

Κανονισμός (ΕΕ) 2016/679 και επεξεργασία προσωπικών δεδομένων από τουριστικά/ταξιδιωτικά γραφεία και ξενοδοχεία

**Επίτροπος Προστασίας
Δεδομένων Προσωπικού Χαρακτήρα**

2 Μαρτίου 2018

1

Ανάγκη αντικατάστασης του υφιστάμενου πλαισίου:

Η υφιστάμενη Οδηγία (95/46/ΕΚ), μετά από περίπου μια εικοσαετία, θεωρείται ξεπερασμένη - δεν ανταποκρίνεται επαρκώς στις ανάγκες της εποχής λόγω:

- Των ραγδαίων τεχνολογικών εξελίξεων π.χ. smartphones, mobile banking
- Της χρήσης του διαδικτύου και των νέων υπηρεσιών που παρέχει π.χ. ηλεκτρονικό εμπόριο
- Της ανάπτυξης της ψηφιακής οικονομίας π.χ. internet banking
- Της ευρείας χρήσης των μέσων κοινωνικής δικτύωσης
- Της αυξανόμενης δημοσιοποίησης προσωπικών πληροφοριών π.χ. δεδομένων υγείας και διάθεσής τους σε παγκόσμιο επίπεδο

2

Καινοτομίες του Κανονισμού

(α) Ομοιόμορφη μεταφορά και εφαρμογή:

- ❖ διαμορφώνεται ενιαίο νομικό πλαίσιο χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας
- ❖ ίδιο επίπεδο νομικά εκτελεστών δικαιωμάτων και υποχρεώσεων, σε όλα τα κράτη μέλη
- ❖ επιβολή ισοδύναμων κυρώσεων από τις ΑΠΔΠΧ

(β) Ενίσχυση υφιστάμενων δικαιωμάτων και δημιουργία νέων

(γ) Ενίσχυση υφιστάμενων αρχών προστασίας των δεδομένων

(δ) Αυστηρότερες υποχρεώσεις στους υπεύθυνους επεξεργασίας

(ε) Δικαίωμα αποζημίωσης και για μη υλική ζημία

(στ) Ενδυνάμωση συνεργασίας ΑΠΔΠΧ σε διασυνοριακές υποθέσεις

(ζ) Εισαγωγή του θεσμού της ενιαίας θυρίδας (one stop shop)

(κάθε πολίτης και κάθε επιχείρηση μπορεί να συναλλάσσεται με μία μόνο ΑΠΔΠΧ)

3

(η) Διενέργεια ελέγχων before the event

(θ) Πρόσβαση από την ΑΠΔΠΧ στις κτιριακές εγκαταστάσεις και στον εξοπλισμό του οργανισμού

(ι) Επιβολή αυστηρότερων κυρώσεων

(κ) Κατάργηση Γνωστοποιήσεων και Αδειών Διασύνδεσης / Διαβίβασης, όπως τις γνωρίζουμε σήμερα

(λ) Ευθύνη τόσο σε υπεύθυνους επεξεργασίας όσο και σε εκτελούντες την επεξεργασία

(μ) Αυστηρές προϋποθέσεις για τη συγκατάθεση: καταργείται η σιωπηρή συγκατάθεση για την επεξεργασία δεδομένων και εισάγονται συγκεκριμένες υποχρεώσεις σχετικά με την απόδειξη ύπαρξης συγκατάθεσης

(ν) Καθιέρωση του θεσμού του Υπεύθυνου Προστασίας Δεδομένων

4

Πεδίο εφαρμογής

- Στο έδαφος της Κυπριακής Δημοκρατίας
- Όταν εφαρμόζεται το κυπριακό δίκαιο δυνάμει διεθνούς δικαίου
- Διασυνοριακές υποθέσεις που αφορούν πρόσωπα σε περισσότερα κράτη μέλη (συνδεδεμένες εταιρείες)
- Σε επεξεργασία εκτός ΕΕ για υποκείμενα που βρίσκονται εντός ΕΕ π.χ. US Airlines, ταξιδιωτικό γραφείο σε τρίτη χώρα που συλλέγει δεδομένα πολιτών Ε.Ε.
- Σε επεξεργασία που εκτελείται στην ΕΕ για υποκείμενα που βρίσκονται εκτός ΕΕ
- **Κύρια εγκατάσταση:** ορίζεται, όταν μια εταιρεία έχει εγκαταστάσεις σε πολλά κράτη μέλη
- ❖ **Για υπεύθυνο επεξεργασίας:** κύρια εγκατάσταση = η εγκατάσταση όπου λαμβάνονται οι αποφάσεις
- ❖ **Για εκτελών την επεξεργασία:** κύρια εγκατάσταση = η εγκατάσταση όπου εκτελείται η επεξεργασία

5

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 απόδειξη συμμόρφωσης**

Τα μέτρα αυτά επανεξετάζονται και επικαιροποιούνται κάθε 3 χρόνια ή όταν αυξάνεται ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των ατόμων *(κατευθυντήριες γραμμές της Ομάδας Εργασίας του Άρθρου 29)*

- **Αρχή της νομιμότητας:** νόμιμη, θεμιτή και διαφανής επεξεργασία

6

- **Αρχή του περιορισμού του σκοπού:**

- ❖ **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, **εφόσον πληρούνται οι προϋποθέσεις του άρθρου 89**
- ❖ Άρθρο 89: υιοθέτηση τεχνικών και οργανωτικών μέτρων, π.χ. ψευδωνυμοποίηση ούτως ώστε να μην ταυτοποιούνται τα υποκείμενα, δεδομένου ότι, οι εν λόγω σκοποί μπορούν να εκπληρωθούν με τον τρόπο αυτό
- **Αρχή της ελαχιστοποίησης των δεδομένων:**
 - ❖ Τα δεδομένα που τυγχάνουν επεξεργασίας είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους έχουν αρχικά συλλεγεί
 - Σύμφωνα με τους Κανονισμούς περί Ξενοδοχείων και Τουριστικών Καταλυμάτων, κάθε ξενοδοχείο τηρεί ειδικό έντυπο / βιβλίο **στο οποίο υποχρεωτικά καταχωρείται το όνομα, η διεύθυνση, η εθνικότητα, το επάγγελμα και η ημέρα άφιξης και αναχώρησης των πελατών**

