Πειραιάς, Μάιος 2018

ΣΥΝΟΠΤΙΚΟΣ ΟΔΗΓΟΣ

ΠΡΟΕΤΟΙΜΑΣΙΑΣ ΓΙΑ ΤΗ ΣΥΜΜΟΡΦΩΣΗ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕ ΤΟ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝΔΕΔΟΜΕΝΩΝ (GDPR)

Στο πλαίσιο της ενημέρωσης των επιχειρήσεων – μελών του, το Εμπορικό και Βιομηχανικό Επιμελητήριο Πειραιώς έχει συντάξει τον παρόντα Οδηγό, ο οποίος, με τη μορφή γενικών ερωτήσεων και παραδειγμάτων, σύμφωνα με τα όσα έχουν ανακοινωθεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, δίνει μία γενική εικόνα- περίγραμμα των βασικών εννοιών και υποχρεώσεων γύρω από τον Γενικό Κανονισμό για την Προστασία Δεδομένων της ΕΕ (GDPR), που τίθεται σε υποχρεωτική εφαρμογή στις 25 Μαΐου 2018.

1. Τι είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων;

Στις 25 Μαΐου 2018 τίθεται σε υποχρεωτική εφαρμογή ο Κανονισμός ΕΕ 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την Προστασία Δεδομένων – General Data Protection Regulation- GDPR).

Ο Κανονισμός είναι γενικής εφαρμογής, υποχρεωτικός και άμεσα εφαρμόσιμος σε όλα τα κράτη μέλη, χωρίς να υπάρχει υποχρέωση για την ενσωμάτωσή του στην εθνική νομοθεσία του κάθε κράτους μέλους. Ο Κανονισμός αφορά οριζόντια κάθε επιχείρηση - υπεύθυνο επεξεργασίας (δηλαδή όλες τις επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα **φυσικών προσώπων**), ανεξάρτητα από κλάδο οικονομικής δραστηριότητας και μέγεθος και εφαρμόζεται στις περιπτώσεις που εκτελείται μερική ή ολική αυτοματοποιημένη ή μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

Ο Κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των οργανισμών αναφορικά με τη διαχείριση προσωπικών δεδομένων, ενώ σε περιπτώσεις μη συμμόρφωσης, το μέγεθος των προβλεπομένων προστίμων (μέχρι 20 εκ. ευρώ ή το 4% του παγκόσμιου τζίρου).

Με τον Κανονισμό διευρύνεται και εξειδικεύεται η έννοια των **απλών** δεδομένων (θέσης, επιγραμμικά [on line] αναγνωριστικά στοιχεία ταυτότητας τα οποία παρέχονται από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα τους και διευκολύνουν τον εντοπισμό του υποκειμένου [ip addresses ή εντοπισμός θέσης μέσω GPS, cookies, RFID]) καθώς και των **ευαίσθητων** προσωπικών δεδομένων (γενετικά και βιομετρικά). Επιπλέον, προστίθενται έννοιες όπως «περιορισμός της επεξεργασίας», «Κατάρτιση προφίλ», «ψευδωνυμοποίηση», «δικαίωμα στη λήθη».

2. Ποιες επιχειρήσεις αφορά ο Κανονισμός και σε ποιες προβλέπονται - και τι είδους – παρεκκλίσεις;

Αφορά όλες τις επιχειρήσεις (ιδιωτικού και δημόσιου δικαίου) που με οποιοδήποτε τρόπο διαχειρίζονται προσωπικά δεδομένα εργαζομένων, συνεργατών, πελατών, προμηθευτών ή άλλων φυσικών προσώπων (δεν αφορά επεξεργασία δεδομένων νομικών οντοτήτων). Δηλαδή αφορά σχεδόν το σύνολο των επιχειρήσεων, συμπεριλαμβανομένων και των ατομικών επιχειρήσεων (επιτηδευματίες).

Ο Κανονισμός προβλέπει παρέκκλιση για επιχειρήσεις και οργανισμούς που απασχολούν λιγότερα από 250 άτομα μόνον ως προς την υποχρέωση τήρησης αρχείων δραστηριοτήτων επεξεργασίας. Κατά τα λοιπά όλες οι επιχειρήσεις πρέπει να τηρούν και να εφαρμόζουν τις υποχρεώσεις που απορρέουν από τον Κανονισμό. Υπενθυμίζουμε ότι η κατηγορία των πολύ μικρών, μικρών και μεσαίων επιχειρήσεων (ΜΜΕ) αποτελείται από επιχειρήσεις που απασχολούν λιγότερους από 250 εργαζομένους και των οποίων ο ετήσιος κύκλος εργασιών δεν υπερβαίνει τα 50 εκατομμύρια ευρώ ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 43 εκατομμύρια ευρώ.

