Εκπαίδευση σχετικά με τον Κανονισμό (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικό Κανονισμό για την Προστασία Δεδομένων)» -TRAIN_GR_CY

Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

27 – 28 Μαρτίου 2019

Περιεχόμενο – 2η Μέρα

- Επιτήρηση στο χώρο εργασίας και χρήση βιομετρικών δεδομένων
- Συγκατάθεση
- Διαβίβαση δεδομένων σε τρίτες χώρες
- Δράσεις της Επιτρόπου και διοικητικοί έλεγχοι

2

Μέρος Ι
Επιτήρηση στο χώρο εργασίας και χρήση βιομετρικών συστημάτων

3

Η επιτήρηση στον χώρο εργασίας: η νέα πρόκληση στην κοινωνία της πληροφορίας

Οι εξελίξεις της τεχνολογίας και η γενίκευση της χρήσης του διαδικτύου στο χώρο εργασίας αυξάνουν τους κινδύνους παραβίασης της ιδιωτικής ζωής των εργαζομένων.

Τα εργαλεία ηλεκτρονικής παρακολούθησης προσφέρουν την δυνατότητα να χρησιμοποιούνται με τρόπο που να παραβιάζει τα θεμελιώδη δικαιώματα και ελευθερίες των εργαζομένων.

4

Διεθνές και ενωσιακό νομικό πλαίσιο

- Κανονισμός (ΕΕ) 2016/679
- Ευρωπαϊκή Σύμβασης των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ) - άρθρο 8
- Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης – άρθρα 7 και 8
- Γνώμη 2/2017 της Ομάδας Εργασίας του Άρθρου 29, σχετικά με την επεξεργασία δεδομένων στην εργασία
- Σύσταση CM/Rec(2015)5 του Συμβουλίου της Ευρώπης αναφορικά με την επεξεργασία δεδομένων στο πλαίσιο της εργασίας

5

Νομολογία ΕΔΑΔ – Niemietz κατά Γερμανίας

- *Στην υπόθεση Niemietz κατά Γερμανίας, το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων αποφάσισε ότι « ο σεβασμός της ιδιωτικής ζωής πρέπει να περιλαμβάνει, ως ένα βαθμό, το δικαίωμα δημιουργίας και ανάπτυξης σχέσεων με άλλους ανθρώπους. Επιπλέον, δεν φαίνεται να υπάρχει λόγος αρχής να θεωρείται ότι αυτή η κατανόηση της έννοιας της «ιδιωτικής ζωής» εξαιρεί τις δραστηριότητες επαγγελματικού χαρακτήρα, δεδομένου ότι, σε τελευταία ανάλυση,* ***οι περισσότεροι άνθρωποι στο τόπο εργασίας τους έχουν μια σημαντική, αν όχι τη μεγαλύτερη, ευκαιρία ανάπτυξης σχέσεων με τον εξωτερικό κόσμο.*** *Η άποψη αυτή υποστηρίζεται από το γεγονός ότι δεν είναι πάντοτε δυνατό να γίνεται σαφής διάκριση όσον αφορά στο ποιες από τις δραστηριότητες ενός ατόμου αποτελούν μέρος της επαγγελματικής ή της επιχειρηματικής ζωής του και ποιες όχι».*

6

Νομολογία ΕΔΑΔ – Halford εν. Ηνωμένου Βασιλείου

- Κατά την άποψη του Δικαστηρίου *«είναι σαφές από την νομολογία του ότι τα τηλεφωνήματα που γίνονται από εγκαταστάσεις επιχειρήσεων καθώς και από τον τόπο κατοικίας μπορούν να καλύπτονται από τις έννοιες της «ιδιωτικής ζωής» και της «αλληλογραφίας» υπό την έννοια του άρθρου 8 παράγραφος 1.*

- *Δεν υπάρχουν ενδείξεις ότι είχε δοθεί καμία προειδοποίηση στην κ. Halford ως χρήστη του εσωτερικού συστήματος τηλεπικοινωνιών ότι οι κλήσεις που γίνονται σε αυτό το σύστημα μπορούσαν να γίνουν αντικείμενο υποκλοπής. Το Δικαστήριο θεωρεί ότι η κ. Halford θα μπορούσε λογικά να περιμένει ότι ισχύει η προστασία της ιδιωτικής ζωής και για τις κλήσεις αυτές…».*

7

Τρόποι παρακολούθησης

- Παρακολούθηση της χρήσης των ΤΠΕ*: τηλέφωνο, περιήγηση στο διαδίκτυο, ηλεκτρονική αλληλογραφία, άμεση ανταλλαγή μηνυμάτων, VoIP κ.λπ.
- Βιντεο-παρακολούθηση
- Παρακολούθηση της χρήσης των οχημάτων με GPS
- Παρακολούθηση της παρουσίας και καταγραφή του χρόνου εργασίας
- Καταγραφή δεδομένων συμβάντων

*ΤΠΕ = τεχνολογίες πληροφοριών και επικοινωνίας

8

Αρχές που διέπουν την επεξεργασία/ επιτήρηση των εργαζομένων

- Οι εργοδότες πρέπει να έχουν πάντα υπόψη τις θεμελιώδεις **αρχές προστασίας** των δεδομένων (ελαχιστοποίηση, περιορισμός του σκοπού κλπ), ανεξάρτητα από την τεχνολογία που χρησιμοποιούν
- Το περιεχόμενο των ηλεκτρονικών επικοινωνιών που πραγματοποιούνται σε επαγγελματικές εγκαταστάσεις απολαμβάνει την ίδια προστασία ως προς τα **θεμελιώδη δικαιώματα** όπως και οι αναλογικές επικοινωνίες
- Η συγκατάθεση είναι εξαιρετικά απίθανο να συνιστά νομική βάση για την επεξεργασία δεδομένων στην εργασία, εκτός εάν οι εργαζόμενοι μπορούν να **αρνηθούν** την επεξεργασία **χωρίς αρνητικές συνέπειες**
- Μπορεί να γίνει επίκληση της εκτέλεσης σύμβασης και των εννόμων συμφερόντων, υπό τον όρο ότι η επεξεργασία είναι αυστηρά απαραίτητη για **νόμιμο σκοπό** και είναι σύμφωνη με τις **αρχές της αναλογικότητας και της επικουρικότητας**
- Οι εργαζόμενοι θα πρέπει να λαμβάνουν **αποτελεσματική ενημέρωση** για την παρακολούθηση που πραγματοποιείται και
- Κάθε διαβίβαση δεδομένων των εργαζομένων σε τρίτες χώρες θα πρέπει να πραγματοποιείται μόνο εφόσον διασφαλίζεται **κατάλληλο επίπεδο προστασίας**.

9

Παρακολούθηση της χρήσης των ΤΠΕ: τηλέφωνο, περιήγηση στο διαδίκτυο, ηλεκτρονική αλληλογραφία, άμεση ανταλλαγή μηνυμάτων, VoIP κ.λπ.)

