



Επτά βήματα για τις επιχειρήσεις



για να είστε έτοιμοι για τον Γενικό
Κανονισμό για την Προστασία των Δεδομένων

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.

Όσο λιγότερο κίνδυνο έχουν οι δραστηριότητές σας για τα προσωπικά δεδομένα, τόσο λιγότερα πρέπει να κάνετε

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 γιεύθυνση, όνομα στο κουδούνι, αλλά δεν χρειάζεται να γνωρίζετε την οικογενειακή κατάσταση του πελάτη) - να δίνετε ιδιαίτερη βάση στα προσωπικά δεδομένα που ελέγχετε.

ΒΗΜΑ 1

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

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 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.

ΒΗΜΑ 2

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

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

Δεν είναι ανάγκη να τους ενημερώνετε, όταν ήδη γνωρίζουν πώς θα χρησιμοποιήσετε τα δεδομένα τους: για παράδειγμα όταν πελάτης σας ζητεί κατ' οίκον 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.

ΒΗΜΑ 3

ΤΗΡΕΙΤΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΜΟΝΟ ΓΙΑ ΟΣΟ ΧΡΕΙΑΖΕΤΑΙ

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).

Διαγράψτε τα δεδομένα, αν δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους τα συλλέξατε.

ΒΗΜΑ 4

ΑΣΦΑΛΙΣΤΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΠΟΥ ΕΠΕΞΕΡΓΑΖΕΣΤΕ

Αν αποθηκεύετε τα δεδομένα αυτά σε **σύστημα ΤΠ**, να περιορίζετε την πρόσβαση στα αρχεία που τα περιέχουν, π.χ. με κωδικό πρόσβασης. Να ενημερώνετε τακτικά τις ρυθμίσεις ασφαλείας του συστήματός σας.

(Σημείωση: ο ΓΚΠΔ δεν υπαγορεύει τη χρήση συγκεκριμένου συστήματος ΤΠ)

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

ΒΗΜΑ 5

ΚΡΑΤΑΤΕ ΦΑΚΕΛΟ ΜΕ ΤΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΣΑΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ετοιμάστε ένα μικρό έγγραφο όπου εξηγείτε τι προσωπικά δεδομένα έχετε στη διάθεσή σας και για ποιον λόγο. Ίσως σας ζητηθεί να προσκομίσετε τον σχετικό φάκελο στην εθνική αρχή σας προστασίας δεδομένων, αν σας το ζητήσει.

Τέτοια έγγραφα πρέπει να περιλαμβάνουν τις παρακάτω πληροφορίες.

ΠΛΗΡΟΦΟΡΙΕΣ	ΠΑΡΑΔΕΙΓΜΑΤΑ
Σκοπός της επεξεργασίας των δεδομένων	Ειδοποίηση πελατών για ειδικές προσφορές / παράδοση κατ' οίκον, πληρωμή προμηθευτών και ασφαλιστική κάλυψη υπαλλήλων
Είδη προσωπικών δεδομένων	Στοιχεία επικοινωνίας πελατών, στοιχεία επικοινωνίας προμηθευτών, δεδομένα υπαλλήλων
Κατηγορίες των σχετικών υποκείμενων δεδομένων	Υπάλληλοι, πελάτες, προμηθευτές
Κατηγορίες παραληπτών	Αρχές εργασίας, φορολογικές αρχές
Περίοδοι αποθήκευσης	Τα προσωπικά δεδομένα των υπαλλήλων μέχρι τη λήξη της σύμβασης εργασίας (και των σχετικών νομικών υποχρεώσεων), τα προσωπικά δεδομένα των πελατών μέχρι τη λήξη της σχέσης με τον πελάτη/συμβατικής σχέσης
Μέτρα τεχνικής και οργανωτικής ασφάλειας για την προστασία προσωπικών δεδομένων	Τακτική ενημέρωση λύσεων συστημάτων ΤΠ, κλειδωμένα ερμάρια/ χρηματοκιβώτια
Αν τα προσωπικά δεδομένα διαβιβάζονται σε παραλήπτες εκτός ΕΕ	Χρήση ενός εκτελούντος την επεξεργασία εκτός της ΕΕ (π.χ. για αποθήκευση στην υπηρεσία νέφους)

ΒΗΜΑ 6

ΒΕΒΑΙΩΘΕΙΤΕ ΟΤΙ Ο ΥΠΕΡΓΟΛΑΒΟΣ ΣΑΣ ΤΗΡΕΙ ΤΟΥΣ ΚΑΝΟΝΕΣ

Αν σε συμβόλαιο υπεργολαβίας με άλλη εταιρία περιλαμβάνεται η επεξεργασία προσωπικών δεδομένων, χρησιμοποιήστε μόνο πάροχο υπηρεσιών που εγγυάται τη συμμόρφωση της επεξεργασίας με τις

απαιτήσεις του ΓΚΠΔ (π.χ. μέτρα ασφαλείας). Πριν από την υπογραφή της σύμβασης, ελέγξτε αν έχουν γίνει οι αλλαγές και η προσαρμογή με τον ΓΚΠΔ. Αυτό πρέπει να τεθεί στη σύμβαση.

