Εφαρμογή του νέου Ευρωπαϊκού Κανονισμού 679/2016 για την προστασία προσωπικών δεδομένων

Τμήμα Φορολογίας

Ειρήνη Λοϊζίδου Νικολαΐδου
Επίτροπος Προστασίας
Δεδομένων Προσωπικού Χαρακτήρα

5 Ιουνίου 2018

Αρχές νόμιμης επεξεργασίας

- Εισαγωγή της **Αρχής της Λογοδοσίας:** ο οργανισμός, θα πρέπει ανά πάσα στιγμή, να καθορίζει και να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα **για να αποδεικνύει συμμόρφωση** με τον Κανονισμό

- Όμοιες αρχές με την Οδηγία:

- Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας
- Αρχή του περιορισμού του σκοπού
- Αρχή της ελαχιστοποίησης των δεδομένων
- Αρχή του περιορισμού της περιόδου αποθήκευσης
- Αρχή της ακεραιότητας και εμπιστευτικότητας

Πότε είναι νόμιμη η επεξεργασία απλών προσωπικών δεδομένων

- Έχει δοθεί η συναίνεση του ατόμου
- Για εκτέλεση σύμβασης
- Για έννομη υποχρέωση του οργανισμού
- Για διαφύλαξη ζωτικού συμφέροντος του ατόμου
- Για δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας
- Για το έννομο συμφέρον του οργανισμού ή του τρίτου

Πότε είναι νόμιμη η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων

Κατά κανόνα απαγορεύεται η επεξεργασία τους

- Επιτρέπεται όταν:

(α) υπάρχει συγκατάθεση

(β) στον τομέα του εργατικού δικαίου, δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας

(γ) για ζωτικό συμφέρον

(δ) για δραστηριότητες ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο – αφορά τα μέλη ή τα πρώην μέλη του ή πρόσωπα που έχουν τακτική επικοινωνία μαζί του και τα δεδομένα δεν κοινοποιούνται σε τρίτους

(ε) για δεδομένα που έχουν δημοσιοποιηθεί από το άτομο

(στ) για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων

(ζ) για λόγους ουσιαστικού δημόσιου συμφέροντος

(η) για προληπτική ή επαγγελματική ιατρική, εκτίμηση ικανότητας εργασίας, ιατρική διάγνωση, υγειονομική ή κοινωνική περίθαλψη ή θεραπεία ή διαχείριση υγειονομικών και κοινωνικών συστημάτων δυνάμει νόμου ή σύμβασης με επαγγελματία στον τομέα της υγείας που τηρεί το επαγγελματικό απόρρητο

(θ) για λόγους δημόσιου συμφέροντος

(ι) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

Πότε είναι νόμιμη η επεξεργασία προσωπικών δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα

- Για επαγγέλματα που το επιβάλλει ο νόμος

  π.χ Τράπεζα, Αστυνομία
- Ο εργοδότης μπορεί να ζητήσει από τον υπάλληλο Πιστοποιητικό Λευκού Ποινικού Μητρώου ακόμα και όταν δεν προβλέπεται από νόμο, δεδομένου ότι έχει συνάφεια με το σκοπό που επιδιώκει
- Ο εργοδότης δεν μπορεί να ζητήσει Πιστοποιητικό Λευκού Ποινικού Μητρώου χωρίς τη συγκατάθεση του ατόμου, η οποία πρέπει να δίνεται ελεύθερα
- Αρχείο προηγούμενων καταδικών τηρείται μόνο από την Αστυνομία

Ενδυνάμωση υφιστάμενων δικαιωμάτων των πολιτών και εισαγωγή νέων

- Δικαίωμα ενημέρωσης
- Δικαίωμα πρόσβασης
- Δικαίωμα διόρθωσης
- Δικαίωμα διαγραφής «Δικαίωμα στη λήθη»
- Δικαίωμα περιορισμού
- Δικαίωμα στη φορητότητα των δεδομένων
- Δικαίωμα εναντίωσης
- Δικαίωμα αντίρρησης σε αυτοματοποιημένη απόφαση περιλαμβανομένης της κατάρτισης προφίλ