Οι τεχνολογικές εξελίξεις δίνουν τη δυνατότητα για νέους τρόπους παρακολούθησης, που είναι κατά πάσα πιθανότητα πιο παρεμβατικοί και πιο εκτεταμένοι, όπως:

- Εργαλεία πρόληψης απώλειας δεδομένων (DLP), που παρακολουθούν τις εξερχόμενες επικοινωνίες με σκοπό τον εντοπισμό ενδεχόμενων παραβιάσεων δεδομένων
- Τείχη προστασίας νέας γενιάς (NGFW) και συστήματα ενιαίας διαχείρισης απειλών (UTM), που μπορούν να παράσχουν μεγάλο εύρος τεχνολογιών παρακολούθησης, στην οποία περιλαμβάνεται η παρακολούθηση ασφάλειας επιπέδου μεταφοράς (TLS), το φιλτράρισμα ιστοτόπων, η παραγωγή αναφορών εντός της συσκευής (on-appliance reporting) και οι πληροφορίες ταυτότητας του χρήστη
- Εφαρμογές και μέτρα ασφαλείας, που περιλαμβάνουν την καταγραφή της πρόσβασης του εργαζόμενου στα συστήματα του εργοδότη
- Τεχνολογία ηλεκτρονικής διερεύνησης στοιχείων, δηλαδή η διερεύνηση ηλεκτρονικών δεδομένων με σκοπό τη χρήση τους ως αποδεικτικών στοιχείων
- Παρακολούθηση της χρήσης εφαρμογών και συσκευών μέσω αφανούς λογισμικού

10

Αρχές που διέπουν τη παρακολούθηση των ΤΠΕ

- Οι εργοδότες πρέπει να εξετάζουν την **αναλογικότητα των μέτρων** που εφαρμόζουν, και κατά πόσον μπορούν να αναληφθούν περαιτέρω δράσεις για τον μετριασμό ή τη μείωση της κλίμακας και των επιπτώσεων της επεξεργασίας δεδομένων.
- Ως παράδειγμα ορθής πρακτικής είναι η **διενέργεια ΕΑ** πριν από τη χρήση οποιασδήποτε τεχνολογίας παρακολούθησης.
- Οι εργοδότες πρέπει να εφαρμόζουν **πολιτικές απορρήτου**, και να γνωστοποιούν πολιτικές αποδεκτής χρήσης, οι οποίες θα περιγράφουν την επιτρεπόμενη χρήση των δικτύων και του εξοπλισμού της εταιρείας και θα **περιγράφουν λεπτομερώς** την πραγματοποιούμενη επεξεργασία.
- Θα πρέπει να διασφαλίζεται ότι οι εργαζόμενοι μπορούν να ορίσουν συγκεκριμένα **ιδιωτικά τμήματα** στα οποία ο εργοδότης δεν μπορεί να έχει πρόσβαση παρά μόνο υπό εξαιρετικές περιστάσεις π.χ. τα ημερολόγια.
- Ορισμένες φορές δεν μπορεί να λαμβάνει χώρα κανενός είδους παρακολούθηση. Για παράδειγμα, αν υπάρχει η δυνατότητα **αποκλεισμού ιστοτόπου** αντί της συνεχούς παρακολούθησης όλων των επικοινωνιών, θα πρέπει να επιλέγεται ο αποκλεισμός ώστε να επιτυγχάνεται η συμμόρφωση με την απαίτηση ελαχιστοποίησης των δεδομένων.
- Θα πρέπει να δίνεται πολύ μεγαλύτερη **βαρύτητα στην πρόληψη** από ότι στον εντοπισμό – τα συμφέροντα του εργοδότη εξυπηρετούνται καλύτερα με την πρόληψη της κατάχρησης του διαδικτύου με τεχνικά μέσα από ότι με τη δαπάνη πόρων για τον εντοπισμό της κατάχρησης.

11

Περίπτωση μελέτης

Παρακολούθηση ηλεκτρονικών επικοινωνιών υπαλλήλου στον χώρο εργασίας

Ιστορικό της υπόθεσης

- Ο Χ εργαζόταν ως πωλητής τροφίμων στην εταιρεία ΑΒ από το 2015. Για την επικοινωνία με τους πελάτες χρησιμοποιούσε το Messenger από τον υπολογιστή της εταιρείας. Ο εσωτερικός κανονισμός της εταιρείας απαγόρευε τη χρήση του εξοπλισμού της εταιρείας για προσωπικούς σκοπούς.
- Τον Ιούλιο του 2018 ενημερώθηκε ότι ο εργοδότης του παρακολουθούσε το περιεχόμενο των ηλεκτρονικών επικοινωνιών του και διαπίστωσε ότι χρησιμοποίησε το Messenger για προσωπικούς σκοπούς. Του παρουσίασε εκτυπωμένο το περιεχόμενο δέκα μηνυμάτων που απέστειλε στην σύζυγο και στον αδελφό του. Ο Χ απολύθηκε από την εργασία του.

12

Ερώτημα

- Έχει δικαίωμα πρόσβασης ο εργοδότης στο περιεχόμενο των προσωπικών μηνυμάτων του υπαλλήλου;

13

Νομικό πλαίσιο

- Οι υπεύθυνοι επεξεργασίας πρέπει να διασφαλίζουν μια δίκαιη εξισορρόπηση μεταξύ των έννομων συμφερόντων τους και του δικαιώματος των υπαλλήλων στην προστασία της ιδιωτικής τους ζωής (άρθρο 15(3) του ΓΚΠΔ).
- Οι εσωτερικοί κανονισμοί της εταιρείας για την χρήση του διαδικτύου δεν μπορούν να εκμηδενίζουν την ιδιωτική και κοινωνική ζωή στο χώρο εργασίας (αιτιολογική σκέψη 47 του ΓΚΠΔ).
- Ο εργοδότης έχει δικαίωμα να ελέγχει την χρήση του διαδικτύου από τους υπαλλήλους δεν μπορεί όμως να έχει πρόσβαση στο περιεχόμενο των προσωπικών μηνυμάτων, ούτε να εκτυπώσει και να κοινοποιήσει το περιεχόμενο τους (Οδηγία Επιτρόπου για τις εργασιακές σχέσεις).
- Ο Χ γνώριζε ότι ο εσωτερικός κανονισμός της εταιρείας απαγόρευε τη χρήση του εξοπλισμού της εταιρείας για προσωπικούς σκοπούς, δεν είχε όμως ενημερωθεί ότι παρακολουθήτο το περιεχόμενο των ηλεκτρονικών επικοινωνιών (άρθρο 13 του ΓΚΠΔ).

14

Κλειστά κυκλώματα βιντεο-παρακολούθησης σε εργασιακούς χώρους – Γνώμη 2/2018 της Επιτρόπου

- Η παρακολούθηση των εργαζομένων στο χώρο εργασίας επιτρέπεται μόνο όταν ο εργοδότης είναι σε θέση να δικαιολογήσει τη **νομιμότητα και την αναγκαιότητα** του της παρακολούθησης και όταν δεν υπάρχει άλλος **λιγότερο παρεμβατικός τρόπος** για την πραγματοποίηση των σκοπών που επιδιώκει.
- Για παράδειγμα, η χρήση του ΚΚΒΠ θα μπορούσε να δικαιολογηθεί σε ειδικές εξαιρετικές περιπτώσεις, όπου αυτό **δικαιολογείται από τη φύση και τις συνθήκες εργασίας** και είναι απαραίτητο για την προστασία της υγείας και της ασφάλειας των εργαζομένων ή την προστασία κρίσιμων χώρων εργασίας (π.χ. στρατιωτικά εργοστάσια, τράπεζες, εγκαταστάσεις υψηλού κινδύνου).

15

- Σε έναν τυπικό χώρο γραφείων επιχείρησης, η βιντεοεπιτήρηση πρέπει να **περιορίζεται σε χώρους** εισόδου και εξόδου, έξω από τους ανελκυστήρες, από τα κλιμακοστάσια, σε χώρο στάθμευσης, σε ταμεία ή χώρους με χρηματοκιβώτια, ηλεκτρομηχανολογικό εξοπλισμό κλπ.
- Οι κάμερες πρέπει να **εστιάζουν στο αγαθό που προστατεύουν** κι όχι στους χώρους των εργαζομένων και στα πρόσωπά τους.
- **Απαγορεύεται** η καταγραφή εργαζομένων στα γραφεία τους, αίθουσες συνεδριάσεων, διαδρόμους, κουζίνα, έξω από αποχωρητήρια, αποδυτήρια.
- Τα δεδομένα που συλλέγονται μέσω συστήματος βιντεοεπιτήρησης **δεν επιτρέπεται** να χρησιμοποιηθούν ως αποκλειστικά κριτήρια για την αξιολόγηση της συμπεριφοράς και της αποδοτικότητας των εργαζομένων.

