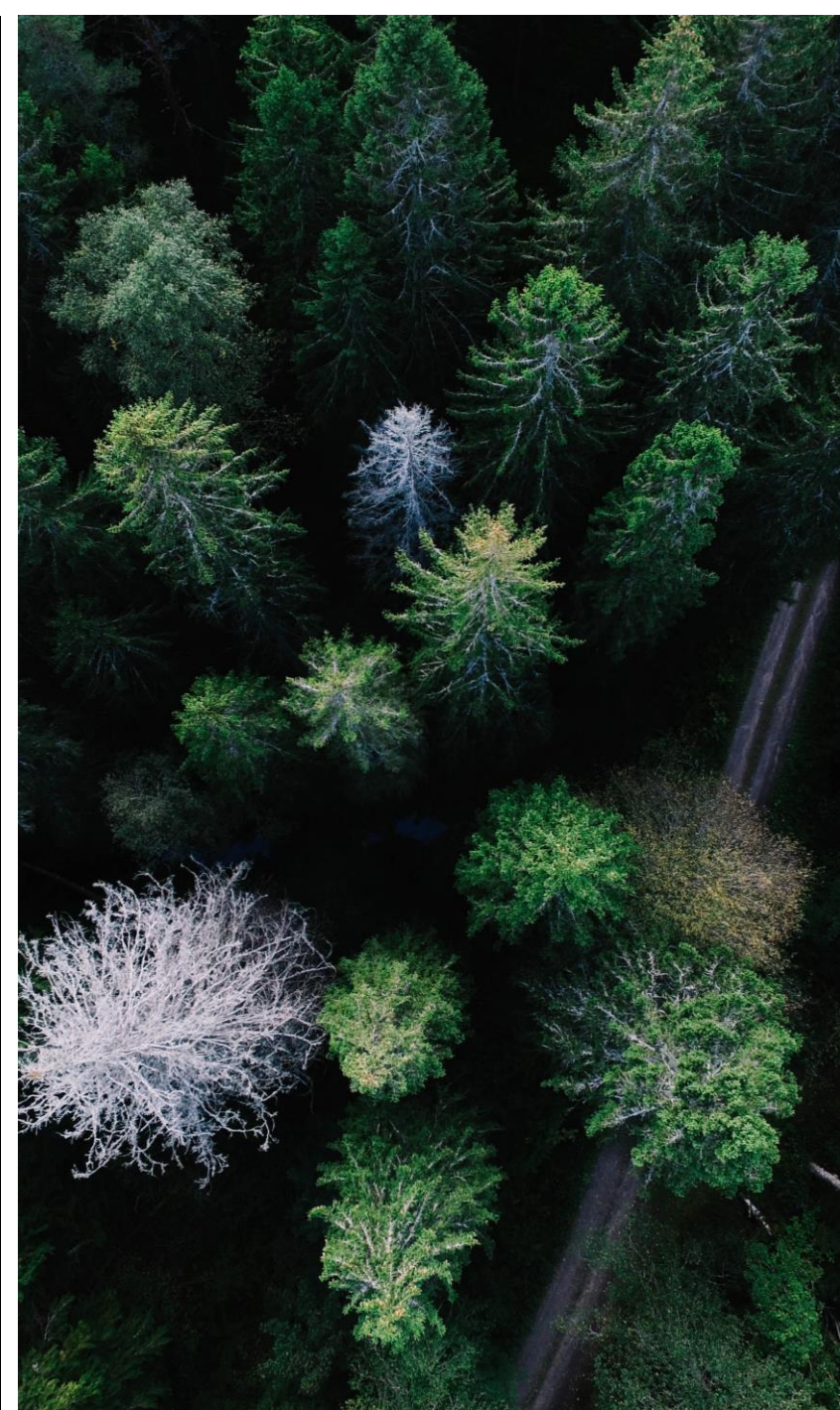




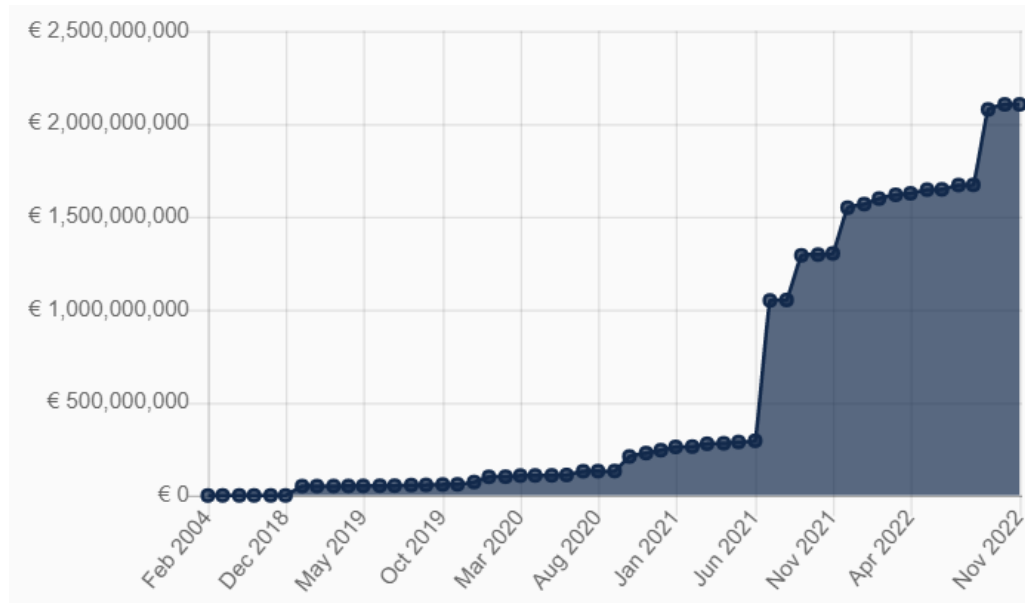
Data Privacy Awareness Training

Χαροκόπειο Πανεπιστήμιο





ΔΙΟΙΚΗΤΙΚΑ ΠΡΟΣΤΙΜΑ



ΜΕΓΑΛΥΤΕΡΕΣ ΠΟΙΝΕΣ ΤΟΥ GDPR ΓΙΑ ΤΟ 2022

1. Meta Platforms Ireland Ltd - €405m Fine
2. Clearview AI Inc. - €20m Fine
3. Clearview AI Inc. - €20m Fine
4. Clearview AI Inc. - €20m Fine
5. Clearview AI Inc. - €20m Fine
6. Meta Platforms Ireland Ltd. - €17m Fine
7. Google LLC - €10m Fine
8. Clearview AI Inc. - €9m Fine
9. REWE International - €8m Fine
10. Cosmote Mobile Telecommunications - €6m Fine
11. Vodafone España - €3.94m Fine
12. Dutch Tax & Customs Administration - €3.7m Fine
13. OTE Group - €3.25m Fine



Data Privacy

Τι είναι Προσωπικά Δεδομένα

Δεδομένα που σχετίζονται με ένα ζωντανό άτομο το οποίο **μπορεί να αναγνωριστεί** από τα δεδομένα και άλλες πληροφορίες που έχουμε στην κατοχή μας (ή είναι πιθανό να έρθουν στην κατοχή μας)

Περιλαμβάνει εκφράσεις απόψεων



Ορισμένες κατηγορίες προσωπικών δεδομένων ορίζονται ως **"Ευαίσθητα"**
Και έχουν μεγαλύτερο επίπεδο προστασίας.

