



Αθήνα, 16 Μαρτίου 2018  
Αρ. Πρωτ. 16/16.03,.2018

Προς  
Μέλη του Συνδέσμου Ελληνικού Οίνου

**ΘΕΜΑ: Κανονισμός για την προστασία των προσωπικών δεδομένων**

Αγαπητά μέλη,

Διά του παρόντος και σε συνέχεια της σχετικής εισήγησης που έλαβε χώρα στην τακτική Γενική Συνέλευση του Συνδέσμου, θα θέλαμε να σας ενημερώσουμε για τις νομοθετικές εξελίξεις που επέρχονται με τον **Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα** και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) και στις υποχρεώσεις που αυτός επέлагεται για την επιχείρησή σας.

**1. Λίγα λόγια για τον Κανονισμό:**

Ο εν λόγω Κανονισμός προστατεύει τα **φυσικά πρόσωπα** (και όχι τις επιχειρήσεις ή τους οργανισμούς) έναντι της **επεξεργασίας** (δηλαδή της συλλογής, καταχώρισης, οργάνωσης, διάρθρωσης, αποθήκευσης, προσαρμογής ή μεταβολής, ανάκτησης, αναζήτησης πληροφοριών, χρήσης, κοινολόγησης με διαβίβαση, διάδοσης ή κάθε άλλης μορφής διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής) **δεδομένων προσωπικού χαρακτήρα** (όπως όνομα, αριθμό ταυτότητας, δεδομένα θέσης, ΑΜΚΑ, ΑΦΜ, διεύθυνση κατοικίας, επιγραμμικό αναγνωριστικό ταυτότητας ή έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική –πχ Δηλώσεις εισοδήματος κι εκκαθαριστικά, Ε9-, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου).

Έτσι λοιπόν, **όσοι** προβαίνουν σε

-εν όλω ή εν μέρει, **αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα που ανήκουν σε φυσικά πρόσωπα,**

-καθώς και στη **μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα που ανήκουν σε φυσικά πρόσωπα** τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης (δηλαδή διατήρηση σε ειδικούς φυσικούς ή ηλεκτρονικούς φακέλους)

υποχρεούνται να συμμορφώνονται στις διατάξεις του Κανονισμού.

Ο Κανονισμός τίθεται σε ισχύ την **25 Μαΐου 2018** και οι συνέπειες της παραβίασής του αφορούν σε πρόστιμα που ανέρχονται σε το πολύ 20 εκατ. Ευρώ ή το 4% των παγκόσμιων εσόδων για την προηγούμενη οικονομική χρονιά. Ενδεχομένως τα κράτη – μέλη να θεσπίσουν άλλες διοικητικές και ποινικές κυρώσεις.

Με βάση τον Κανονισμό, η παραβίαση των υποχρεώσεων των υπεύθυνων επεξεργασίας προκύπτει

- εάν υποβληθεί σχετική καταγγελία από το υποκείμενο των προσωπικών δεδομένων προς την αρμόδια Αρχή ότι α) η επεξεργασία των δεδομένων του έγινε παράνομα, β) ότι παρεμποδίστηκε στην άσκηση των δικαιωμάτων που προβλέπει ο Κανονισμός ή γ) ότι αυτά δεν έγιναν σεβαστά

- σε περίπτωση παραβίασης και διαρροής των προσωπικών δεδομένων.

Άρα, **προς το παρόν δεν προβλέπονται προληπτικοί έλεγχοι** τήρησης του εν λόγω Κανονισμού, **ούτε απαιτείται κάποια επίσημη ενέργεια** από την πλευρά των υπεύθυνων επεξεργασίας προς την αρμόδια ανεξάρτητη Αρχή ή τρίτο. **Δεν απαιτείται επίσης η λήψη πιστοποιητικών σύννομης λειτουργίας, ούτε η τήρηση οποιουδήποτε τύπου.** Απαιτούνται μόνο **προληπτικές ενέργειες** αναφορικά με

- την επεξεργασία της εταιρικής πολιτικής
- τον επανασχεδιασμό των υποδομών
- την εφαρμογή κατάλληλων λύσεων
- την εκπαίδευση υπαλλήλων

ώστε να μην ανακύψει ζήτημα ή όταν αυτό ανακύψει να γίνει σωστή διαχείρισή του.

Βέβαια, ενδέχεται η Εθνική Αρχή ή και η Ευρωπαϊκή Επιτροπή να επανέλθει στο ζήτημα θέτοντας και προληπτικούς ελέγχους, ωστόσο, αυτό δεν συντρέχει προς το παρόν.