16

Σχετικές αποφάσεις ΕΠΔΠΧ

- 20/9/2010 - Απόφαση για απεγκατάσταση και λειτουργία Κλειστού Κυκλώματος Βιντεο-παρακολούθησης (ΚΚΒΠ) σε γραφεία υπαλλήλων εταιρείας για σκοπούς προστασίας της εταιρείας
- 10/2/2011 – Απόφαση για απεγκατάσταση Καμερών (ΚΚΒΠ) σε γραφεία Τράπεζας
- 28/11/2011 – Απόφαση για απεγκατάσταση Καμερών (ΚΚΒΠ) στη κουζίνα, σε γραφεία και στην υποδοχή ξενοδοχείου
- 25/4/2016 - Απόφαση για απεγκατάσταση ΚΚΒΠ στο εσωτερικό των γραφείων των εργοδοτούμενων σε επενδυτική εταιρεία και μη εγκυρότητα της συγκατάθεσης στο εργασιακό πλαίσιο
- 24/5/2018 - Απόφαση για απεγκατάσταση ΚΚΒΠ, το οποίο καταγράφει και ήχο, στα Γραφεία εταιρείας

17

Απόφαση Επιτρόπου

Εγκατάσταση και λειτουργία Κλειστού Κυκλώματος Βίντεο-παρακολούθησης, το οποίο καταγράφει και ήχο στα γραφεία της εταιρείας ΑΩ

Γεγονότα

- Η εταιρεία ΑΩ είχε εγκατεστημένες συνολικά 32 κάμερες στους χώρους εξυπηρέτησης πελατών της σε Λευκωσία, Λάρνακα, Πάφο και Παραλίμνι, στα κεντρικά γραφεία στη Λεμεσό στους χώρους που επισκέπτονται οι πελάτες/ συνεργάτες/ προμηθευτές, καθώς και εξωτερικά περιμετρικά των κεντρικών γραφείων και στα server rooms.
- Οι υπάλληλοι και οι πελάτες δεν ενημερώνονταν επαρκώς για την εν λόγω επεξεργασία.

18

Θέση της εταιρείας

- Ο σκοπός λειτουργίας του ΚΚΒΠ είναι η ασφάλεια των εγκαταστάσεων από βιαιοπραγίες και η ασφάλεια του προσωπικού από ενδεχόμενες απειλές, ο εσωτερικός έλεγχος (του προσωπικού) και η εκπαίδευση και η επίλυση διαφορών σε επίπεδο εξυπηρέτησης.
- Οι λόγοι για τους οποίους υπάρχει ανάγκη καταγραφής ήχου είναι επειδή κάθετι που επικαλείται υπάλληλος της εταιρείας την δεσμεύει, και προς απόδειξη τούτου μπορεί να χρησιμοποιηθεί το εν λόγω καταγραμμένο υλικό. Η καταγραφή ήχου χρησιμοποιείται επίσης και για θέματα ελέγχου και εκπαίδευσης του προσωπικού.

19

Νομική βάση

Οδηγία Επιτρόπου για τις εργασιακές σχέσεις (2005):

- Τα συστήματα βιντεοεπιτήρησης που έχουν ως άμεσο στόχο τον εξ' αποστάσεως έλεγχο της ποιότητας και ποσότητας των εργασιακών δραστηριοτήτων κατά κανόνα δεν επιτρέπονται. Οι εργαζόμενοι δεν εγκαταλείπουν το δικαίωμα για προστασία της ιδιωτικής ζωής τους και της προσωπικότητας τους στο κατώφλι της εισόδου του χώρου εργασίας τους.
- Ο διαρκής έλεγχος των χώρων εργασίας με μέσα παρακολούθησης προσβάλλει την αξιοπρέπεια και ιδιωτικότητα των εργαζομένων. Η βαρύτητα της προσβολής επιβάλλει όπως ο έλεγχος γίνεται μόνο εφόσον αυτό δικαιολογείται από τη φύση και τις ιδιαίτερες συνθήκες εργασίας και είναι απαραίτητος για την προστασία της υγείας και της ασφάλειας των εργαζομένων και της ασφάλειας των χώρων εργασίας, όπως για παράδειγμα σε στρατιωτικές εγκαταστάσεις, τράπεζες και εργοστάσια με εγκαταστάσεις υψηλού κινδύνου.

20

Άρθρο 5(1)(γ) του ΓΚΠΔ:

- Η επεξεργασία που γίνεται μέσω του ΚΚΒΠ, το οποίο καταγράφει ταυτόχρονα εικόνα και ήχο, είναι **υπερβολική** σε σχέση με την επίτευξη των σκοπών του εργοδότη.
- Για αντιμετώπιση των κίνδυνων που επικαλείται ο υπεύθυνος επεξεργασίας, είναι εφικτή η χρήση μέσων που είναι λιγότερο επαχθή και παρεμβατικά όπως: έλεγχοι από προσωπικό ασφαλείας, συστήματα συναγερμού, συστήματα ελέγχου πρόσβασης, κ.α
- Ο έλεγχος/ επιτήρηση και η εκπαίδευση των εργαζομένων μέσω του ΚΚΒΠ παραβιάζει την αρχή της αναγκαιότητας και της ελαχιστοποίησης. Πιο συγκεκριμένα, ο υπεύθυνος επεξεργασίας συλλέγει και επεξεργάζεται περισσότερα δεδομένα από εκείνα που απαιτούνται για την επίτευξη του σκοπού της επεξεργασίας, καθώς η χρήση των συγκεκριμένων μέσων οδηγεί στην τακτική και συστηματική παρακολούθηση των εργαζομένων.

21

- Η καταγραφή δεδομένων ήχου (συνομιλιών) μέσω του συστήματος ΚΚΒΠ κρίνεται ως άκρως παρεμβατική για την ιδιωτική ζωή, προσβάλλει την ανθρώπινη αξιοπρέπεια και γενικά απαγορεύεται. Τα υποκείμενα των δεδομένων δεν αναμένουν ότι θα καταγράφονται όλες οι συνομιλίες τους και έχουν εύλογες προσδοκίες σχετικά με την αντιμετώπιση των δεδομένων τους, καθώς και εύλογη προσδοκία για την προστασία της ιδιωτικής τους ζωής.
- Μια τέτοια δραστηριότητα επεξεργασίας απαιτεί την διενέργεια εκτίμησης αντικτύπου (άρθρο 35(1) του ΓΚΠΔ).
- Τα υποκείμενα των δεδομένων δεν ενημερώθηκαν επαρκώς για το σκοπό της επεξεργασίας, τη νόμιμη βάση και για τα δικαιώματα τους (άρθρο 13 του ΓΚΠΔ).
- Ο εργοδότης δεν μπορεί να χρησιμοποιήσει την συγκατάθεση ως τη νόμιμη βάση για την επεξεργασία επειδή στα πλαίσια της εργασιακής σχέσης η συγκατάθεση δεν μπορεί να θεωρηθεί ελεύθερη.

22

Κύρωση

- Τη διοικητική κύρωση της χρηματικής ποινής ύψους **πέντε χιλιάδων ευρώ** (€5,000)

- Τη διοικητική κύρωση της **διακοπής της επεξεργασίας** και καταστροφής των σχετικών **δεδομένων εικόνας και ήχου**, που αφορά στην παρακολούθηση των εργαζομένων μέσω του ΚΚΒΠ. Αποκλειστική **προθεσμία έξι εβδομάδων** συμμόρφωσης από την ημερομηνία της απόφασης και σχετική απόδειξη διακοπής της επεξεργασίας και καταστροφής των δεδομένων.