Κατ’ εξαίρεση, εφόσον η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, εφόσον η επεξεργασία δεν είναι περιστασιακή ή εφόσον περιλαμβάνει ειδικές κατηγορίες δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα, τότε και οι επιχειρήσεις αυτές (ΜΜΕ) οφείλουν να τηρούν αρχεία δραστηριοτήτων επεξεργασίας.

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

3. Τι περιλαμβάνει ένα αρχείο δραστηριοτήτων επεξεργασίας;

Η καταγραφή επεξεργασιών από τους υπευθύνους επεξεργασίας που απασχολούν πάνω από 250 άτομα ή επεξεργάζονται υψηλού κινδύνου δεδομένα ή δεδομένα ειδικών κατηγοριών, γίνεται μετά από τεκμηρίωση με τα ακόλουθα στοιχεία:

- Το σκοπό της επεξεργασίας
- Τα δεδομένα και τα υποκείμενα
- Τους αποδέκτες των δεδομένων
- Τις ενδεχόμενες διαβιβάσεις εκτός ΕΕ
- Το χρόνο τήρησης
- Τα οργανωτικά και τεχνικά μέτρα προστασίας

Παρόμοια υποχρέωση θεσπίζεται από τον Κανονισμό και για τον εκτελούντα την επεξεργασία.

4. Τι θεωρείται προσωπικό δεδομένο; Τι είναι επεξεργασία;

«**Δεδομένα προσωπικού χαρακτήρα**»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

Προσωπικά δεδομένα είναι, ενδεικτικά:

- Το ονοματεπώνυμο
- Το ΑΦΜ
- Ο ΑΜΚΑ
- Κωδικοί Taxis
- Η διεύθυνση
- Το τηλέφωνο
- Ταυτότητα
- Τα οικονομικά δεδομένα
- Τα περιουσιακά στοιχεία

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

«**Επεξεργασία**»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

5. Βασικές Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

5.1 Τα δεδομένα προσωπικού χαρακτήρα:

α) Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»).

β) Συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς («περιορισμός του σκοπού»).

γ) Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»).

δ) Είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»).

ε) Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο Κανονισμός για τη

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»).
στ) Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

5.2 Η επεξεργασία είναι **σύννομη** μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:
α) Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.
β) Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.
γ) Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας.
δ) Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
ε) Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
στ) Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν, έναντι των συμφερόντων αυτών, υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Παράδειγμα:
Ερ. 1: Μπορεί η έκδοση ενός φορολογικού στοιχείου (π.χ. Τ.Π.Υ) από επιχείρηση μετά την έναρξη ισχύος του Κανονισμού, να τεκμαίρει την συναίνεση του υποκειμένου των δεδομένων για την επεξεργασία των δεδομένων του;

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

Απ: Η συναίνεση του υποκειμένου των δεδομένων αναβαθμίζεται από τον Κανονισμό ως προαπαιτούμενο για τη νομιμοποίηση κάθε επεξεργασίας. Καθίσταται σαφής και δεσμευτική. Δεν αρκεί η σιωπηρή και η τεκμαιρόμενη αποδοχή του υποκειμένου. Απαιτείται ευδιάκριτη, ρητή και ιδιαίτερη δήλωση μετά από εμπεριστατωμένη πληροφόρηση του υποκειμένου για το σκοπό και την έκταση της επεξεργασίας των δεδομένων του. Η σιωπή, τα προ-συμπληρωμένα τετραγωνίδια ή η αδράνεια του υποκειμένου δεν εκλαμβάνονται ως συγκατάθεση. Ως εκ τούτου, δεν μπορεί έμμεσα δια του Τ.Π.Υ. να τεκμαίρεται η συναίνεση του υποκειμένου.