## **2. Πρακτικά, τα παραπάνω σημαίνουν για τις οινοποιητικές επιχειρήσεις ότι:**

Για όλα τα προσωπικά δεδομένα που συλλέγουν για τους εργαζομένους τους ή τους πελάτες ή τους προμηθευτές τους (όταν πρόκειται για φυσικά πρόσωπα και όχι για επιχειρήσεις), θα πρέπει οι οινοποιητικές επιχειρήσεις να συστήσουν διαδικασίες και να λάβουν μέτρα ώστε

### **A) Τα δεδομένα αυτά να συλλέγονται με βάση την συναίνεση του υποκειμένου ή για κάποιο νόμιμο σκοπό.**

Ειδικότερα:

-Είτε θα πρέπει να ληφθεί **η συναίνεση του υποκειμένου**, δηλαδή συνταχθεί ένα έγγραφο που θα εξηγήει στο υποκείμενο ποια δεδομένα του

συλλέγονται, με ποιό σκοπό, για πόσο διάστημα και στο οποίο διά της υπογραφής του από το υποκείμενο θα δίδεται συναίνεση επεξεργασίας.

-Είτε θα πρέπει η επιχείρηση να έχει μία **νόμιμη βάση για τη συλλογή** τους, δηλαδή να συλλέξει και να επεξεργαστεί μόνο εκείνα τα προσωπικά δεδομένα του υποκειμένου τα οποία είναι απαραίτητα:

- για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος (πχ για την πληρωμή του υπαλλήλου)
- για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,
- για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, (πχ ασφάλιση στο ΙΚΑ)
- για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, (πχ εξασφάλιση απαίτησης)

**B) Να παρέχεται πληροφόρηση στο υποκείμενο για την επεξεργασία των προσωπικών δεδομένων του και ειδικότερα η επιχείρηση να ενημερώνει για:**

- α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας,
- β) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,
- γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,
- δ) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,
- ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων,
- στ) όταν η επεξεργασία σε συναίνεση, την ύπαρξη του δικαιώματος να ανακαλέσει τη συναίνεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,
- ζ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,
- η) κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών.

Παράδειγμα: η οινοποιητική επιχείρηση διαθέτει ηλεκτρονική σελίδα, στην οποία ένας καταναλωτής συμπληρώνοντας μία φόρμα παρέχει προσωπικά

του στοιχεία, προκειμένου να εγγραφεί στο club του οινοποιείου. Η επιχείρηση είναι υποχρεωμένη να έχει ειδικό ενημερωτικό μπάνερ, στο οποίο θα αναφέρονται όλα τα παραπάνω.

### **Γ) Να εξασφαλίζεται η άσκηση των δικαιωμάτων των υποκειμένων**

Τα δικαιώματα αυτά είναι:

- *Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων* : Δηλαδή η οινοποιητική επιχείρηση είναι υποχρεωμένη **κατόπιν αιτήματος** να ενημερώνει το υποκείμενο για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία. Επιπλέον, θα πρέπει, εάν συμβαίνει τούτο, να παρέχει τις εξής πληροφορίες: α) τους σκοπούς της επεξεργασίας, β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς, δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα, ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία, στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή, ζ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους, η) καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.
- *Δικαίωμα διόρθωσης*: Δηλαδή η οινοποιητική επιχείρηση είναι υποχρεωμένη, **κατόπιν αιτήματος**, να προβαίνει σε διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα ή συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, εφόσον της υποβληθεί σχετικό αίτημα.
- *Δικαίωμα διαγραφής -«δικαίωμα στη λήθη»*: Δηλαδή η οινοποιητική επιχείρηση είναι υποχρεωμένη, **κατόπιν αιτήματος** του υποκειμένου, να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους λόγους που προβλέπει ο Κανονισμός:
  - α) τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν (πχ έληξε η σύμβαση εργασίας)

