

## Απάντηση 1

### 1. Νομιμότητα, Διαφάνεια και Δίκαιη Επεξεργασία

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται:

Με νόμιμο τρόπο,

Με διαφάνεια προς τα υποκείμενα των δεδομένων,

Και με δίκαιη μεταχείριση.

### 2. Περιορισμός Σκοπού

Τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία που δεν συνάδει με αυτούς τους σκοπούς.

### 3. Ελαχιστοποίηση Δεδομένων

Η επιχείρηση οφείλει να συλλέγει μόνο τα απολύτως απαραίτητα δεδομένα για την επίτευξη του σκοπού της.

### 4. Ακρίβεια

Τα δεδομένα πρέπει να είναι ακριβή και, όπου χρειάζεται, επικαιροποιημένα. Η διόρθωση ή διαγραφή ανακριβών δεδομένων είναι υποχρεωτική.

### 5. Περιορισμός Περιόδου Αποθήκευσης

Τα δεδομένα να διατηρούνται μόνο για όσο διάστημα είναι απαραίτητο για τους σκοπούς για τους οποίους συλλέχθηκαν.

### 6. Ακεραιότητα και Εμπιστευτικότητα (Ασφάλεια)

Η επιχείρηση πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει:

Την προστασία των δεδομένων από απώλεια,

Μη εξουσιοδοτημένη πρόσβαση,

Καταστροφή ή αλλοίωση.

### 7. Λογοδοσία

Η επιχείρηση πρέπει να είναι σε θέση να αποδεικνύει τη συμμόρφωσή της με τον Κανονισμό ανά πάσα στιγμή (αρχή της λογοδοσίας).

### 8. Καταγραφή Δραστηριοτήτων Επεξεργασίας

Η επιχείρηση οφείλει να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας που διενεργεί, εφόσον εμπίπτει στις προϋποθέσεις του άρθρου 30 του Κανονισμού.

#### 9. Σεβασμός των Δικαιωμάτων των Υποκειμένων

Η επιχείρηση πρέπει να εξασφαλίζει τη δυνατότητα άσκησης των δικαιωμάτων των πολιτών, όπως:

Δικαίωμα πρόσβασης,

Διόρθωσης,

Διαγραφής («δικαίωμα στη λήθη»),

Περιορισμού της επεξεργασίας,

Φορητότητας των δεδομένων,

Αντίρρησης.

#### 10. Διαχείριση Συγκατάθεσης (όπου απαιτείται)

Όταν η νομική βάση της επεξεργασίας είναι η συγκατάθεση, αυτή πρέπει να είναι:

Ελεύθερη,

Ενημερωμένη,

Σαφής,

Και να μπορεί να αποδειχθεί και να ανακληθεί ανά πάσα στιγμή.

#### 11. Γνωστοποίηση Παραβιάσεων Δεδομένων

Σε περίπτωση παραβίασης δεδομένων, η επιχείρηση οφείλει να ειδοποιήσει:

Την Αρχή Προστασίας Δεδομένων εντός 72 ωρών, και

Τα υποκείμενα των δεδομένων, όταν συντρέχει σοβαρός κίνδυνος.

#### 12. Ορισμός Υπευθύνου Προστασίας Δεδομένων (DPO)

Αν η επιχείρηση πληροί συγκεκριμένα κριτήρια (π.χ. επεξεργασία ευαίσθητων δεδομένων μεγάλης κλίμακας), υποχρεούται στον διορισμό DPO.

#### Απάντηση 2

##### 1. Συμμόρφωση με τη Νομοθεσία (π.χ. ΓΚΠΔ - GDPR)

Οι πελάτες πρέπει να δίνουν ρητή συγκατάθεση για τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων.

Η εταιρεία οφείλει να είναι διαφανής σχετικά με τη χρήση των δεδομένων.

Οι πελάτες έχουν δικαίωμα πρόσβασης, διόρθωσης και διαγραφής των δεδομένων τους.

## 2. Ασφάλεια Δεδομένων

Τα δεδομένα πρέπει να αποθηκεύονται με ασφαλείς μεθόδους (π.χ. κρυπτογράφηση).