© Baker Tilly Southeast Europe

Αρμοδιότητες «Υπεύθυνου επεξεργασίας δεδομένων» και «Εκτελών την Επεξεργασία»

Ο **υπεύθυνος επεξεργασίας** δεδομένων είναι η οντότητα που καθορίζει τους σκοπούς, τις προϋποθέσεις και τα μέσα επεξεργασίας προσωπικών δεδομένων και είναι η κύρια οντότητα και το αρμόδιο όργανο συλλογής δεδομένων. Αυτός οι αρμοδιότητες του υπευθύνου επεξεργασίας περιλαμβάνουν τη συλλογή της συνείδησης των ατόμων, την αποθήκευση των δεδομένων, τη διαχείριση της ανάλυσης, την παροχή του δικαιώματος πρόσβασης, καταγραφή και απόκριση σε παραβιάσεις δεδομένων. Επιπλέον, πρέπει να διαθέτει την ικανότητα να αποδεικνύει τη συμμόρφωση με τις αρχές που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Ο **εκτελών την επεξεργασία** υπονοείται να χρησιμοποιεί προσωπικά δεδομένα που του έχουν ανατεθεί για σκοπούς διαφορετικούς από αυτούς που περιγράφονται από τον υπεύθυνο επεξεργασίας δεδομένων. Κατόπιν αιτήματος, ο εκτελών την επεξεργασία πρέπει να διαγράψει ή να απεργαστεί όλα τα προσωπικά δεδομένα στον υπεύθυνο επεξεργασίας κατά την λήξη της σύμβασης παροχής υπηρεσιών.

Αυτές οι αρχές στο GDPR είναι:



Μπορεί να μεταφέρει προσωπικά δεδομένα σε τρίτη χώρα μόνο αφού λάβει την άδεια εξουσιοδότησης.

Πρέπει να λάβει γραπτή άδεια από τον υπεύθυνο επεξεργασίας πριν διατεθεί έναν υπαλλήλο και να αναλύσει την πλήρη εύληξη για αδυναμία του να τηρούν τις διατάξεις του GDPR.

Ο εκτελών την επεξεργασία πρέπει να επιτρέψει και να συμβάλει σε ελέγχους συμμόρφωσης που διενεργούνται από τον υπεύθυνο επεξεργασίας ή έναν εκπρόσωπο του υπεύθυνου επεξεργασίας.

Εάν υπάρχει παραβίαση δεδομένων, ο εκτελών την επεξεργασία αναμένεται να ενημερώσει τους υπευθύνους επεξεργασίας δεδομένων χωρίς αδικαιολόγητη καθυστέρηση.

© Baker Tilly Southeast Europe

Υποχρεώσεις εργαζομένων

- Προστασία προσωπικών δεδομένων με κάθε μέσο, πολιτική και διαδικασία που έχει γνωστοποιηθεί
- Επεξεργασία μόνο στο πλαίσιο των επιχειρηματικών σκοπών
- Άμεση ειδοποίηση σε περίπτωση σοβαρού συμβάντος (ή παραλίγο αστοχίας) στους καθυστερούμενους αρμόδιους φορείς (αφάρδια πληροφοριών, απόρρητο δεδομένων)
- Συμμόρφωση με τις πολιτικές του ιδρύματος, τις διαδικασίες ασφάλειας και προστασίας δεδομένων
- Προσωπική ευθύνη για τη διασφάλιση ότι οι προσωπικές πληροφορίες χρησιμοποιούνται δίκαια και νόμιμα στο πλαίσιο των εργασιακών δραστηριοτήτων.

© Baker Tilly Southeast Europe

Δικαιώματα των εργαζομένων

- Αιτήματα πρόσβασης υποκειμένων - 30 ημέρες
- Διόρθωση ανακριβών / διαγραφή πληροφοριών
- Αποτροπή του άμεσου μάρκετινγκ
- Αποτροπή της αυτοματοποιημένης λήψης αποφάσεων και δημιουργία προφίλ
- Φορητότητα δεδομένων - μεταφέρετε τα δεδομένα σας εάν αλλάζουν οι περιστάσεις σας

1/6/2023

© Baker Tilly Southeast Europe 10

Επεξεργασία Προσωπικών Δεδομένων

Η Επεξεργασία Δεδομένων περιλαμβάνει κάθε εργασία ή σύνολο εργασιών που εκτελείται σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε αυτοματοποιημένα είτε όχι, όπως συλλογή, καταγραφή, οργάνωση, διαμόρφωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, διαβούλευση, χρήση γνωστοποίηση μέσω μετάδοσης, διάδοσης ή άλλης διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής.