23

Χρήση βιομετρικών δεδομένων στην εργασία – Γνώμη 2/2018 της Επιτρόπου

- Η χρήση βιομετρικών συστημάτων (αναγνώριση προσώπου-facial recognition ή δακτυλοσκόπηση), για σκοπούς ελέγχου της ώρας προσέλευσης και αποχώρησης των υπαλλήλων στο χώρο εργασίας τους, **απαγορεύεται**.
- Ο εργοδότης πρέπει να επιλέγει άλλα μέσα λιγότερο παρεμβατικά/ επαχθή για την ανθρώπινη αξιοπρέπεια από αυτά που συνεπάγεται η συλλογή και χρήση δακτυλικών αποτυπωμάτων. Ως τέτοια μέσα είναι για παράδειγμα το σύστημα του κτυπήματος της κάρτας, οι συχνοί/ απροειδοποίητοι έλεγχοι από το Διευθυντή/ Προϊστάμενο στο σύστημα της κάρτας, η παρουσία ενός επόπτη στο χώρο όπου λειτουργεί το σύστημα ή εναλλακτικά η τοποθέτηση κάμερας παρακολούθησης πάνω από το μηχάνημα κάρτας.

24

- Ακόμη και στην περίπτωση που ο εργοδότης έχει εξασφαλίσει τη συγκατάθεση των υπαλλήλων, η εν λόγω συγκατάθεση δεν αίρει την παρανομία και δεν τη νομιμοποιεί, αφού στον εργασιακό τομέα η συγκατάθεση των εργαζομένων δεν δίνεται ελεύθερα.
- Κατ' εξαίρεση, η χρήση βιομετρικών συστημάτων **επιτρέπεται** αποκλειστικά **για λόγους ασφάλειας των χώρων**, όταν πρόκειται για χώρους υψηλού κινδύνου ή υψίστης ασφαλείας (όπως λιμάνια, αεροδρόμια, στρατιωτικές εγκαταστάσεις), για σκοπούς **ελέγχου της φυσικής πρόσβασης** των εργαζομένων σε αυτούς (όχι για τον έλεγχο της τήρησης του ωραρίου).

25

Σχετικά με το θέμα:

- Η Απόφαση του Επιτρόπου, ημερομηνίας 2.10.2012, η οποία αφορά σε Ιδιωτικό Νοσηλευτήριο (βλ. ιστοσελίδα)
- Η Εγκύκλιος που εξέδωσε η Επίτροπος προς τους προμηθευτές συστημάτων ελέγχου πρόσβασης, ημερομηνίας 13.1.2009, (βλ. ιστοσελίδα)

26

Μέρος ΙΙ
Συγκατάθεση

27

Συγκατάθεση ως νόμιμη βάση για την επεξεργασία

- Η συγκατάθεση μπορεί να αποτελεί κατάλληλη νόμιμη βάση μόνο εάν στο υποκείμενο των δεδομένων δίνεται πραγματική επιλογή όσον αφορά την αποδοχή ή την απόρριψη των προσφερόμενων όρων ή την απόρριψη αυτών χωρίς ζημία.
- Όταν ο υπεύθυνος επεξεργασίας ζητεί συγκατάθεση, πρέπει να εξετάζει αν πληρούνται όλες οι απαιτήσεις για την εξασφάλιση έγκυρης συγκατάθεσης.

28

Στοιχεία έγκυρης συγκατάθεσης

Το άρθρο 4 σημείο 11 του ΓΚΠΔ ορίζει ότι ως συγκατάθεση του υποκειμένου των δεδομένων ορίζεται κάθε ένδειξη βουλήσεως:

- ελεύθερη
- συγκεκριμένη
- εν πλήρει επιγνώσει και
- ρητή, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν

29

Ελεύθερη συγκατάθεση

- «Ελεύθερη» σημαίνει ότι τα υποκείμενα των δεδομένων έχουν πραγματική επιλογή και έλεγχο.
- Εάν το υποκείμενο των δεδομένων δεν έχει πραγματική επιλογή, νιώθει ότι εξαναγκάζεται να συγκατατεθεί ή ότι θα υποστεί αρνητικές συνέπειες εάν δεν συγκατατεθεί, η συγκατάθεση δεν είναι έγκυρη.
- Η συγκατάθεση δεν θεωρείται ελεύθερη εάν το υποκείμενο των δεδομένων δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί.

30

Παράδειγμα

Δήμος προγραμματίζει έργα συντήρησης του οδικού δικτύου. Καθώς τα οδικά έργα ενδέχεται να δημιουργήσουν προβλήματα στην κυκλοφορία για μεγάλο χρονικό διάστημα, ο δήμος παρέχει στους δημότες τη δυνατότητα να εγγραφούν σε κατάλογο διευθύνσεων ηλεκτρονικού ταχυδρομείου, ώστε να λαμβάνουν ενημερώσεις σχετικά με την πρόοδο των έργων και τις αναμενόμενες καθυστερήσεις. Ο δήμος καθιστά σαφές ότι η συμμετοχή δεν είναι υποχρεωτική και ζητεί συγκατάθεση για τη χρήση των διευθύνσεων ηλεκτρονικού ταχυδρομείου (αποκλειστικά) για τον σκοπό αυτό. Οι δημότες που δεν συγκατατίθενται δεν θα στερηθούν καμία βασική υπηρεσία του δήμου ούτε θα απολέσουν τη δυνατότητα άσκησης οποιουδήποτε δικαιώματος και, επομένως, μπορούν ελεύθερα να παράσχουν ή να αρνηθούν τη συγκατάθεσή τους στη συγκεκριμένη χρήση των δεδομένων. Όλες οι πληροφορίες σχετικά με τα οδικά έργα θα είναι επίσης διαθέσιμες στον δικτυακό τόπο του δήμου.

31

Παράδειγμα

Ένας έμπορος λιανικής ζητεί, εντός του ίδιου αιτήματος συγκατάθεσης, από τους πελάτες του να συγκατατεθούν στη χρήση των δεδομένων τους ώστε να τους αποστέλλει ηλεκτρονικά μηνύματα εμπορικής προώθησης καθώς και για να διαβιβάσει τα στοιχεία τους σε άλλες εταιρείες του ομίλου του. Η συγκατάθεση αυτή δεν είναι αναλυτική, καθώς δεν υπάρχουν χωριστές συγκαταθέσεις για τους δύο αυτούς χωριστούς σκοπούς και, επομένως, η συγκατάθεση δεν θα είναι έγκυρη. Στην περίπτωση αυτή, θα πρέπει να ληφθεί συγκεκριμένη συγκατάθεση για τη διαβίβαση των στοιχείων επικοινωνίας σε εμπορικούς εταίρους. Η συγκεκριμένη αυτή συγκατάθεση θα θεωρείται έγκυρη για κάθε εταίρο του οποίου η ταυτότητα παρασχέθηκε στο υποκείμενο των δεδομένων κατά τη λήψη της συγκατάθεσής του, εφόσον η συγκατάθεση διαβιβάζεται σε αυτούς για τον ίδιο σκοπό (στο παρόν παράδειγμα: σκοπός εμπορικής προώθησης).