Ερ.2: Πελάτης (φυσικό πρόσωπο) προβαίνει σε μία τηλεφωνική παραγγελία ενός προϊόντος για πρώτη φορά μετά την έναρξη ισχύος του Κανονισμού. Η επιχείρηση πρέπει να του αποστείλει έντυπο συγκατάθεσης για την επεξεργασία των προσωπικών του δεδομένων ή αρκεί η λήψη προφορικής συγκατάθεσης κατά την τηλεφωνική τους επικοινωνία;

Απ: Για να διασφαλίσει ότι έχει λάβει προσηκόντως τη συγκατάθεση του υποκειμένου, η επιχείρηση θα πρέπει να διαθέτει τουλάχιστον σύστημα ηχογραφημένης επικοινωνίας, στην οποία θα παρέχεται η ρητή και αδιαμφισβήτητη συγκατάθεση του υποκειμένου.

Ερ.3: Μπορεί μετά την 25.5.2018 μία επιχείρηση να αποστέλλει σε καταχωρημένους πελάτες της έντυπα επικοινωνίας (flyers) ή email με τα οποία θα τους ενημερώνει για μελλοντικές προσφορές, εκπτώσεις, εταιρικές εκδηλώσεις (εγκαίνια νέου καταστήματος) κλπ;

Απ.: Μετά την 25.5.2018 δεν μπορεί να χρησιμοποιούνται οι βάσεις δεδομένων που έχουν δημιουργηθεί στο πλαίσιο της συμβατικής υποχρέωσης ή της επαγγελματικής δραστηριότητας για άλλους λόγους, εκτός και αν τα υποκείμενα προηγουμένως ρητώς συναινέσουν ότι αποδέχονται να τους αποστέλλονται ενημερωτικά με τις συγκεκριμένες πληροφορίες.

6. Ποιοι είναι οι βασικότεροι ορισμοί του Κανονισμού;

- «**Υπεύθυνος επεξεργασίας**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

Με άλλα λόγια, κάθε Επιχείρηση είναι υπεύθυνος επεξεργασίας, αν επεξεργάζεται προσωπικά δεδομένα εργαζομένων της, μελών της, πελατών της, προμηθευτών της κ.λπ. (φυσικών προσώπων).

- «**Εκτελών την επεξεργασία**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Εκτελών την επεξεργασία μπορεί να είναι για παράδειγμα μία επιχείρηση που έχει αναλάβει για λογαριασμό σας και σας παρέχει υπηρεσίες λογιστηρίου ή τη μισθοδοσία του προσωπικού σας, υπηρεσίες στον τομέα της στοχευμένης διαφήμισης και εμπορικής προώθησης, υπηρεσίες επαγγελματικής υγείας κλπ. Μεταξύ του υπευθύνου και του εκτελούντος την επεξεργασία πρέπει να διατυπωθούν συμβατικές ρήτρες, δεσμευτικές για τα μέρη, που θα οριοθετούν την μεταξύ τους ευθύνη.

- **«Αποδέκτης»:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτο είτε όχι. Ωστόσο, **οι δημόσιες αρχές** που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους **δεν θεωρούνται ως αποδέκτες**.
- **«Τρίτος»:** οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.
- «**Παραβίαση δεδομένων προσωπικού χαρακτήρα**»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
- «**Υπεύθυνος Προστασίας δεδομένων**» - **Data Protection Officer (DPO)**: Πρόκειται για το φυσικό πρόσωπο που θα ενημερώνει τους χρήστες των οποίων τα δεδομένα επεξεργάζεται ο φορέας / επιχείρηση αλλά και θα είναι εκείνος ο οποίος έρχεται σε επικοινωνία με την Εποπτική Αρχή. Η ανάθεση

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

καθηκόντων υπευθύνου προστασίας είναι υποχρεωτική υπό συγκεκριμένες προϋποθέσεις.

7. Ποιες είναι οι βασικότερες απαιτήσεις του Κανονισμού από τις επιχειρήσεις;