© Baker Tilly Southeast Europe

Διαρροή Δεδομένων

- Ο Υπεύθυνος Επεξεργασίας Δεδομένων πρέπει να κοινοποιεί τις παραβιάσεις όπου υπάρχει κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων στην τοπική Αρχή Προστασίας Δεδομένων **«χωρίς αδικαιολόγητη καθυστέρηση»** και εντός 72 ωρών.
- Για το λόγο αυτό, κάθε περιστατικό διαρροής προσωπικών δεδομένων (ακόμα και υπόνοια διαρροής) θα πρέπει να αναφέρεται στην αρμόδια Μενόδα για την έγκαιρη και αποτελεσματική διαχείριση της υπόθεσης.
- Σε περιπτώσεις όπου υπάρχει **«υψηλός κίνδυνος»** για δικαιώματα και ελευθερίες, το επηρεαζόμενο Υποκείμενο Δεδομένων πρέπει επίσης να ειδοποιηθεί **«χωρίς αδικαιολόγητη καθυστέρηση»**.

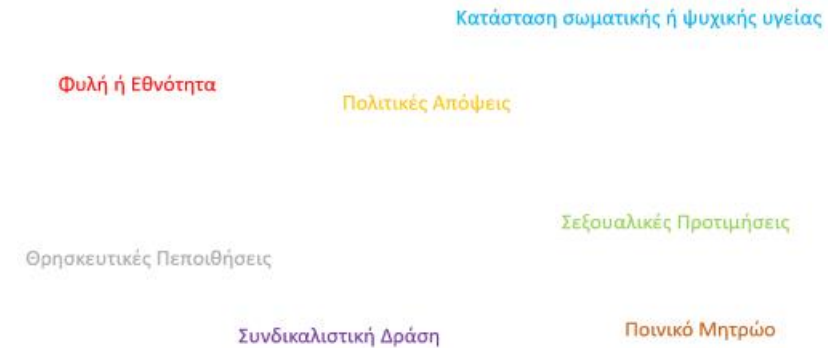
© Baker Tilly Southeast Europe



Τι είναι Προσωπικά Δεδομένα

Δεδομένα που σχετίζονται με ένα ζωντανό άτομο το οποίο **μπορεί να αναγνωριστεί** από τα δεδομένα και άλλες πληροφορίες που έχουμε στην κατοχή μας (ή είναι πιθανό να έρθουν στην κατοχή μας)

Περιλαμβάνει εκφράσεις απόψεων



Ορισμένες κατηγορίες προσωπικών δεδομένων ορίζονται ως **“Ευαίσθητα”**

Και έχουν μεγαλύτερο επίπεδο προστασίας.

Κατάσταση σωματικής ή ψυχικής υγείας

Φυλή ή Εθνότητα

Πολιτικές Απόψεις

Σεξουαλικές Προτιμήσεις

Θρησκευτικές Πεποιθήσεις

Συνδικαλιστική Δράση

Ποινικό Μητρώο

“Ευαίσθητα”



Αρμοδιότητες «Υπεύθυνου επεξεργασίας δεδομένων» και «Εκτελών την Επεξεργασία»

Ο **υπεύθυνος επεξεργασίας** δεδομένων είναι η οντότητα που καθορίζει τους σκοπούς, τις προϋποθέσεις και τα μέσα επεξεργασίας προσωπικών δεδομένων και είναι η κύρια οντότητα για τις αρμοδιότητες συλλογής δεδομένων. Αυτές οι αρμοδιότητες του υπεύθυνου επεξεργασίας περιλαμβάνουν τη συλλογή της συναίνεσης των ατόμων, την αποθήκευση των δεδομένων, τη διαχείριση της ανάκλησης συγκατάθεσης, την παροχή του δικαιώματος πρόσβασης, καταγραφής και απάντησης σε παραβιάσεις δεδομένων. Επιπλέον, πρέπει να διαθέτει την ικανότητα να αποδεικνύει τη συμμόρφωση με τις αρχές που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Αυτές οι αρχές στο GDPR είναι