32

Συγκεκριμένη συγκατάθεση

- Οι μηχανισμοί συγκατάθεσης δεν πρέπει μόνο να είναι αναλυτικοί προκειμένου να ανταποκρίνονται στην απαίτηση «ελεύθερης» συγκατάθεσης, αλλά πρέπει επίσης να είναι «συγκεκριμένοι».
- Αυτό σημαίνει ότι υπεύθυνος επεξεργασίας, ο οποίος ζητεί συγκατάθεση για περισσότερους και διαφορετικούς σκοπούς θα πρέπει να παρέχει χωριστή δυνατότητα επιλογής συμμετοχής για κάθε σκοπό, ώστε τα υποκείμενα των δεδομένων να μπορούν να παρέχουν συγκεκριμένη συγκατάθεση για συγκεκριμένους σκοπούς.

33

Λεπτομερής ανάλυση

- Η συγκατάθεση δεν παρασχέθηκε ελεύθερα και δεν είναι συγκεκριμένη εάν η διαδικασία για την εξασφάλισή της δεν επιτρέπει στα υποκείμενα των δεδομένων να παρέχουν αντίστοιχα χωριστή συγκατάθεση σε διαφορετικές πράξεις επεξεργασίας.
- Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς.
- Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται ξεχωριστή συγκατάθεση για κάθε ένα από τους σκοπούς (αιτιολογική σκέψη 32).

34

- Παράδειγμα

Εφαρμογή για φορητές συσκευές για την επεξεργασία φωτογραφιών ζητεί από τους χρήστες της να ενεργοποιήσουν τον εντοπισμό της θέσης τους μέσω GPS για τη χρήση των υπηρεσιών της. Η εφαρμογή ενημερώνει επίσης τους χρήστες της ότι θα χρησιμοποιήσει τα δεδομένα που θα συλλέξει για σκοπούς συμπεριφορικής διαφήμισης. Ο γεωγραφικός εντοπισμός και η διαδικτυακή συμπεριφορική διαφήμιση δεν είναι στοιχεία αναγκαία για την παροχή της υπηρεσίας επεξεργασίας φωτογραφιών και υπερβαίνουν την παροχή της βασικής υπηρεσίας. Δεδομένου ότι οι χρήστες δεν μπορούν να χρησιμοποιήσουν την εφαρμογή χωρίς να συγκατατεθούν στους σκοπούς αυτούς, η συγκατάθεση δεν μπορεί να θεωρηθεί ότι παρέχεται ελεύθερα.

35

Ζημία

- Ο υπεύθυνος επεξεργασίας θα πρέπει να αποδείξει ότι το υποκείμενο των δεδομένων μπορεί να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί (αιτιολογική σκέψη 42).
- Για παράδειγμα, ο υπεύθυνος επεξεργασίας πρέπει να αποδείξει ότι η ανάκληση της συγκατάθεσης δεν συνεπάγεται κανένα κόστος για το υποκείμενο των δεδομένων και, επομένως, κανένα σαφές μειονέκτημα για εκείνον που ανακαλεί τη συγκατάθεσή του.

36

- Παράδειγμα

Υποκείμενο δεδομένων εγγράφεται συνδρομητής σε ενημερωτικό δελτίο εμπόρου λιανικής πώλησης ειδών μόδας, το οποίο περιλαμβάνει γενικές εκπτώσεις. Ο έμπορος λιανικής ζητεί τη συγκατάθεση του υποκειμένου των δεδομένων για τη συλλογή περισσότερων δεδομένων σχετικά με τις αγοραστικές προτιμήσεις του, ώστε να προσαρμόσει τις προσφορές στις προτιμήσεις του υποκειμένου των δεδομένων βάσει του ιστορικού αγορών ή ερωτηματολογίου το οποίο συμπληρώνεται προαιρετικά. Εάν το υποκείμενο των δεδομένων ανακαλέσει αργότερα τη συγκατάθεση, θα λαμβάνει εκ νέου μη εξατομικευμένες εκπτώσεις στα είδη μόδας. Αυτό δεν συνιστά ζημία, καθώς χάθηκε μόνο το επιτρεπόμενο κίνητρο.

37

Εν πλήρει επιγνώσει συγκατάθεση

- Η παροχή πληροφοριών στα υποκείμενα των δεδομένων πριν από την εξασφάλιση της συγκατάθεσής τους είναι ουσιώδης προκειμένου να παρέχεται σε αυτά η δυνατότητα να λαμβάνουν ενημερωμένες αποφάσεις, να κατανοούν αυτό στο οποίο συγκατατίθενται και να ασκούν, για παράδειγμα, το δικαίωμα ανάκλησης της συγκατάθεσής τους.
- Εάν ο υπεύθυνος επεξεργασίας δεν παρέχει προσβάσιμες πληροφορίες, ο έλεγχος του χρήστη καθίσταται πλασματικός και η συγκατάθεση είναι ανίσχυρη βάση για την επεξεργασία.
- «Εν πλήρει επιγνώσει» συγκατάθεση μπορεί να υπάρξει ακόμη και όταν δεν αναφέρονται κατά τη διαδικασία εξασφάλισης της συγκατάθεσης όλα τα στοιχεία που προβλέπονται στα άρθρα 13 του Κανονισμού
- Όμως, τα στοιχεία αυτά πρέπει να αναφέρονται σε άλλα σημεία, όπως στην ανακοίνωση της εταιρείας σχετικά με την προστασία των δεδομένων (privacy policy).

38

Τρόπος παροχής των πληροφοριών

- Ο ΓΚΠΔ δεν καθορίζει τον τρόπο ή τη μορφή με την οποία πρέπει να παρέχονται οι πληροφορίες προκειμένου να πληρούται η απαίτηση της εν πλήρει επιγνώσει συγκατάθεσης.
- Έγκυρες πληροφορίες μπορούν να παρέχονται με διάφορους τρόπους, όπως με
  - γραπτές ή προφορικές δηλώσεις ή
  - ακουστικά ή οπτικά μηνύματα

39

Εξασφάλιση ρητής συγκατάθεσης

- Ο όρος ρητή σημαίνει ότι το υποκείμενο των δεδομένων πρέπει να προβεί σε ρητή δήλωση συγκατάθεσης.
- Ένας προφανής τρόπος είναι η γραπτή δήλωση.
- Η χρήση προφορικών δηλώσεων μπορεί επίσης να είναι ικανοποιητική για την εξασφάλιση έγκυρης ρητής συγκατάθεσης, όμως
- Ο υπεύθυνος επεξεργασίας μπορεί να αντιμετωπίσει δυσκολίες στο να αποδείξει ότι πληρούνταν όλες οι προϋποθέσεις έγκυρης ρητής συγκατάθεσης όταν για παράδειγμα ηχογραφήθηκε η δήλωση.

40

- Παράδειγμα

Ο υπεύθυνος επεξεργασίας δεδομένων μπορεί επίσης να εξασφαλίσει ρητή συγκατάθεση από επισκέπτη στον δικτυακό τόπο του προσφέροντας μια οθόνη ρητής συγκατάθεσης η οποία περιέχει τετραγωνίδια «Ναι» και «Όχι», υπό τον όρο ότι στο κείμενο αναφέρεται σαφώς η συγκατάθεση, για παράδειγμα, «Με το παρόν συγκατατίθεμαι στην επεξεργασία των δεδομένων μου», και όχι, για παράδειγμα, «Αντιλαμβάνομαι ότι τα δεδομένα μου θα υποβληθούν σε επεξεργασία». Εξυπακούεται ότι πρέπει να πληρούνται οι προϋποθέσεις για εν πλήρει επιγνώσει συγκατάθεση καθώς και οι λοιπές προϋποθέσεις για την εξασφάλιση έγκυρης συγκατάθεσης.