Αυστηρότατες Υποχρεώσεις Υπεύθυνων Επεξεργασίας

1. Φέρει το βάρος της απόδειξης όσον αφορά στην παροχή συγκατάθεσης (Άρθρο 7)
2. Λήψη συγκατάθεσης για ανήλικους κάτω των 16 σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών (Άρθρο 8)
3. Υποχρέωση κατασκευαστών στο στάδιο του σχεδιασμού και εξ΄ορισμού (privacy by default and by design) (Άρθρο 25)
4. Υποχρέωση καθορισμού ευθυνών μέσω συμφωνίας όταν υπάρχουν από κοινού υπεύθυνοι επεξεργασίας (Άρθρο 26)
5. Υποχρέωση εκπροσώπησης υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση (Άρθρο 27)
6. Επιλογή εκτελούντων την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων (Άρθρο 28)

7. Τήρηση αρχείων των δραστηριοτήτων επεξεργασίας (Άρθρο 30)
8. Υποχρέωση τήρησης της ασφάλειας της επεξεργασίας (Άρθρο 32)
9. Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας (Άρθρο 33)
10. Υποχρέωση ανακοίνωσης παραβιάσεων ασφάλειας (Άρθρο 34)
11. Διενέργεια εκτίμησης αντικτύπου (Άρθρο 35): στην ιστοσελίδα του Γραφείου μου αναρτήθηκε πληροφοριακό υλικό και Κατάλογος με τα είδη των πράξεων επεξεργασίας για τα οποία απαιτείται η διενέργεια εκτίμησης αντικτύπου
12. Ορισμός Υπεύθυνου Προστασίας Δεδομένων (Άρθρο 37)
13. Τήρηση κώδικα δεοντολογίας (Άρθρα 40 – 41)
14. Πιστοποίηση (Άρθρα 42-43)
15. Διαβιβάσεις σε τρίτες χώρες (Άρθρα 46 – 49)

Εποπτική αρχή

- Ανεξάρτητη, χωρίς εξωτερικές επιρροές, δεν ζητεί ούτε λαμβάνει οδηγίες από κανέναν
- Τα μέλη της διορίζονται με διαφανή διαδικασία και απέχουν από κάθε πράξη ασυμβίβαστη προς τα καθήκοντά τους
- Διαθέτει τους απαραίτητους ανθρώπινους, τεχνικούς και οικονομικούς πόρους και τις αναγκαίες εγκαταστάσεις και υποδομές
- Διαθέτει δικούς της υπαλλήλους
- Υπόκειται σε οικονομικό έλεγχο ο οποίος δεν επηρεάζει την ανεξαρτησία της και διαθέτει δικό της ετήσιο προϋπολογισμό
- Τα μέλη και οι υπάλληλοι δεσμεύονται από το επαγγελματικό απόρρητο κατά τη διάρκεια της θητείας και μετά το πέρας αυτής
- Δια νόμου προβλέπεται η σύσταση της εποπτικής αρχής, τα προσόντα, η διάρκεια θητείας των μελών *(δεν πρέπει να είναι μικρότερη από 6 χρόνια)*

Ρόλος του Γραφείου της Επιτρόπου μετά την εφαρμογή του νέου Κανονισμού

- Αυξημένη εποπτεία των ιδιωτικών εταιρειών, δημόσιων αρχών και νομικών προσώπων δημοσίου δικαίου (λόγω των αυξημένων υποχρεώσεων τους)
- Αυξημένοι διοικητικοί έλεγχοι
- Διερεύνηση περισσότερων καταγγελιών/παραπόνων σε περίπτωση μη τήρησης των υποχρεώσεων των υπεύθυνων και εκτελούντων και/ή μη ικανοποίησης των δικαιωμάτων των πολιτών
- Έλεγχοι των αρχείων δραστηριοτήτων των υπεύθυνων επεξεργασίας
- Διαβούλευση με το Γραφείο μου, όταν η εκτίμηση αντικτύπου υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο και ο οργανισμός δεν είναι σε θέση να λάβει μέτρα μετριασμού του κινδύνου
- Έλεγχος και υποδείξεις ενδεδειγμένων ενεργειών σε περιπτώσεις παραβίασης προσωπικών δεδομένων

- Έγκριση πιστοποιητικών και κριτηρίων πιστοποίησης
- Επανεξέταση των πιστοποιήσεων
- Παροχή διαπίστευσης σε φορείς πιστοποίησης
- Έκδοση γνωμών για σχέδια κωδίκων δεοντολογίας και έγκριση τους
- Έγκριση δεσμευτικών εταιρικών κανόνων
- Έγκριση τυποποιημένων ρητρών
- Επιβολή αυξημένων διοικητικών προστίμων
- Συνεργασία με άλλες ΑΠΔΠΧ και το Συμβούλιο Προστασίας Δεδομένων

Τι καταργείται!