- Να έχουν ενημερώσει και εκπαιδεύσει κατάλληλα το ανθρώπινο δυναμικό τους για τις νέες υποχρεώσεις που απορρέουν από τον Κανονισμό.
- Να έχουν τα κατάλληλα μέτρα ασφαλείας και τις αναγκαίες πολιτικές για την προστασία των πληροφοριών που επεξεργάζονται, διενεργώντας ελέγχους ασφαλείας ανά τακτά χρονικά διαστήματα.
- Να καθορίσουν το σκοπό επεξεργασίας προσωπικών δεδομένων. Είναι ο σκοπός σαφής; Γίνεται επεξεργασία μόνο στο πλαίσιο αυτού του σκοπού; Πώς έχουν ληφθεί τα δεδομένα; Είναι τα απολύτως απαραίτητα και αναγκαία για τον εν λόγω σκοπό; Πόσος χρόνος απαιτείται για την επεξεργασία των δεδομένων;
- Να καθορίσουν με σαφήνεια τους εκτελούντες την επεξεργασία των προσωπικών δεδομένων των υποκειμένων. Ποια πρόσωπα εξουσιοδοτούνται για την πρόσβαση; Έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας; Οι συνεργαζόμενες εταιρείες παρέχουν εγγυήσεις για τη συμμόρφωση με τον Κανονισμό;
- Να λάβουν ρητή συγκατάθεση των υποκειμένων για την επεξεργασία των δεδομένων τους. Είναι η συγκατάθεση ελεύθερη, συγκεκριμένη και ρητή, για σαφώς προσδιορισμένο σκοπό; Έχει προέλθει κατόπιν δήλωσης με σαφή θετική ενέργεια;
- Να καθορίσουν με σαφήνεια την περίοδο διατήρησης των προσωπικών δεδομένων των υποκειμένων. Πόσο ασφαλής είναι η τήρηση και περαιτέρω επεξεργασία των δεδομένων; Κρυπτογραφούνται; Ψευδωνυμοποιούνται;
- Να ενημερώσουν με σαφήνεια τα υποκείμενα για τους ακριβείς λόγους επεξεργασίας.
- Να προβούν σε αξιολόγηση υφιστάμενων συμβάσεων τρίτων παρόχων αλλά και καθορισμό πλαισίου για μελλοντικές συνεργασίες, σχετικά με την διαχείριση προσωπικών δεδομένων.
- Να μεταφέρουν δεδομένα μόνο σε περίπτωση σαφούς πλαισίου, ιδιαίτερα όταν πρόκειται για τρίτες χώρες.
- Να κάνουν αναλύσεις των επιπτώσεων που μπορούν να προκύψουν λόγω παραβίασης ιδιωτικότητας (Privacy Impact Assessment). Πρέπει να γίνεται

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

με συστηματικό τρόπο λαμβάνοντας υπόψη τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.

- Να σχεδιάζουν προϊόντα και υπηρεσίες λαμβάνοντας υπόψη την προστασία της ιδιωτικότητας (Προστασία δεδομένων εξ ορισμού, privacy by default: ο Κανονισμός επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητο για τον σκοπό της επεξεργασίας. Προστασία δεδομένων κατά το σχεδιασμό, privacy by design: Ο Κανονισμός επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων).
- Εκπόνηση και τήρηση Κωδίκων Δεοντολογίας. **Ενθαρρύνεται η εκπόνηση Κωδίκων ιδίως για πολύ μικρές, μικρές ή μεσαίες επιχειρήσεις.**
- Να ενημερώνουν τις αρμόδιες αρχές και τα υποκείμενα εντός 72 ωρών από τον εντοπισμό συμβάντος παραβίασης συστημάτων και απώλειας δεδομένων (data breach notification).
- Να έχουν ορίσει, όπου απαιτείται, υπεύθυνο για την προστασία των δεδομένων (Data Protection Officer).
- Να έχουν πλάνο αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων (Incident Response Plan).
- Να αποζημιώνουν τους πελάτες των οποίων απέτυχαν να προστατεύσουν τα δεδομένα τους.
- Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης, προστασίας δεδομένων, σφραγίδων και σημάτων.
- Ενθαρρύνεται η χρήση προηγμένων κρυπτογραφικών τεχνικών, μηχανισμών ασφαλείας και προστασίας δεδομένων, η ανωνυμοποίηση και ψευδωνυμοποίηση δεδομένων κατά την επεξεργασία.
  Παράδειγμα: εργαζόμενος μίας επιχείρησης που είναι εξουσιοδοτημένος για να έχει πρόσβαση σε προσωπικά δεδομένα πελατών/προμηθευτών της, έχει απομακρυσμένη πρόσβαση στα στοιχεία αυτά από προσωπικό Η/Υ, με τη συγκατάθεση της επιχείρησης. Διαθέτει μάλιστα usb stick. Τα στοιχεία αυτά πρέπει να είναι κρυπτογραφημένα, ώστε να αποφεύγεται ο κίνδυνος περαιτέρω αθέμιτης επεξεργασίας τους σε περίπτωση απώλειας ή κλοπής.