- β) το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,
- γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία
- δ) τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,
- *Δικαίωμα περιορισμού της επεξεργασίας* : Δηλαδή η οινοποιητική επιχείρηση είναι υποχρεωμένη να περιορίζει **κατόπιν αιτήματος** του υποκειμένου την επεξεργασία των δεδομένων, όταν συντρέχουν κάποιες προϋποθέσεις:
    - α) το υποκείμενο των δεδομένων αμφισβητεί την ακρίβεια των δεδομένων προσωπικού χαρακτήρα, υπό την προϋπόθεση ότι αφορά σε χρονικό διάστημα που επιτρέπει στην επιχείρηση να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα (δηλ. δεν μπορεί κάποιος να ζητήσει στοιχεία που συλλέχθηκαν πολύ παλιά),
    - β) η επεξεργασία είναι παράνομη (δηλαδή δεν έχει γίνει με βάση την συναίνεση ή κάποιο νόμιμο λόγο) και το υποκείμενο των δεδομένων ζητεί τον περιορισμό της χρήσης τους,
    - γ) η επιχείρηση δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων (για παράδειγμα, ένας εργαζόμενος που θέλει να διεκδικήσει οφειλόμενα από υπερωρίες μπορεί να ζητήσει τη διατήρηση των δεδομένων του από την επιχείρηση, ακόμη κι αν έχει απολυθεί),
    - δ) όταν το υποκείμενο έχει υποβάλει αντιρρήσεις για την επεξεργασία, και αναμένεται επαλήθευση του κατά πόσον οι νόμιμοι λόγοι της επιχείρησης υπερσχύουν έναντι των λόγων του υποκειμένου των δεδομένων (πχ ο εργαζόμενος που απολύθηκε έχει αντίρρηση για τη διατήρηση των δεδομένων του, αλλά η επιχείρηση του αντιτείνει ότι από το νόμο έχει υποχρέωση να τα διατηρήσει για ένα χρονικό διάστημα μετά την απόλυσή του)
  - *Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας*: Δηλαδή η οινοποιητική επιχείρηση οφείλει να ανακοινώνει στο υποκείμενο κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων
  - *Δικαίωμα εναντίωσης*: Η οινοποιητική επιχείρηση οφείλει να δίδει το δικαίωμα στο υποκείμενο να αρνείται αιτιολογημένα την επεξεργασία των προσωπικών του δεδομένων.

**Δ) Να έχουν ληφθεί κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων παραβίασης**

Ειδικότερα και σε συνεργασία με Τεχνικό Ασφαλείας Υπολογιστών θα πρέπει κατά περίπτωση να λάβουν χώρα ενέργειες για την εξασφάλιση:

- α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,
- β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,
- γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,
- δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

**Ε) Να εξασφαλίζεται η ενημέρωση της Αρχής ή και των υποκειμένων όταν αυτό είναι απαραίτητο σε περίπτωση παραβίασης**

Ειδικότερα, η οιοποιητική επιχείρηση είναι υποχρεωμένη να προβεί σε:

**1. Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή, εντός 72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η γνωστοποίηση πρέπει να περιλαμβάνει κατ'ελάχιστον τα στοιχεία που προβλέπει ο Κανονισμός.

**2. Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων,** όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η γνωστοποίηση πρέπει να περιλαμβάνει κατ'ελάχιστον τα στοιχεία που προβλέπει ο Κανονισμός. Η ανακοίνωση αυτή είναι προαιρετική όταν πληρούνται οι προϋποθέσεις που προβλέπει ο Κανονισμός (όταν δηλαδή α) η επιχείρηση εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση, β) η επιχείρηση έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει

υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, γ) προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

### **3. Η οργάνωση της επιχείρησής σας σε δέκα βήματα:**

Βήμα 1: Ενημερωθείτε για το νέο Κανονισμό και σκεφτείτε πώς λειτουργεί σήμερα η επιχείρησή σας και ειδικότερα ποιες είναι οι πηγές των δεδομένων, με ποιον τρόπο περιέχονται σε εσάς, πώς χειρίζεστε τα δεδομένα και το φάσμα των μέτρων ασφάλειας της πληροφορικής που διαθέτετε. Εξετάστε ποιους τύπους δεδομένων συλλέγετε αυτήν τη στιγμή από τους προμηθευτές, τους πελάτες και τους εργαζομένους σας, για ποιο σκοπό και πού αποθηκεύονται αυτά τα δεδομένα.

Βήμα 2: Ελαχιστοποιείστε τα συλλεγόμενα προσωπικά δεδομένα: συλλέξτε μόνο τα δεδομένα που είναι απολύτως απαραίτητα για τους σκοπούς για τους οποίους συλλέγονται. Αποφύγετε την αντιμετώπιση ευαίσθητων δεδομένων (εθνική φυλετική καταγωγή, θρησκευτική ή φιλοσοφική άποψη, ιδιότητα μέλους συνδικαλιστικών οργανώσεων, γενετικά δεδομένα, βιομετρικά δεδομένα και γενετήσιος προσανατολισμός).

Βήμα 3: Εξασφαλίστε τη νομική βάση για την επεξεργασία δεδομένων: δείτε εάν πρόκειται για περίπτωση συγκατάθεσης του ατόμου, νομικής υποχρέωσης της εταιρίας σας ή έννομα συμφέροντα του συλλέκτη δεδομένων. Σύμφωνα με το GDPR ορισμένα δικαιώματα των υποκειμένων τροποποιούνται ανάλογα με τη νόμιμη βάση για την επεξεργασία των προσωπικών τους δεδομένων. Συνήθως οι περισσότερες περιπτώσεις συλλογής δεδομένων στις οινοποιητικές επιχειρήσεις αποτελούν νομική υποχρέωση. Η διαμόρφωση και λήψη έγγραφης συναίνεσης σε κάθε περίπτωση μπορεί να άρει τυχόν αμφιβολίες. Και όταν πρόκειται να επεξεργαστείτε προσωπικά δεδομένα στην ειδοποίησή σας σχετικά με το απόρρητο ή όταν απαντάτε σε ένα αίτημα, θα πρέπει επίσης να εξηγήσετε και να τεκμηριώσετε τη νόμιμη βάση σας.