41

Απόφαση Επιτρόπου

Δημοσίευση προσωπικών δεδομένων πελατών της εταιρείας ΧΒ στο διαδίκτυο και σε περιοδικά

Γεγονότα

- Η εταιρεία ΧΒ δραστηριοποιείται στον τομέα της διαιτολογίας και προσφέρει προγράμματα για μείωση του σωματικού βάρους.
- Οι πελάτες που συμμετέχουν στο πρόγραμμα υπογράφουν συμφωνία για συμμετοχή στο πρόγραμμα και στην συμφωνία υπάρχει ρήτρα που προβλέπει ότι οι φωτογραφίες τους μαζί με προσωπικά δεδομένα τους, περιλαμβανομένων και δεδομένων που αφορούν στην υγεία π.χ. αν πάσχουν από κάποια ασθένεια που συμβάλλει στην αύξηση του σωματικού βάρους, πιθανόν να δημοσιευτούν στην ιστοσελίδα της ΧΒ και στα μέσα κοινωνικής δικτύωσης Facebook και Instagram.

42

Νομική βάση

- Η επεξεργασία των προσωπικών δεδομένων των πελατών (όνομα, στοιχεία επικοινωνίας, δεδομένα υγείας, φωτογραφίες) για συμμετοχή στο πρόγραμμα έχει ως νόμιμη βάση την σύμβαση (άρθρο 6(1)(β) του ΓΚΠΔ).
- Η δημοσίευση των προσωπικών δεδομένων των πελατών στην ιστοσελίδα της ΧΒ και στα μέσα κοινωνικής δικτύωσης Facebook και Instagram δεν μπορεί να είναι μέρος της συμφωνία που υπογράφει ο πελάτης για συμμετοχή του στο πρόγραμμα και ούτε πρέπει να αποτελεί προϋπόθεση για τη συμμετοχή του (άρθρα 5(1)(β) και 7 του ΓΚΠΔ).
- Η δημοσίευση των προσωπικών δεδομένων των πελατών μπορεί να γίνει μόνο με την **ξεχωριστή** συγκατάθεση τους (άρθρα 6(1)(β) και 7 του ΓΚΠΔ).

43

Κύρωση

- Με βάση το άρθρο 58 παράγραφος 2(δ) του Κανονισμού, η Επίτροπος έδωσε εντολή στον υπεύθυνο επεξεργασίας, να αναθεωρήσει τα έντυπα ενημέρωσης και συγκατάθεσης ώστε να τα καταστήσει σύμφωνα με τις διατάξεις των άρθρων 7 και 13 του ΓΚΠΔ.

44

Μέρος ΙΙΙ
Διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς

45

Τι είναι τρίτη χώρα

- Τρίτη χώρα είναι κάθε χώρα που είναι εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ).
- Οι χώρες του ΕΟΧ είναι τα 28 κράτη-μελή της Ευρωπαϊκής Ένωσης, καθώς και η Ισλανδία, Νορβηγία και Λιχνενστάιν.

46

Διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς - Γενικός κανόνας

- Κατά τη διαβίβαση δεδομένων, ο Κανονισμός επιβάλλει αυστηρούς περιορισμούς στις μεταφορές σε σημεία εκτός του ΕΟΧ, όταν τα δεδομένα προορίζονται να υποβληθούν σε επεξεργασία μετά από τη διαβίβασή τους σε τρίτη χώρα ή διεθνή οργανισμό.
- Αυτό γίνεται προκειμένου να διασφαλιστεί ότι το επίπεδο προστασίας των φυσικών προσώπων που εγγυάται ο κανονισμός θα παραμένει το ίδιο μετά την διαβίβαση.

47

- Παράδειγμα

Εάν μια θυγατρική ενός διεθνούς ομίλου επιχειρήσεων που είναι εγκατεστημένη σε διάφορα κράτη μέλη, μεταξύ των οποίων η Σλοβενία και η Γαλλία, αποστέλλει προσωπικά δεδομένα από τη Σλοβενία στη Γαλλία, μια τέτοια ροή δεδομένων δεν μπορεί να περιορίζεται ή να απαγορεύεται από το εθνικό δίκαιο της Σλοβενίας για λόγους προστασίας προσωπικών δεδομένων.

Εάν, ωστόσο, η θυγατρική της Γαλλίας επιθυμεί να διαβιβάσει τα ίδια προσωπικά δεδομένα σε εκτελούντα την επεξεργασία στη Μαλαισία, τότε ο Σλοβένος εξαγωγέας δεδομένων πρέπει να λάβει υπόψη του κανόνες του κεφαλαίου V του ΓΚΠΔ.

48

Διαβιβάσεις βάσει απόφαση επάρκειας

- Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό μπορεί να πραγματοποιηθεί εφόσον η Ευρωπαϊκή Επιτροπή έχει αποφασίσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας (adequacy decision) από την τρίτη χώρα, από έδαφος ή από έναν ή περισσότερους συγκεκριμένους τομείς στην εν λόγω τρίτη χώρα ή από τον εν λόγω διεθνή οργανισμό.
- Για μια τέτοια διαβίβαση δεν απαιτείται ειδική άδεια.

➔ Βλέπετε **ιστοσελίδα της Ευρωπαϊκής Επιτροπής** αναφορικά με τις αποφάσεις επάρκειας μετά την εφαρμογή του ΓΚΠΔ.

49

Αποφάσεις επάρκειας της Ευρωπαϊκής Επιτροπής

- Η Ευρωπαϊκή Επιτροπή έχει κρίνει ότι η διαβίβαση στις ακόλουθες 11 χώρες είναι ασφαλής επειδή εξασφαλίζουν ισοδύναμο επίπεδο προστασίας ΠΔ:
  - Ανδόρα
  - Αργεντινή
  - Ελβετία
  - Καναδάς (μερική)
  - Νήσοι Φαρόε
  - Ισραήλ
  - Νήσος του Μαν
  - Τσέρσεϋ
  - Νέα Ζηλανδία
  - Ουρουγουάη
  - Ιαπωνία (2019)

➔ Βλέπετε **ιστοσελίδα της Ευρωπαϊκής Επιτροπής** αναφορικά με τις αποφάσεις επάρκειας μετά την εφαρμογή του ΓΚΠΔ.

50

Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις

- Αν δεν υπάρχει απόφαση επάρκειας, ο υπεύθυνος επεξεργασίας ή ο εκτελών μπορεί να διαβιβάσει προσωπικά δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό μόνο εάν υπάρχουν **κατάλληλες εγγυήσεις**, και
- υπό την προϋπόθεση ότι υπάρχουν **εκτελεστά δικαιώματα** και **αποτελεσματικά ένδικα μέσα** για τα υποκείμενα των δεδομένων.

51

Οι κατάλληλες εγγυήσεις μπορεί να προβλέπονται χωρίς Άδεια της Επιτρόπου με:

- **Νομικά δεσμευτικό μέσο** μεταξύ δημόσιων αρχών π.χ. πολυμερής συμφωνία, FATCA ή
- **Δεσμευτικούς εταιρικούς κανόνες** (binding corporate rules – BCRs) - για ομίλους επιχειρήσεων - που εγκρίνονται από την Επίτροπο στα πλαίσια του μηχανισμού συνεκτικότητας και υπό τον όρους του άρθρου 47 ή
- **Τυποποιημένες ρήτρες** (standard DP clauses) που εκδίδονται από την Επιτροπή (σύμφωνα με τη διαδικασία εξέτασης του άρθρου 93(2) του Κανονισμού) ή
- **Τυποποιημένες ρήτρες** (standard DP clauses) που εκδίδονται από την Επίτροπο και εγκρίνονται από την Επιτροπή (σύμφωνα με τη διαδικασία εξέτασης του άρθρου 93(2) του Κανονισμού) ή
- **Κώδικα δεοντολογίας**, ο οποίος εγκρίνεται από την Επίτροπο ή από το Συμβούλιο Προστασίας Δεδομένων, εάν αφορά διάφορα ΚΜ ή
- **Μηχανισμό πιστοποίησης**, ο οποίος εγκρίνεται από την Επίτροπο ή τον εθνικό οργανισμό πιστοποίησης ή και από τους δύο

52

Επιτρέπεται επίσης η διαβίβαση που υπόκεινται σε κατάλληλες εγγυήσεις με Άδεια της Επιτρόπου:

- Εάν ο Οργανισμός επιλέξει ως νομική βάση για τη διαβίβαση **συμβατικές ρήτρες** (contractual clauses) που θα ετοιμάσει και θα εγκριθούν από την Επίτροπο
- Εάν από τη διαβίβαση επηρεάζονται πολίτες ΚΜ, οι συμβατικές ρήτρες θα εγκριθούν στα πλαίσια του μηχανισμού συνεκτικότητας*

* Θεσπίζεται μηχανισμός συνεκτικότητας για τη συνεργασία μεταξύ των εποπτικών αρχών, ιδιαίτερα όταν μια εποπτική αρχή θεσπίζει μέτρο που επηρεάζει ουσιωδώς σημαντικό αριθμό υποκειμένων των δεδομένων σε περισσότερα από ένα ΚΜ.

