετε στη διάθεση σας και για ποιον λόγο. Ίσως σας ζητηθεί να προσκομίσετε το σχετικό φάκελο στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Τέτοια έγγραφα πρέπει να περιλαμβάνουν τις παρακάτω πληροφορίες:

Σκοπός, Είδη και Κατηγορίες των δεδομένων
Κατηγορίες Παραληπτών
Χρόνους τήρησης
Μέτρα τεχνικής και οργανωτικής ασφάλειας που έχετε λάβει για την προστασία τους
Αν διαβιβάζονται εκτός Ευρωπαϊκής Ένωσης

ΚΡΑΤΗΣΤΕ ΦΑΚΕΛΟ ΜΕ ΤΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΠΡΑΓΜΑΤΟΠΟΙΕΙΤΕ

7

ΒΗΜΑ

Για την καλύτερη προστασία των προσωπικών δεδομένων, οι οργανισμοί ενδεχομένως να χρειαστεί να διορίσουν **υπεύθυνο προστασίας δεδομένων (DPO)**. Ωστόσο δεν χρειάζεται να ορίσετε υπεύθυνο προστασίας δεδομένων αν η επεξεργασία δεδομένων δεν αποτελεί βασικό στοιχείο της επιχειρησης σας, δεν είναι επικίνδυνη, και η δραστηριότητα σας είναι μικρής κλίμακας.
Για παράδειγμα, αν η εταιρεία σας συλλέγει μόνο δεδομένα πελατών σας για κατ' οίκων παράδοση δεν χρειάζεται να ορίσετε ΥΠΔ.
Δεν είναι απαραίτητο να είναι υπάλληλος της εταιρείας σας και να τον επιφορτίσετε και με το καθήκον αυτό. Μπορείτε να προσλάβετε εξωτερικό σύμβουλο με τον ίδιο τρόπο που χρησιμοποιείτε εξωτερικό λογιστή.

Συνήθως δεν χρειάζεται να εκτελέσετε **εκτίμηση αντικτύπου (DPIA)** σχετικά με την προστασία δεδομένων. Εκτίμηση Αντικτύπου απαιτείται σε όσους θέτουν περισσότερους κινδύνους για τα προσωπικά δεδομένα όπως είναι η ύπαρξη συστήματος βιντεοεπιτήρησης.
Σε περίπτωση που διαχειρίζεστε μισθούς υπαλλήλων ή λίστες πελατών δεν χρειάζεται γι αυτές τις επεξεργασίες να εκτελείτε εκτίμηση αντικτύπου

ΕΛΕΓΞΤΕ ΑΝ ΣΑΣ ΑΦΟΡΟΥΝ ΟΙ ΣΥΓΚΕΚΡΙΜΕΝΕΣ ΔΙΑΤΑΞΕΙΣ

Πρόστιμα

Οι εποπτικές αρχές προστασίας δεδομένων είναι εξουσιοδοτημένες να τιμωρούν παραβάσεις των κανόνων προστασίας δεδομένων. Μπορούν να εγκρίνουν διορθωτικά μέτρα (για παράδειγμα, διοικητική εντολή ή προσωρινή αναστολή της επεξεργασίας) ή και να επιβάλουν πρόστιμο

Η απόφασή τους για επιβολή προστίμου πρέπει να είναι αναλογική και να βασίζεται σε αξιολόγηση όλων των περιστάσεων της ατομικής υπόθεσης

Αν αποφασίσουν να επιβάλουν πρόστιμο, το ύψος αυτού θα εξαρτάται και από τις περιστάσεις της υπόθεσης, συμπεριλαμβανομένης της βαρύτητας της παράβασης, ή από το αν η παράβαση ήταν εκούσια ή από αμέλεια.

Θα λάβουν επίσης υπ όψιν τη συμπεριφορά και της προθέσεις σας

Τι μπορεί να κάνει για εσάς η GDPR Experts Team

Αναλαμβάνουμε όλες τις απαραίτητες διαδικασίες σχετικά με τη δημιουργία των αρχείων δραστηριότητας της επεξεργασίας των δεδομένων που τηρείτε
Διενεργούμε την εκτίμηση αντικτύπου στην περίπτωση που απαιτείται (π.χ. διαθέτετε σύστημα παρακολούθησης στο χώρο σας)
Εκπαιδεύουμε και ενημερώνουμε όλο το προσωπικό σας για το Γενικό Κανονισμό Προστασίας Δεδομένων και το πως πρέπει να ενημερώνουν τους πελάτες/προμηθευτές σας.
Δημιουργούμε όλο το φάκελο συμμόρφωσης με όλα τα απαιτούμενα έντυπα και φόρμες.
Δημιουργούμε όλα τα απαραίτητα έγγραφα - συμβάσεις που απαιτούνται για τις σχέσεις με τους συνεργάτες, υπαλλήλους ή προμηθευτές σας
Ορίζουμε Υπευθυνο Προστασίας Δεδομένων στην περίπτωση που απαιτείται

Για περισσότερες πληροφορίες:

1. Συμβουλευτείτε την GDPR Experts Team μέσω τηλεφώνου στο 210 3459781 ή μέσω email στο info@bmlsecurity.gr ή μέσα από το site της BML Security www.bmlsecurity.gr

2. Επισκεφτείτε τον διαδικτυακό οδηγό της Ευρωπαϊκής Επιτροπής σχετικά με τη μεταρρύθμιση της προστασίας των δεδομένων - διαθέσιμος σε όλες τις γλώσσες της ΕΕ: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_el

3. Συμβουλευτείτε την εθνική αρχή σας προστασίας δεδομένων: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

BML
SECURITY
Συστήματα Ασφαλείας
www.bmlsecurity.gr