Ο **εκτελών την επεξεργασία** απαγορεύεται να χρησιμοποιεί προσωπικά δεδομένα που του έχουν ανατεθεί για σκοπούς διαφορετικούς από αυτούς που περιγράφονται από τον υπεύθυνο επεξεργασίας δεδομένων. Κατόπιν αιτήματος, ο εκτελών την επεξεργασία πρέπει να διαγράψει ή να επιστρέψει όλα τα προσωπικά δεδομένα στον υπεύθυνο επεξεργασίας κατά την λήξη της σύμβασης παροχής υπηρεσιών.

Μπορεί να μεταφέρει προσωπικά δεδομένα σε τρίτη χώρα μόνο αφού λάβει τη νόμιμη εξουσιοδότηση.

Πρέπει να λάβει γραπτή άδεια από τον υπεύθυνο επεξεργασίας πριν δεσμεύσει έναν υπεργολάβο και να αναλάβει την πλήρη ευθύνη για αδυναμίες του να τηρήσουν τις διατάξεις του GDPR.

Ο εκτελών την επεξεργασία πρέπει να επιτρέπει και να συμβάλλει σε ελέγχους συμμόρφωσης που διενεργούνται από τον υπεύθυνο επεξεργασίας ή έναν εκπρόσωπο του υπεύθυνου επεξεργασίας.

Εάν υπάρξει παραβίαση δεδομένων, ο εκτελών την επεξεργασία αναμένεται να ενημερώσει τους υπευθύνους επεξεργασίας δεδομένων χωρίς αδικαιολόγητη καθυστέρηση.

Αυτές οι αρχές στο GDPR είναι

- 1.** Νομιμότητα, Αντικειμενικότητα, διαφάνεια
Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε δίκαιη και νόμιμη επεξεργασία
- 2.** Περιορισμός Σκοπού
Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία για τον σκοπό για τον οποίο συλλέγονται
- 3.** Ελαχιστοποίηση δεδομένων
Τα προσωπικά δεδομένα πρέπει να είναι επαρκή, σχετικά και όχι υπερβολικά
- 4.** Ακρίβεια
Τα προσωπικά δεδομένα πρέπει να είναι ακριβή και ενημερωμένα
- 5.** Storage Limitation
Τα προσωπικά δεδομένα δεν πρέπει να διατηρούνται για περισσότερο από ό,τι είναι απαραίτητο
- 6.** Εμπιστευτικότητα & Ακεραιότητα
Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία με τέτοιο τρόπο ώστε να διασφαλίζεται η κατάλληλη ασφάλεια, ακεραιότητα και εμπιστευτικότητα
- 7.** Λογοδοσία
Η εταιρεία είναι υπεύθυνη να μπορεί να αποδείξει τη συμμόρφωση με τον GDPR με όλες αυτές τις αρχές



Δίκαιη και νόμιμη επεξεργασία

Σε καθαρή γλώσσα, πρέπει να ενημερώσουμε τα υποκείμενα των δεδομένων:

- Ότι τα προσωπικά τους δεδομένα υποβάλλονται σε επεξεργασία
- Γιατί υποβάλλονται σε επεξεργασία τα προσωπικά τους δεδομένα
- Σχετικά με τυχόν «μη προφανείς» λόγους για τους οποίους θα επεξεργαστούμε τα δεδομένα τους (π.χ. σκοπούς μάρκετινγκ.)