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680
Website: www.pcci.gr, E-Mail: evep@pcci.gr

8. Ποιες επιχειρήσεις/οργανισμοί πρέπει να ορίσουν υπεύθυνο Προστασίας Δεδομένων (DPO)[1];

Ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός σε ορισμένες περιπτώσεις που αναφέρονται στον Κανονισμό:

- Εάν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (ανεξάρτητα από το είδος/όγκο των δεδομένων που υφίστανται επεξεργασία).
- Εάν οι βασικές δραστηριότητες του υπευθύνου Επεξεργασίας ή του εκτελούντος την Επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα.
- Εάν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Σύμφωνα με τη δεύτερη περίπτωση, ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός, όταν οι *βασικές* δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε *μεγάλη κλίμακα.*

Ως βασικές δραστηριότητες μπορούν να θεωρηθούν οι καίριες πράξεις που είναι αναγκαίες για την επίτευξη των στόχων του υπευθύνου επεξεργασίας (δεν εμπίπτει στην έννοια των βασικών δραστηριοτήτων η επεξεργασία δεδομένων που γίνεται ως παρεπόμενη δραστηριότητα).

Στην έννοια της «μεγάλης κλίμακας» εμπίπτουν πράξεις επεξεργασίας μεγάλης κλίμακας που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο[2]. Για τον

[1] Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr

[2] Βλ. Κατευθυντήριες Γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων της Ομάδας Προστασίας των Προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29 σε www.dpa.gr

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

προσδιορισμό της έννοιας «μεγάλη κλίμακα» συνίσταται να λαμβάνονται υπόψη οι ακόλουθοι παράγοντες:

- Ο αριθμός των εμπλεκομένων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού,
- Ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υφίστανται επεξεργασία
- Η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων
- Η γεωγραφική έκταση της δραστηριότητας επεξεργασίας

Πάντως σύμφωνα με την ΑΠΔΠΧ κάθε οργανισμός/επιχείρηση μπορεί να ορίσει DPO. Ακόμη και στις περιπτώσεις που ο ορισμός DPO δεν είναι υποχρεωτικός, ενθαρρύνονται τέτοιου είδους εθελοντικές ενέργειες. Όταν ένας οργανισμός ορίζει DPO σε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι ίδιες απαιτήσεις ως εάν ο ορισμός να ήταν υποχρεωτικός.

8.1 Ποια είναι τα καθήκοντα του DPO;

Τα καθήκοντα του DPO είναι, ενδεικτικά, τα ακόλουθα:

- Να ενημερώνει και να συμβουλεύει την επιχείρηση / οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων.
- Να παρακολουθεί την εσωτερική συμμόρφωση με τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).
- Να παρέχει συμβουλές για την εκτίμηση αντικτύπου και να παρακολουθεί την υλοποίησή της.
- Να είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, πελάτες κ.λπ.).
- Να συνεργάζεται με την εποπτική αρχή.

8.2 Ποιες είναι οι υποχρεώσεις του εργοδότη ενός DPO;

Ο εργοδότης υποχρεούται να δημοσιεύσει τα στοιχεία επικοινωνίας του DPO και να τα ανακοινώσει στην εποπτική αρχή. Επίσης, οφείλει να διασφαλίζει ότι ο DPO:

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680
Website: www.pcci.gr, E-Mail: evep@pcci.gr

- Συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων (π.χ. παρουσία σε συσκέψεις ανώτερων και μεσαίων στελεχών της διοίκησης και κατά τη λήψη αποφάσεων, καταγραφή λόγων διαφωνίας με τις συμβουλές του, έγκαιρη διαβίβαση πληροφοριών για παροχή γνώμης, άμεση λήψη γνώμης σε περίπτωση περιστατικού παραβίασης).
- Έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας.
- Έχει στη διάθεσή του τους απαραίτητους πόρους για την εκπλήρωση των καθηκόντων του (π.χ. ενεργή στήριξη από τα ανώτερα διοικητικά στελέχη, οικονομικούς πόρους, υποδομές, συνεχή κατάρτιση).
- Εκπληρώνει τα καθήκοντά του με ανεξάρτητο τρόπο (δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του) και δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.
- Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του εργοδότη.
- Όταν ασκεί πρόσθετα καθήκοντα, αυτά να μην συνεπάγονται σύγκρουση συμφερόντων (π.χ. δεν μπορεί να κατέχει θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας, όπως θέσεις ανώτερης διοίκησης).
- Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.