53

Παρεκκλίσεις σε ειδικές καταστάσεις

- Το Άρθρο 49 του Κανονισμού επιτρέπει τη διαβίβαση σε τρίτη χώρα, στη βάση παρεκκλίσεων όπως τη συγκατάθεση του υποκειμένου των δεδομένων, την εκτέλεση σύμβασης ή για προσυμβατικά μέτρα ή την άσκηση νομικών αξιώσεων,
- **Μόνο όμως**, εφόσον ο οργανισμός δεν μπορεί να διαβιβάζει τα εν λόγω δεδομένα στη βάση των κατάλληλων εγγυήσεων.
- Η διαβίβαση στη βάση παρεκκλίσεων, είναι το έσχατο μέτρο που μπορεί να επιλέξει ο οργανισμός. Με βάση την Αρχή της Λογοδοσίας, θα πρέπει να είναι σε θέση να αποδείξει, τόσο στα υποκείμενα των δεδομένων όσο και στην Επίτροπο, γιατί δεν μπορεί να βασιστεί στα Άρθρα 46 και 47.
- Σύμφωνα με τις αρχές που είναι εγγενείς στο Ευρωπαϊκό δίκαιο, οι παρεκκλίσεις πρέπει να ερμηνεύονται στενά ώστε η εξαίρεση να μην καθίσταται κανόνας.

➔ Αναφορικά με τις παρεκκλίσεις του άρθρου 49 υπάρχουν **κατευθυντήριες γραμμές 2/2018** που έκδωσε το EDPB (25/5/2018)

54

- Παράδειγμα

Μια εταιρεία παροχής υπηρεσιών παγκόσμιου συστήματος διανομής (GDS), με έδρα στις ΗΠΑ, παρέχει το σύστημα επιγραμμικών κρατήσεων για πολλαπλές αεροπορικές εταιρείες, ξενοδοχεία και κρουαζιέρες σε όλο τον κόσμο, και επεξεργάζεται για τον σκοπό αυτό δεδομένα δεκάδων εκατομμυρίων ατόμων στην ΕΕ. Για την αρχική διαβίβαση δεδομένων στους κεντρικούς υπολογιστές στις Η.Π.Α., η εταιρεία GDS βασίζεται σε μια παρέκκλιση ως νόμιμη βάση για τη διαβίβαση, αυτή είναι η αναγκαιότητα σύναψης σύμβασης. Έτσι, δεν παρέχει άλλες εγγυήσεις για τα προσωπικά δεδομένα που προέρχονται από την Ευρώπη, διαβιβάζονται στις ΗΠΑ και στη συνέχεια ανακατανέμονται σε ξενοδοχεία σε όλο τον κόσμο (δηλαδή δεν υπάρχουν εγγυήσεις για μεταγενέστερες διαβιβάσεις). Η εταιρεία GDS δεν συμμορφώνεται με τις απαιτήσεις του Κανονισμού για νόμιμες διεθνείς διαβιβάσεις δεδομένων, διότι βασίζεται σε παρέκκλιση ως νόμιμη βάση για μαζικές διαβιβάσεις.

55

Η «Ασπίδα Προστασίας της Ιδιωτικής Ζωής ΕΕ–ΗΠΑ» - PRIVACY SHIELD

- Το PRIVACY SHIELD είναι ένας μηχανισμός αυτοπιστοποίησης για εταιρείες που εδρεύουν στις ΗΠΑ ο οποίος έχει αναγνωριστεί με Εκτελεστή Απόφαση της Ευρωπαϊκής Επιτροπής (ΕΕ) 2016/1250 ότι εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων που διαβιβάζονται από οργανισμούς της Ε.Ε, σε οργανισμούς στις ΗΠΑ. Οι εν λόγω εταιρείες έχουν αυτοπιστοποιηθεί ότι παρέχουν τις κατάλληλες νομικές εγγυήσεις για αυτές τις διαβιβάσεις και δεσμεύονται να τηρούν ένα σύνολο αρχών προστασίας της ιδιωτικής ζωής.
- Αυτό σημαίνει ότι προσωπικά δεδομένα μπορούν να διαβιβάζονται ελεύθερα προς τους οργανισμούς στις ΗΠΑ που περιλαμβάνονται στον «κατάλογο της ασπίδας προστασίας της ιδιωτικής ζωής», ο οποίος τηρείται και δημοσιεύεται από το Υπουργείο Εμπορίου των ΗΠΑ.

➔ Οι εταιρείες που περιλαμβάνονται στον «κατάλογο της ασπίδας προστασίας της ιδιωτικής ζωής» είναι διαθέσιμες στην ιστοσελίδα του **Privacy Shield Framework**.

56

Μέρος IV
Δράσεις της Επιτρόπου και Διοικητικοί έλεγχοι

57

Δράσεις του Γραφείου της Επιτρόπου από το 2016

Ευαισθητοποίηση

- Ευαισθητοποίηση του κοινού και των υπεύθυνων επεξεργασίας
- Δημόσιες δράσεις επικοινωνίας: ανακοινώσεις στον τύπο, ιστοσελίδα
- Συνέδρια, επιμορφωτικά εργαστήρια
- Οδηγίες, συστάσεις και κατευθυντήριες γραμμές

58

28η Ιανουαρίου – Ημέρα προστασίας δεδομένων

59

Συμβουλευτικός ρόλος

- Παροχή γνωμοδοτήσεων σε κοινοβουλευτικές επιτροπές, στην κυβέρνηση, ανεξάρτητους θεσμούς, φορείς δημόσιου και ιδιωτικού δικαίου.