- Γνωστοποιήσεις Σύστασης και Λειτουργίας Αρχείου/Έναρξης Επεξεργασίας – αντικαθίστανται με την τήρηση Αρχείου Δραστηριοτήτων της επεξεργασίας
- Άδεια για επεξεργασία ευαίσθητων δεδομένων *(νυν ειδικών κατηγοριών προσωπικών δεδομένων)* στον τομέα του εργατικού δικαίου
- Άδεια για διασύνδεση αρχείων
- Έκδοση Απόφασης από την Επίτροπο για άρση της υποχρέωσης ενημέρωσης των υποκειμένων των δεδομένων
- Καταβολή τέλους των €17 από τα υποκείμενα για άσκηση του δικαιώματος πρόσβασης και αντίρρησης

Τι αλλάζει!

- Άδειες διαβίβασης σε τρίτες χώρες – όμως η ΑΠΔΠΧ εγκρίνει τη νομική βάση της διαβίβασης π.χ. τυποποιημένες συμβατικές ρήτρες, δεσμευτικούς εταιρικούς κανόνες, κώδικα δεοντολογίας, μηχανισμό πιστοποίησης

- Με εφαρμοστικές διατάξεις, η ΑΠΔΠΧ μπορεί να περιορίσει την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων και δεδομένων που αφορούν στην υγεία

Άλλα σημαντικά θέματα και ορθές πρακτικές

Διασυνδέσεις αρχείων Τμήματος Φορολογίας με αρχεία άλλων δημόσιων υπηρεσιών

- Όλες οι υφιστάμενες άδειες διασύνδεσης έχουν ισχύ μέχρι τις 24/05/2018
- Στο νομοσχέδιο περιλήφθηκε πρόνοια για διασύνδεση αρχείων, ανάλογη με το άρθρο 8 του υφιστάμενου Νόμου
- Πολλές διασυνδέσεις προβλέπουν την ανταλλαγή πληροφοριών με ηλεκτρονικό ταχυδρομείο ή με κρυπτογραφημένα CDs
- Αυτοί οι τρόποι ελλοχεύουν κινδύνους και σταδιακά θα πρέπει να εξευρεθούν άλλοι, ασφαλείς τρόποι
- Όπου είναι δυνατό, οι διασυνδέσεις θα πρέπει να γίνονται μέσω της ΚΑΠ
- Αυτό συνεπάγεται μεγάλο φόρτο εργασίας για το ΤΥΠ
- Το ΤΥΠ έστειλε Εγκύκλιο προς όλες τις ΔΥ, την οποία ετοίμασε σε συνεργασία με το Γραφείο μου
- **Η κάθε ΔΥ πρέπει να ενημερώσει το ΤΥΠ για υφιστάμενες και μελλοντικές ανάγκες Διασύνδεσης, για έγκαιρο προγραμματισμό**

Ηχογράφηση τηλεφωνικών συνδιαλέξεων

Ισχύουν οι διατάξεις για το Απόρρητο των επικοινωνιών (άρθρο 99) του Νόμου 112(I)/2004

Παρέμβαση στις επικοινωνίες επιτρεπτή αν:

- εξασφαλίζεται η συγκατάθεση των επικοινωνούντων ή
- προβλέπεται από νομοθεσία (πρωτογενή /δευτερογενή) και με άδεια του Δικαστηρίου ή
- αν πρόκειται για νόμιμη επαγγελματική πρακτική επιτρέπεται η καταγραφή συνδιαλέξεων με σκοπό την εξασφάλιση αποδεικτικών στοιχείων κάποιας εμπορικής συναλλαγής και/ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα

Ισχύουν και οι διατάξεις του Νόμου 138(Ι)/2001, δυνάμει των οποίων:

- προτού αρχίσει η τηλεφωνική συνομιλία, υπάρχει προειδοποιητική σήμανση ότι η συνομιλία ηχογραφείται,
- στο περιεχόμενο της προειδοποιητικής σήμανσης, να αναφέρονται τα ακόλουθα:
  - η ταυτότητα του υπεύθυνου επεξεργασίας,
  - ο σκοπός της ηχογράφησης,
  - εάν η ηχογραφημένη συνομιλία θα κοινοποιηθεί σε τρίτους και ότι
  - το φυσικό πρόσωπο μπορεί να έχει πρόσβαση στο περιεχόμενο της ηχογραφημένης τηλεφωνικής συνομιλίας

Εγκατάσταση και Λειτουργία Κ.Κ.Β.Π.