Ερ.: Μία πολύ μικρή εμπορική επιχείρηση, η οποία διαθέτει μόνο δεδομένα προμηθευτών – συνεργατών, τερματικό POS και εκδίδει τιμολόγια (σε φυσικά και νομικά πρόσωπα), σε τι ενέργειες πρέπει να προβεί προκειμένου να είναι σύννομη με τον GDPR;
Απ.: Να ακολουθήσει τα βασικά βήματα (βλ. υπό 7) προετοιμασίας και συμμόρφωσης με τον Κανονισμό. Στα βήματα εμπλέκονται άμεσα η Διοίκηση της επιχείρησης σε συνεργασία με Νομικούς και Πληροφορικούς. Η προσέγγιση είναι πολυεπίπεδη και απαιτεί έγκαιρο εντοπισμό υποχρεώσεων και συστηματοποίηση των βημάτων ώστε να καταγραφούν οι βασικές ελλείψεις και να γίνει προσπάθεια εξεύρεσης τρόπου αντιμετώπισής τους.

9. Τι εννοεί ο Κανονισμός με το «δικαίωμα στη λήθη»;
Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr

χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένα από τα εξής: α) τα δεδομένα δεν είναι πλέον απαραίτητα, β) ανάκληση συγκατάθεσης, γ) το υποκείμενο αντιτίθεται στην επεξεργασία, δ) παράνομη επεξεργασία, ε) τα δεδομένα πρέπει να διαγραφούν βάσει νομικής υποχρέωσης, στ) έχουν συλλεχθεί κατά την παροχή υπηρεσίας σε ανηλίκους. Η διαγραφή δεδομένων παιδιών είναι υποχρεωτική, ακόμα και αν αλλάξει η βάση νομιμότητας ή εάν έχει εντωμεταξύ ενηλικιωθεί ο ανήλικος.

Περιορισμοί του δικαιώματος διόρθωσης και διαγραφής: στο πλαίσιο της ελευθερίας της έκφρασης, του δημοσίου συμφέροντος, της αρχειοθέτησης, της θεμελίωσης νομικών αξιώσεων.

Παράδειγμα 1: μία επιχείρηση τηρεί τα στοιχεία πελάτη (φυσικού προσώπου) σε αρχείο. Το υποκείμενο (πελάτης) ζητά να διαγραφεί από το αρχείο της επιχείρησης αναφέροντας ότι δεν επιθυμεί άλλη συνεργασία με την επιχείρηση. Η επιχείρηση εξετάζει το αίτημά του, ανατρέχοντας στο αρχείο της όπου υπάρχουν τα προσωπικά δεδομένα του. Διαπιστώνεται ότι ο συγκεκριμένος πελάτης έχει ανεξόφλητη οφειλή ή υπάρχει δικαστική διένεξη. Η επιχείρηση οφείλει να ενημερώσει το υποκείμενο των δεδομένων (πελάτη της) ότι δεν μπορεί να τον διαγράψει γιατί έχει νόμιμο δικαίωμα να τηρεί τα στοιχεία του για όσο χρόνο υφίσταται η αξίωση ή η διένεξη, αλλά και στο πλαίσιο της αρχειοθέτησης.

Παράδειγμα 2: Ένας φορέας οφείλει βάσει της κείμενης νομοθεσίας να αναρτήσει τα στοιχεία προμηθευτή του (επωνυμία, ΑΦΜ κλπ) και τιμολογίου (ποσό, αιτία) στη ΔΙΑΥΓΕΙΑ. Ο προμηθευτής ζητά από τον υπεύθυνο επεξεργασίας (φορέας) να μην αναρτηθούν στο ΔΙΑΥΓΕΙΑ τα προσωπικά του δεδομένα. Ο φορέας οφείλει να ενημερώσει τον προμηθευτή του ότι δεν μπορεί να προβεί στην ενέργεια αυτή, καθώς η ανάρτηση αποτελεί συμμόρφωση με το ισχύον κανονιστικό πλαίσιο.

Γ. Κασιμάτη 1 πλ. Οδησσού, 18531 Πειραιάς, Τηλ: 210 4177241-5, Φαξ: 210 4178680

Website: www.pcci.gr, E-Mail: evep@pcci.gr