ΒΗΜΑ 7

ΕΛΕΓΞΤΕ ΑΝ ΣΑΣ ΑΦΟΡΟΥΝ ΟΙ ΠΑΡΑΚΑΤΩ ΔΙΑΤΑΞΕΙΣ

> Για την καλύτερη προστασία των προσωπικών δεδομένων, οι οργανισμοί ενδεχομένως να χρειαστεί να προσλάβουν υπεύθυνο προστασίας δεδομένων (ΥΠΔ). **Ωστόσο, δεν χρειάζεται να ορίσετε υπεύθυνο προστασίας δεδομένων**, αν η επεξεργασία δεδομένων δεν αποτελεί βασικό στοιχείο της επιχείρησής σας, δεν είναι επικίνδυνη, και η δραστηριότητά σας είναι μικρής κλίμακας.

Για παράδειγμα, αν η εταιρία σας συλλέγει μόνο δεδομένα πελατών σας για κατ' οίκον παράδοση, δεν χρειάζεται να προσλάβετε ΥΠΔ.

Ακόμη και αν χρειαστείτε τις υπηρεσίες ενός ΥΠΔ, αυτός/αυτή πρέπει να είναι ήδη υπάλληλος της εταιρίας, έχοντας επιφορτιστεί με το καθήκον αυτό, πέρα από τα άλλα του/της καθήκοντα. Μπορεί, επίσης, να είναι

εξωτερικός σύμβουλος, με τον ίδιο τρόπο που πολλοί οργανισμοί χρησιμοποιούν εξωτερικούς λογιστές.

> **Συνήθως δεν χρειάζεται να εκτελέσετε εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων**

Τέτοια εκτίμηση αντικτύπου προορίζεται για όσους θέτουν περισσότερους κινδύνους για τα προσωπικά δεδομένα, π.χ. μέσω της ευρείας κλίμακας παρακολούθησης δημόσια προσβάσιμης περιοχής (βιντεοεπιτήρηση).

Αν είστε μικρή επιχείρηση που διαχειρίζεται μισθούς υπαλλήλων και λίστα πελατών, δεν χρειάζεται να εκτελείτε εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων για αυτές τις λειτουργίες επεξεργασίας.

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 επιβάλλουν 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, υπόψη τη συμπεριφορά και τις προθέσεις σας.

Για περισσότερες πληροφορίες:

1. Επισκεφτείτε τον διαδικτυακό οδηγό της Ευρωπαϊκής Επιτροπής σχετικά με τη μεταρρύθμιση της προστασίας των δεδομένων - διαθέσιμος σε όλες τις γλώσσες της ΕΕ:

europa.eu/dataprotection/el

2. Συμβουλευτείτε την εθνική αρχή σας προστασίας δεδομένων:

edpb.europa.eu/about-edpb/board/members_el

ΣΗΜΑΝΤΙΚΗ ΣΗΜΕΙΩΣΗ

Οι πληροφορίες σε αυτόν τον οδηγό στοχεύουν να συμβάλουν στην καλύτερη κατανόηση των κανόνων προστασίας δεδομένων της ΕΕ.

Ο παρών οδηγός προορίζεται να χρησιμεύσει αποκλειστικά ως εργαλείο καθοδήγησης — μόνο το κείμενο του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ) έχει νομική ισχύ. Ως αποτέλεσμα, μόνο ο ΓΚΠΔ δύναται να δημιουργήσει δικαιώματα και υποχρεώσεις για φυσικά πρόσωπα. Η παρούσα καθοδήγηση δεν δημιουργεί κανένα εκτελεστό δικαίωμα ή προσδοκία.

Η δεσμευτική ερμηνεία της νομοθεσίας της ΕΕ αποτελεί αποκλειστική αρμοδιότητα του Δικαστηρίου της Ευρωπαϊκής Ένωσης. Οι απόψεις που εκφράζονται στο παρόν έγγραφο καθοδήγησης δεν θίγουν τη θέση που μπορεί να πάρει η Επιτροπή ενώπιον του Δικαστηρίου.

Ούτε η Ευρωπαϊκή Επιτροπή ούτε οποιοδήποτε άλλο πρόσωπο που ενεργεί εξ ονόματός της φέρει ευθύνη για την ενδεχόμενη χρήση των πληροφοριών που περιλαμβάνονται στον οδηγό.

Καθώς το παρόν έγγραφο αντικατοπτρίζει τις τελευταίες εξελίξεις κατά τον χρόνο της σύνταξής του, θα πρέπει να θεωρείται ως ένα «ζωντανό εργαλείο» που επιδέχεται βελτιώσεις και το περιεχόμενό του μπορεί να υπόκειται σε τροποποιήσεις χωρίς προηγούμενη ειδοποίηση.



Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης, 2018

© Ευρωπαϊκή Ένωση, 2018

Η περαιτέρω χρήση επιτρέπεται εφόσον αναφέρεται η πηγή.

Print

ISBN 978-92-79-85394-4

doi:10.2838/91614

DS-02-18-544-EL-C

PDF

ISBN 978-92-79-85401-9

doi:10.2838/131202

DS-02-18-544-EL-N