Η πρόσβαση στα δεδομένα πρέπει να είναι περιορισμένη μόνο σε εξουσιοδοτημένο προσωπικό.

Να υπάρχουν αντίγραφα ασφαλείας (backups) και πλάνο ανάκτησης σε περίπτωση απώλειας ή παραβίασης.

## 3. Αρχή της Ελαχιστοποίησης & Περιορισμός Σκοπού

Συλλέγονται μόνο τα απολύτως απαραίτητα δεδομένα.

Τα δεδομένα χρησιμοποιούνται μόνο για τον σκοπό για τον οποίο έχουν συλλεχθεί.

Απαιτείται νέα συγκατάθεση για κάθε επιπλέον χρήση.

## 4. Εσωτερικές Πολιτικές & Εκπαίδευση Προσωπικού

Καθιέρωση εσωτερικής πολιτικής προστασίας δεδομένων.

Εκπαίδευση όλων των εργαζομένων σχετικά με τον ΓΚΠΔ και τις καλές πρακτικές.

## 5. Αντιμετώπιση Παραβιάσεων Δεδομένων (Data Breach)

Καθορισμένο σχέδιο αντίδρασης σε περίπτωση παραβίασης.

Άμεση ενημέρωση των αρμόδιων αρχών και των πελατών εντός 72 ωρών, όταν απαιτείται.

## Απάντηση 3

Πιο αναλυτικά:

Η κατάρτιση προφίλ περιλαμβάνει:

Συλλογή δεδομένων: όπως είναι οι συνήθειες, προτιμήσεις, τοποθεσία, ιστορικό αγορών, δραστηριότητα στο διαδίκτυο, κοινωνική συμπεριφορά κ.ά.

Ανάλυση των δεδομένων: μέσω τεχνολογιών όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση.

Δημιουργία προφίλ: δηλαδή η δημιουργία ενός «μοντέλου» που προβλέπει τι μπορεί να κάνει ή να θέλει ένα άτομο π.χ. τι προϊόν θα αγοράσει, αν πληροί κριτήρια για δάνειο, ή αν είναι κατάλληλο για

μια εργασία.

Παραδείγματα χρήσης:

Στο μάρκετινγκ: για την προβολή στοχευμένων διαφημίσεων.

Στην αστυνόμευση: για τον εντοπισμό υπόπτων συμπεριφορών.

Στον τραπεζικό τομέα: για την αξιολόγηση πιστοληπτικής ικανότητας.

Στα μέσα κοινωνικής δικτύωσης: για την εξατομίκευση περιεχομένου.

Νομικές και ηθικές διαστάσεις:

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR):

Η κατάρτιση προφίλ θεωρείται ιδιαίτερα ευαίσθητη όταν βασίζεται σε αυτοματοποιημένη λήψη αποφάσεων με έννομες συνέπειες (όπως η απόρριψη ενός δανείου).

Ο πολίτης έχει δικαίωμα πληροφόρησης, πρόσβασης, αντίρρησης και σε ορισμένες περιπτώσεις μη υποβολής σε αυτοματοποιημένες αποφάσεις.

Συμπερασματικά:

Η κατάρτιση προφίλ αποτελεί ένα ισχυρό εργαλείο για την κατανόηση και πρόβλεψη της ανθρώπινης συμπεριφοράς, ωστόσο εγκυμονεί κινδύνους, όπως η παραβίαση της ιδιωτικότητας, η διάκριση, και η κατάχρηση δεδομένων, κάτι που καθιστά απαραίτητη τη σωστή ρύθμιση και προστασία των ατομικών δικαιωμάτων.

#### Απάντηση 4

##### 1. Υποβολή Αιτήματος Διαγραφής (Right to Erasure – «Δικαίωμα στη Λήθη»)

Ο πελάτης μπορεί να υποβάλει γραπτό αίτημα προς τον υπεύθυνο επεξεργασίας (την εταιρεία ή τον οργανισμό) ζητώντας τη διαγραφή των προσωπικών του δεδομένων. Το αίτημα μπορεί να σταλεί μέσω email, επιστολής ή μέσω φόρμας που μπορεί να παρέχει η εταιρεία στην ιστοσελίδα της.