Προστασία και επιβολή του νόμου

- Ουσιαστική πρόσβαση των πολιτών στα δεδομένα τους
- Εξέταση καταγγελιών
- Επιβολή κυρώσεων
- Διοικητικοί έλεγχοι

60

Αναλυτικά τι ελέγχεται σε ένα τυπικό διοικητικό έλεγχο

1. Ορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO)

- έχει οριστεί DPO;
- αν έχει οριστεί -
  - έχει τα προσόντα που προβλέπονται από τον ΓΚΠΔ;
  - υπάρχει σύγκρουση καθηκόντων;
  - είναι ξεκάθαρος ο ρόλος του;

61

2. Αρχείο Δραστηριοτήτων της επεξεργασίας

- τηρείται το αρχείο δραστηριοτήτων;
- είναι ορθά συμπληρωμένο και ενημερώνεται όπως προβλέπει ο κανονισμός;

62

3. Έλεγχος των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας:

- είναι σύμφωνα με το σκοπό για τον οποίο έχουν αρχικά συλλεχθεί;
- είναι μόνο τα απαραίτητα;
- είναι ορθά και ενημερωμένα;
- διατηρούνται μόνο για όσο χρονικό διάστημα είναι απολύτως απαραίτητα;
- χρησιμοποιούνται τα εργαλεία της κρυπτογράφησης ή ψευδωνυμοποίησης εκεί όπου είναι απαραίτητα;

63

4. Υιοθέτηση των απαιτήσεων ασφάλειας των δεδομένων:

- λαμβάνονται τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφάλειας και προστασίας τους;
- αυτά τα μέτρα αναθεωρούνται τακτικά για να λαμβάνουν υπόψη τις νέες τεχνολογικές εξελίξεις;
- έχουν αντικατασταθεί οι υφιστάμενες λίστες ελέγχου που αφορούν στους κινδύνους της επεξεργασίας λαμβάνοντας υπόψη τη φύση, πεδίο εφαρμογής, περιεχόμενο και σκοπό της επεξεργασίας;
- έχει υιοθετηθεί σύστημα διοίκησης για τακτική αναθεώρηση, αξιολόγηση και βελτίωση των μέτρων ασφάλειας;
- έχουν ληφθεί μέτρα π.χ. ψευδωνυμοποίηση και κρυπτογράφηση για προστασία από παράνομη επεξεργασία από εσωτερικούς και εξωτερικούς εισβολείς;

64

5. Εσωτερικές διαδικασίες:

- υπάρχει εσωτερική διαδικασία αναφοράς της παραβίασης;
- υπάρχει «πλάνο ανταπόκρισης» (response plan) σε περίπτωση παραβίασης;
- υπάρχει διαδικασία γνωστοποίησης ενδεχόμενης παραβίασης στην Επίτροπο, εντός 72 ωρών;

65

6. Διενέργεια εκτίμησης αντικτύπου όταν η επεξεργασία ενέχει υψηλό κίνδυνο / ρίσκο στα δικαιώματα, ελευθερίες και συμφέροντα των ατόμων:

- έχει υιοθετηθεί μέθοδος που να αναγνωρίζει εάν υπάρχει υψηλός κίνδυνος;
- έχει επιλεγεί διαδικασία για διενέργεια ΕΑ;
- έχει υιοθετηθεί πολιτική με προκαθορισμένη διαδικασία για αντιμετώπιση του υψηλού κινδύνου;
- έχει ληφθεί υπόψη ο ενδεικτικός κατάλογος που βρίσκεται αναρτημένος στην ιστοσελίδα του Γραφείο;

66

7. Εκπαίδευση και ευαισθητοποίηση του προσωπικού

- έχει εκπαιδευτεί κατάλληλα το προσωπικό σε σχέση με τους ρόλους και τις ευθύνες τους;
- έχουν λάβει την κατάλληλη εκπαίδευση για την ασφάλεια των δεδομένων που χειρίζονται;
- μπορούν να αναγνωρίσουν μια παραβίαση προσωπικών δεδομένων;

67

8. Δεδομένα εκτός του οργανισμού

- έλεγχος των συμφωνιών μεταξύ 2 υπεύθυνων επεξεργασίας, σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας
- έλεγχος των συμβολαίων/συμβάσεων που συνάπτονται με εκτελούντες την επεξεργασία (βλ. άρθρο 28 του Κανονισμού για το τι πρέπει να περιλαμβάνει μία σύμβαση ανάθεσης εργασίας σε εκτελούντα)

68

9. Διαβίβαση δεδομένων σε τρίτες χώρες

- διαβιβάζονται δεδομένα σε χώρες εκτός ΕΕ;
- έχει επιλεγεί η νομική βάση για την διαβίβαση (άρθρα 45-49 του ΓΚΠΔ);
- εάν ο Οργανισμός έχει επιλέξει ως νομική βάση για τη διαβίβαση τις συμβατικές ρήτρες, υπάρχει διασφάλιση ότι αυτές έχουν εγκριθεί από την Επίτροπο;

10. Σε περίπτωση διασυνοριακής επεξεργασίας, εντός της ΕΕ

- έχει οριστεί το ΚΜ της κύριας εγκατάστασης, του οποίου η εποπτεύουσα αρχή θα είναι αρμόδια ως επικεφαλής αρχή, για την εποπτεία της νομιμότητας της επεξεργασίας εντός της Ε.Ε;

69

11. Ενημέρωση των υποκειμένων των δεδομένων (υπαλλήλων και πελατών)

Τα υποκείμενα ενημερώνονται κατάλληλα;
Για παράδειγμα:

- ποιος είναι ο υπεύθυνος επεξεργασίας
- σκοπός της επεξεργασίας
- νομική βάση για την επεξεργασία
- νομική βάση για διαβίβαση σε τρίτη χώρα (εάν ισχύει)
- χρονικό διάστημα διατήρησης των δεδομένων
- τα δικαιώματα που μπορούν να ασκήσουν
- στοιχεία επικοινωνίας του DPO
- δικαίωμα υποβολής παραπόνου στην Επίτροπο
- σε περίπτωση που η συγκατάθεση είναι η νομική βάση της επεξεργασίας, να γνωρίζουν ότι μπορούν να την ανακαλέσουν ανά πάσα στιγμή
- σε περίπτωση αυτοματοποιημένης λήψης απόφασης (π.χ. κατάρτιση προφίλ), τη λογική, σημασία και επιπτώσεις τέτοιας επεξεργασίας στο υποκείμενο
- σε περίπτωση συλλογής των δεδομένων, όχι από το ίδιο το υποκείμενο, την πηγή/προέλευση τους

70

Ρόλος του DPO στα πλαίσια του διοικητικού ελέγχου

Έχει σημαντικό ρόλο:

- Διευκολύνει την πρόσβαση της Επιτρόπου και των λειτουργών της σε όλες τις ζητούμενες πληροφορίες και έγγραφα.
- Παρίσταται στον έλεγχο και παρέχει όλες τις απαιτούμενες πληροφορίες και έγγραφα.
- Διασφαλίζει ότι ο έλεγχος διεξάγεται ομαλά και αποτελεσματικά.

71

Αποτελέσματα έλεγχου που διενεργήθηκε σε δείγμα του Τραπεζικού τομέα (Νοέμβριος 2018)

Σημεία που χρήζουν βελτίωσης και επαναξιολόγησης

- Ορθή επιλογή DPO χωρίς συγκρουσιακές καταβολές
- Κατάρτιση και εκπαίδευση του προσωπικού
- Αναθεώρηση εγχειριδίων και πολιτικών
- Αναθεώρηση εγγράφων προς τους πελάτες
- Επαναξιολόγηση όλων των περιπτώσεων διαβίβασης σε τρίτες χώρες
- Ορθή συμπλήρωση του Αρχείου Δραστηριοτήτων
- Αναθεώρηση συμβάσεων ανάθεσης επεξεργασίας σε εκτελούντα
- Βελτίωση των διαδικασιών ικανοποίησης των αιτημάτων για άσκηση των δικαιωμάτων των υποκειμένων
- Ενίσχυση μέτρων ασφάλειας με διαδικασίες κρυπτογράφησης.

72

Αποτελέσματα ελέγχου ΚΟΑ για σύστημα Κάρτας Φιλάθλου

Σημεία που χρήζουν βελτίωσης και επαναξιολόγησης

- Ξεχωριστή ηλεκτρονική διεύθυνση για τον DPO
- Βελτίωση του privacy policy
- Εκπαίδευση λειτουργών του ΚΟΑ για θέματα εμπιστευτικότητας
- Θέσπιση διαδικασιών για εύκολη διαγραφή τους από το Μητρώο Φιλάθλων
- Λήψη τεχνικών μέτρων για ενίσχυση του επιπέδου ασφάλειας του συστήματος

73

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

This seminar was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

74