Αυτές οι πληροφορίες περιέχονται στη Δήλωση Απορρήτου μας



Επεξεργασία για περιορισμένους σκοπούς

- Πρέπει να έχουμε έναν πολύ συγκεκριμένο λόγο για την επεξεργασία δεδομένων – σύνδεση με την πρώτη αρχή
- Τα δεδομένα μπορούν να υποβληθούν σε επεξεργασία μόνο για τον συγκεκριμένο σκοπό
- Η συναίνεση δεν απαιτείται πάντα – το μεγαλύτερο μέρος της επεξεργασίας που κάνουμε μπορεί να γίνει χωρίς συγκατάθεση



Επαρκές, σχετικό και όχι υπερβολικό

Σχετικά με τη συλλογή της σωστής ποσότητας πληροφοριών για τον καθορισμένο σκοπό – ούτε λιγότερο ούτε περισσότερο

- Ποιες πληροφορίες είναι απολύτως κρίσιμες για τη διαδικασία – το ελάχιστο που απαιτείται για την εκπλήρωση του σκοπού
- Ό,τι απομένει, **δεν μπορεί να δικαιολογηθεί** ως απαραίτητο και ενδέχεται να θεωρηθεί υπερβολικό!



Ακριβή και επίκαιρα δεδομένα

- Πρέπει να ληφθούν μέτρα για να βεβαιωθείτε ότι τα δεδομένα είναι ακριβή και ενημερωμένα
- Αυτό αποτρέπει την ενόχληση, τη ζημιά ή την δυσφορία



Δεν διατηρούνται δεδομένα για περισσότερο από όσο είναι απαραίτητο

- Μόλις τα προσωπικά δεδομένα εξυπηρετήσουν τον σκοπό τους, πρέπει να απορριφθούν με ασφάλεια
- Τακτικός έλεγχος και διαγραφή δεδομένων που δεν απαιτούνται πλέον
- Όσο περισσότερο διατηρούνται τα αρχεία, τόσο περισσότερο πρέπει να διασφαλίσουμε ότι είναι ακριβή
- Η διατήρηση πληροφοριών που δεν έχουν πλέον κανένα χρήσιμο σκοπό θα μπορούσε να θεωρηθεί ως «υπερβολική»
- Πολιτική Ασφάλειας Πληροφοριών και Προστασίας Δεδομένων – πίνακας διατήρησης

Ασφάλεια



Λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα κατά της μη εξουσιοδοτημένης ή παράνομης επεξεργασίας προσωπικών δεδομένων και κατά της τυχαίας απώλειας ή καταστροφής / βλάβης δεδομένων προσωπικού χαρακτήρα

Τεχνικά

Κωδικοί Κρυπτογράφηση Κλείδωμα Οθόνης
Τείχη Προστασίας Κάρτες Πρόσβασης Πολιτική IT

Οργανωτικά

Τοποθέτηση Οθονών Κατάρτιση και Ευαισθητοποίηση Εργολάβοι
Κλειδωμένα ντουλάπια αρχειοθέτησης Πολιτική Ασφάλειας Πληροφοριών και Προστασίας Δεδομένων
Εμπιστευτική Διάθεση Απορριμμάτων Housekeeping Εκτιμήσεις Κινδύνου

Τεχνικά

Κωδικοί

Κρυπτογράφηση

Κλείδωμα Οθόνης

Τείχη Προστασίας

Κάρτες Πρόσβασης

Πολιτική IT

Οργανωτικά

Τοποθέτηση Οθονών

Κατάρτιση και Ευαισθητοποίηση

Εργολάβοι

Κλειδωμένα ντουλάπια αρχειοθέτησης

Πολιτική Ασφάλειας Πληροφοριών και
Προστασίας Δεδομένων

Εμπιστευτική Διάθεση Απορριμμάτων

Housekeeping

Εκτιμήσεις Κινδύνου



Επεξεργασία Προσωπικών Δεδομένων

Η Επεξεργασία Δεδομένων περιλαμβάνει κάθε εργασία ή σύνολο εργασιών που εκτελείται σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε αυτοματοποιημένα είτε όχι, όπως συλλογή, καταγραφή, οργάνωση, διαμόρφωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, διαβούλευση, χρήση γνωστοποίηση μέσω μετάδοσης, διάδοσης ή άλλης διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής.