- Κατά κανόνα απαγορεύεται ενόψει της απουσίας νομοθετικής ρύθμισης
- Επιτρέπεται σε δημόσιους χώρους όταν το έννομο συμφέρον του υπεύθυνου επεξεργασίας υπερέχει των δικαιωμάτων των πολιτών *(π.χ. για σκοπούς ασφαλείας, προστασίας του χώρου από διαρρήξεις και κλοπές)*
- **Επιτρέπεται η εγκατάσταση και λειτουργία κάμερας πάνω από το μηχάνημα κάρτας**
- **Σε κάθε περίπτωση, οι υπάλληλοι θα πρέπει να ενημερώνονται**
- Τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας μέσω Κ.Κ.Β.Π. πρέπει να χρησιμοποιούνται μόνο για τους σκοπούς που έχουν εγκατασταθεί και όχι γι' άλλους σκοπούς π.χ. για έλεγχο της αποδοτικότητας και προσωπικής συμπεριφοράς των υπαλλήλων

➢ Επιτρέπεται η εγκατάσταση και λειτουργία κάμερας:

- εισόδους / εξόδους
- χώρους φύλαξης χρημάτων (π.χ. ταμεία/ θυρίδες / χρηματοκιβώτια)
- χώρους στάθμευσης
- χώρους εισόδου/εξόδου των ανελκυστήρων στους ορόφους και των κλιμακοστασίων

➢ **Δεν επιτρέπεται** η εγκατάσταση ΚΚΒΠ σε:

(Σχετική είναι και η Απόφαση της Ελληνικής Αρχής 192/2012)

- χώρους εστίασης π.χ. εστιατόρια, μπαρ, καφετέριες
- χώρο υποδοχής / αναμονής
- διαδρόμους
- τουαλέτες
- χώροι όπου πραγματοποιούνται δραστηριότητες αναψυχής (όπως πισίνες, γυμναστήρια, χώροι άθλησης, αποδυτήρια κλπ.)
- παιδότοπους
- μέσα στο ασανσέρ
- εξωτερικές κάμερες που λαμβάνουν εικόνες από πεζοδρόμια, δρόμους, γειτονικά καταστήματα
- σε γραφεία όπου απασχολείται ένας ή μικρός αριθμός υπαλλήλων

(Υπάρχουν σχετικές Αποφάσεις Επιτρόπου για απεγκατάσταση των καμερών ή λειτουργία τους κατά τις μη εργάσιμες ώρες)

- Απαραίτητη η σήμανση με ευδιάκριτα γράμματα για ενημέρωση των πολιτών/υπαλλήλων **πριν** από την είσοδό τους στο κτίριο

- Σε περίπτωση που υπάρχει ΚΚΒΠ σε κάθε όροφο, **η ενημέρωση θα πρέπει να γίνεται σε κάθε όροφο ξεχωριστά**

- Δεν επιτρέπεται η μυστική παρακολούθηση

Ορθή τηλεξυπηρέτηση κοινού

Δεν πρέπει να δίνονται δεδομένα μέσω τηλεφώνου αφού δεν επιβεβαιώνεται ότι τα δεδομένα ανακοινώνονται στα άτομα στα οποία αναφέρονται τα δεδομένα

Έλεγχος της ώρας προσέλευσης/αποχώρησης των υπαλλήλων από την εργασία μέσω συστήματος δακτυλικών αποτυπωμάτων

- Δεν επιτρέπεται εκτός από ορισμένες εξαιρετικές περιπτώσεις που αυτό επιβάλλεται από ιδιαίτερες απαιτήσεις ασφαλείας των χώρων εργασίας και εφόσον δεν υπάρχει άλλο μέσο για την επίτευξη του σκοπού αυτού *(π.χ. αμυντικές εγκαταστάσεις, εργαστήρια υψηλού κινδύνου)*

- Ο υπεύθυνος επεξεργασίας θα πρέπει να σταθμίζει τους κινδύνους, την έκταση των κινδύνων αυτών και τις υπάρχουσες εναλλακτικές δυνατότητες αντιμετώπισης των κινδύνων και από την άλλη, τις προσβολές της προσωπικότητας και της ιδιωτικότητας του ατόμου από τη χρήση τέτοιων μεθόδων

Ευχαριστώ για την προσοχή σας!

ΕΡΩΤΗΣΕΙΣ

Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Ιάσονος 1, 1082 Λευκωσία
Τ.Θ. 23378, 1682 Λευκωσία

Τηλ: 22818456, Φαξ: 22304565
E-mail: commissioner@dataprotection.gov.cy

www.dataprotection.gov.cy