Βήμα 4: Ενημερώστε τους ανθρώπους των οποίων τα δεδομένα συλλέγονται: δημιουργείστε έντυπο ή ηλεκτρονικό κείμενο νομικής ειδοποίησης (ταυτότητα του υπεύθυνου επεξεργασίας δεδομένων, σκοποί και βάση της επεξεργασίας, περίοδος διατήρησης των δεδομένων, δικαιώματα προσώπων στα προσωπικά τους δεδομένα).

Βήμα 5: Δημιουργείτε διαδικασίες επεξεργασίας προσωπικών. Ορίστε ποιό τμήμα ή ποιος υπάλληλος θα παραλαμβάνει τα προσωπικά δεδομένα και πώς θα τα επεξεργάζεται νόμιμα.

Βήμα 6: Ορίστε συγκεκριμένες ημέρες και τμήματα που θα ελέγχουν εάν πρέπει να εξακολουθείτε να διατηρείτε τα ήδη συλλεγμένα προσωπικά δεδομένα.

Βήμα 7: Θεσπίστε διαδικασίες σεβασμού των δικαιωμάτων των ατόμων σχετικά με τα δεδομένα που τα αφορούν: το δικαίωμα να αντιταχθούν στη συλλογή τους, το δικαίωμα πρόσβασης, το δικαίωμα διόρθωσης, το δικαίωμα παραγραφής, το δικαίωμα να ξεχαστεί και το δικαίωμα μεταφοράς. Ορίστε διαδικασίες και υπεύθυνο απάντησης των οικείων αιτημάτων. Για παράδειγμα: Στις περισσότερες περιπτώσεις δεν θα μπορείτε να χρεώσετε για την ικανοποίηση ενός αιτήματος. Θα έχετε ένα μήνα για να συμμορφωθείτε. Μπορείτε να αρνηθείτε ή να χρεώσετε αιτήσεις που είναι προδήλως αβάσιμες ή υπερβολικές. Εάν απορρίψετε ένα αίτημα, πρέπει να το αιτιολογήσετε στο υποκείμενο και να το ενημερώσετε ότι έχει το δικαίωμα να υποβάλει καταγγελία στην εποπτική αρχή και σε ένδικα μέσα. Πρέπει να το κάνετε αυτό χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός ενός μηνός

Βήμα 8: Εξασφαλίστε την ασφάλεια των προσωπικών δεδομένων: υιοθετήστε ένα επίπεδο ασφάλειας προσαρμοσμένο στον κίνδυνο μέσω τεχνικών μέτρων (κωδικοί πρόσβασης, ενημέρωση του λογισμικού προστασίας του υπολογιστή σας, τοποθετήστε τα αρχεία ή τον υπολογιστή σε ένα δωμάτιο που κλείνει κλειδί ...), οργανωτικά (να ενημερώνονται οι εργαζόμενοι για τα δεδομένα αυτά σχετικά με την προστασία τους ...) και συμβατικά (εάν χρησιμοποιείτε έναν υπεργολάβο στον οποίο αναθέτετε αυτά τα στοιχεία, να τον ρωτήσετε στην απόφασή του ή στην επιστολή αποστολής του για την προστασία των προσωπικών δεδομένων που διαβιβάστηκαν ...).

Βήμα 9: Εντοπισμός, αναφορά και διερεύνηση παραβίασης προσωπικών δεδομένων. Θα πρέπει να τεθούν σε εφαρμογή διαδικασίες για την αποτελεσματική ανίχνευση, αναφορά και διερεύνηση μιας παραβίασης των προσωπικών δεδομένων. Θα πρέπει να ειδοποιήσετε την Εθνική Αρχή για μια παραβίαση μόνο όταν είναι πιθανό να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων. Όταν υπάρχει κίνδυνος να παραβιαστούν τα προσωπικά δεδομένα, αξίζει να διασφαλιστεί ότι η επιχείρησή σας πληροί τις απαιτήσεις ασφάλειας δεδομένων GDPR. Αυτό θα πρέπει να γίνει με τη βοήθεια εξειδικευμένων τεχνικών.





Βήμα 10: Δημιουργείστε συστήματα και κανάλια επικοινωνίας με την αρχή προστασίας δεδομένων. Ορίστε ποιος θα είναι ο υπεύθυνος της επικοινωνίας.

Με τιμή,

Θεόδωρος Γεωργόπουλος  
Καθηγητής Νομικής – Πανεπιστήμιο Reims, Γαλλία  
Διεθντής ΣΕΟ  
Δικηγόρος