Υποχρεώσεις εργαζομένων

- Προστασία προσωπικών δεδομένων με κάθε μέσο, πολιτική και διαδικασία που έχει γνωστοποιηθεί
- Επεξεργασία μόνο στο πλαίσιο των επιχειρηματικών σκοπών
- Άμεση ειδοποίηση σε περίπτωση σοβαρού συμβάντος (ή παραλίγο αστοχίας) στους καθορισμένους αρμόδιους φορείς (ασφάλεια πληροφοριών, απόρρητο δεδομένων)
- Συμμόρφωση με τις πολιτικές του Ιδρύματος, τις διαδικασίες ασφάλειας και προστασίας δεδομένων
- Προσωπική ευθύνη για τη διασφάλιση ότι οι προσωπικές πληροφορίες χρησιμοποιούνται δίκαια και νόμιμα στο πλαίσιο των εργασιακών δραστηριοτήτων.



Δικαιώματα των εργαζομένων

- Αιτήματα πρόσβασης υποκειμένων – 30 ημέρες
- Διόρθωση ανακρίβειών / διαγραφή πληροφοριών
- Αποτροπή του άμεσου μάρκετινγκ
- Αποτροπή της αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ
- Φορητότητα δεδομένων - μεταφέρετε τα δεδομένα σας εάν αλλάξουν οι περιστάσεις σας



Διαρροή Δεδομένων

- Ο Υπεύθυνος Επεξεργασίας Δεδομένων πρέπει να κοινοποιεί τις παραβιάσεις όπου υπάρχει κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων στην τοπική Αρχή Προστασίας Δεδομένων **«χωρίς αδικαιολόγητη καθυστέρηση»** και εντός 72 ωρών.
Για το λόγο αυτό, κάθε περιστατικό διαρροής προσωπικών δεδομένων (ακόμα και υπόνοια διαρροής) θα πρέπει να αναφέρεται στην αρμόδια Μονάδα για την έγκαιρη και αποτελεσματική διαχείριση της υπόθεσης.
- Σε περιπτώσεις όπου υπάρχει **«υψηλός κίνδυνος»** για δικαιώματα και ελευθερίες, το επηρεαζόμενο Υποκείμενο Δεδομένων πρέπει επίσης να ειδοποιηθεί **«χωρίς αδικαιολόγητη καθυστέρηση»**



Πως να προετοιμαστείτε

1. Διαβάστε και επισκοπήστε

- Πολιτική ασφάλειας και προστασίας δεδομένων
- Πολιτική αποδεκτής χρήσης
- Οδηγίες και κατευθυντήριες γραμμές

2. Κατανοήστε γιατί επεξεργάζεστε δεδομένα

- Ελαχιστοποιήστε την επεξεργασία όπου είναι δυνατόν
- Σαφήνεια σχετικά με το τι δεδομένα που διατηρείτε και γιατί
- Παρακολουθήστε την εκπαίδευση, διαβάστε οδηγούς, μιλήστε με συναδέλφους

3. Σκεφτείτε την Ασφάλεια

- Ποιος μπορεί να έχει πρόσβαση σε πληροφορίες; Κωδικοί πρόσβασης και κρυπτογράφηση
- Μπορούμε να ελαχιστοποιήσουμε τα δεδομένα; Εξετάστε το ενδεχόμενο χρήσης Bcc σε λίστες αλληλογραφίας.

4. Θέσπιση Συμφωνιών Κοινής Χρήσης Δεδομένων

- Με ποιον μοιραζόμαστε δεδομένα
- Γιατί μοιραζόμαστε αυτά τα δεδομένα
- Τι συμβαίνει όταν τα δεδομένα δεν απαιτούνται πλέον



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού,
Εκπαίδευση και Διά Βίου Μάθηση

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