##### 2. Αιτιολόγηση Αιτήματος (προαιρετική)

Αν και δεν είναι απαραίτητο να αιτιολογήσει πλήρως το αίτημά του, το να αναφέρει συγκεκριμένους λόγους (π.χ. τα δεδομένα δεν είναι πλέον απαραίτητα, ανακαλεί τη συγκατάθεσή του, τα δεδομένα έχουν υποστεί παράνομη επεξεργασία) μπορεί να επιταχύνει τη διαδικασία.

### 3. Απάντηση από την Εταιρεία

Η εταιρεία οφείλει να απαντήσει στο αίτημα εντός ενός μηνός. Σε εξαιρετικές περιπτώσεις, η προθεσμία μπορεί να παραταθεί κατά δύο επιπλέον μήνες, αλλά ο πελάτης πρέπει να ενημερωθεί σχετικά.

### 4. Πιθανή Απόρριψη Αιτήματος

Το αίτημα μπορεί να απορριφθεί σε ορισμένες περιπτώσεις, π.χ.:

Όταν τα δεδομένα είναι απαραίτητα για την εκπλήρωση νομικής υποχρέωσης.

Όταν απαιτούνται για την άσκηση ή υπεράσπιση νομικών αξιώσεων.

Όταν η επεξεργασία είναι απαραίτητη για λόγους δημοσίου συμφέροντος.

Σε περίπτωση απόρριψης, η εταιρεία πρέπει να αιτιολογήσει την απόφασή της.

### 5. Καταγγελία στην Αρχή Προστασίας Δεδομένων

Αν ο πελάτης δεν λάβει απάντηση ή η απάντηση δεν είναι ικανοποιητική, μπορεί να υποβάλει καταγγελία στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

## Απάντηση 5

### 1. Εμφάνιση Μπανιέρας Cookies (Cookie Banner)

Κατά την πρώτη επίσκεψη:

Εμφανίζεται αναδυόμενο παράθυρο/μπάνερ με:

Πληροφορίες για τη χρήση cookies.

Επιλογή: [Αποδοχή όλων] [Απόρριψη μη απαραίτητων] [Προσαρμογή]

Σύνδεσμο προς την Πολιτική Cookies.

Παράδειγμα μηνύματος:

«Χρησιμοποιούμε cookies για να βελτιώσουμε την εμπειρία σας. Μπορείτε να προσαρμόσετε τις προτιμήσεις σας ή να αποδεχθείτε όλα τα cookies.»

## 2. Κατηγορίες Cookies

Οι cookies πρέπει να διαχωρίζονται, τουλάχιστον, στις εξής κατηγορίες:

Απαραίτητα (λειτουργικά, δεν απαιτούν συγκατάθεση)

Αναλυτικά/Στατιστικά (π.χ. Google Analytics)

Διαφημιστικά/Marketing

Προτιμήσεων

## 3. Πολιτική Cookies (Cookie Policy)

Δημοσιεύεται ξεχωριστά ή μέσα στην Πολιτική Απορρήτου και περιλαμβάνει:

Τι είναι τα cookies.

Αναλυτική λίστα cookies που χρησιμοποιούνται (όνομα, πάροχος, σκοπός, διάρκεια).

Τρίτοι πάροχοι και μεταφορά δεδομένων.

Πώς μπορεί ο χρήστης να απενεργοποιήσει ή να διαγράψει τα cookies από τον browser.

## 4. Ανάκληση Συγκατάθεσης

Ο χρήστης πρέπει να μπορεί να αλλάξει γνώμη εύκολα και ανά πάσα στιγμή.

Προτείνεται σταθερό κουμπί "Διαχείριση Cookies" στο υποσέλιδο (footer).

## 5. Καταγραφή Συγκατάθεσης

Η συγκατάθεση πρέπει να τεκμηριώνεται (π.χ. ημερομηνία, IP, κατηγορίες που αποδέχθηκε).

Μπορεί να χρησιμοποιηθεί εργαλείο διαχείρισης (π.χ. Cookiebot, iubenda, OneTrust).