7

- **Αρχή της ακρίβειας:**

Λαμβάνονται μέτρα που διασφαλίζουν ότι τα προσωπικά δεδομένα είναι ακριβή, διαγράφονται ή διορθώνονται χωρίς καθυστέρηση

- **Αρχή του περιορισμού της περιόδου αποθήκευσης:**

Τα δεδομένα διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των ατόμων μόνο για το διάστημα που απαιτείται για την πραγματοποίηση του σκοπού. Για μεγαλύτερα χρονικά διαστήματα: για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, με τη λήψη κατάλληλων μέτρων

- **Αρχή της ακεραιότητας και εμπιστευτικότητας:**

Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια τους

8

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 (ανθρωπιστικοί σκοποί π.χ. επιδημίες, ανταπόκριση σε καταστροφές)
- Για δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας
- Για το έννομο συμφέρον του οργανισμού ή του τρίτου

9

Πότε είναι νόμιμη η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων

❖ Κατά κανόνα απαγορεύεται η επεξεργασία τους

❖ **Επιτρέπεται όταν:**

(α) **υπάρχει συγκατάθεση**

- το άτομο την δίνει ελεύθερα
- είναι σε θέση να επιλέξει
- δεν διατρέχει τον κίνδυνο εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν συγκατατεθεί
- Ο υπεύθυνος επεξεργασίας **πρέπει να αποδείξει** ότι το άτομο έδωσε τη συγκατάθεσή του
- Μπορεί να ανακληθεί ανά πάσα στιγμή

10

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

(γ) αφορά σε ζωτικό συμφέρον

(δ) αφορά σε 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) αφορά σε δεδομένα που έχουν δημοσιοποιηθεί από το άτομο

(στ) αφορά σε θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων

(ζ) αφορά σε λόγους ουσιαστικού δημόσιου συμφέροντος

11

(η) αφορά σε 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) αφορά σε λόγους δημόσιου συμφέροντος: π.χ. δημόσια υγεία, διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και φαρμάκων ή των ιατροτεχνολογικών προϊόντων

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

12

Ενδυνάμωση υφιστάμενων δικαιωμάτων των πολιτών και εισαγωγή νέων

- **Δικαίωμα ενημέρωσης**

Η ενημέρωση πρέπει να γίνεται σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά

- ❖ Αυστηρότερες προϋποθέσεις για παροχή συγκατάθεσης τόσο σε ενήλικους (άρθρα 6, 7) όσο και σε παιδιά (άρθρο 8)

13

- **Δικαίωμα πρόσβασης**

- ❖ Το υποκείμενο δικαιούται να λάβει ατελώς, σε έντυπη ή ηλεκτρονική μορφή, πληροφορίες που αφορούν στην υγεία του, **τις οποίες το ίδιο ή άλλο πρόσωπο** έδωσε στον υπεύθυνο επεξεργασίας

– **Καταργείται το τέλος των €17**

- ❖ Έντυπη ή ηλεκτρονική μορφή

- Πληροφορίες για αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ
- Δικαίωμα παροχής αντιγράφου, νοούμενου ότι δεν επηρεάζει δυσμενώς τα δικαιώματα άλλων προσώπων

- **Δικαίωμα διόρθωσης**

Το άτομο έχει δικαίωμα διόρθωσης στα ανακριβή προσωπικά του δεδομένα, χωρίς αδικαιολόγητη καθυστέρηση

14

- **Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)**

- Το υποκείμενο έχει δικαίωμα διαγραφής δεδομένων υγείας που τον αφορούν όταν, μεταξύ άλλων, **ανακαλέσει τη συγκατάθεση του** για την επεξεργασία των εν λόγω δεδομένων και δεν υπάρχει άλλη νομική βάση για την επεξεργασία
- **Δεν μπορεί να ασκηθεί το δικαίωμα** όταν η επεξεργασία είναι απαραίτητη, μεταξύ άλλων:
 - ❖ για σκοπούς δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας
 - ❖ για σκοπούς **αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς**

15

- **Δικαίωμα στη φορητότητα των δεδομένων**

- Είναι το δικαίωμα του υποκειμένου των δεδομένων να λαμβάνει ένα υποσύνολο των προσωπικών δεδομένων που το αφορούν και έχουν υποβληθεί σε επεξεργασία από υπεύθυνο επεξεργασίας, σε ψηφιακή μορφή (σε μορφή αναγνώσιμη, τόσο από τον άνθρωπο όσο και από το μηχανογραφημένο σύστημα του άλλου οργανισμού) και να αποθηκεύει τα δεδομένα αυτά για περαιτέρω προσωπική χρήση
- Η αποθήκευση μπορεί να γίνεται σε ιδιωτική συσκευή ή ιδιωτικό υπολογιστικό σύννεφο, χωρίς, κατ' ανάγκη, διαβίβαση των δεδομένων σε άλλο υπεύθυνο επεξεργασίας

16

- **Δικαίωμα εναντίωσης**

Το υποκείμενο έχει δικαίωμα να αντιταχθεί / εναντιωθεί όταν προσωπικά του δεδομένα υφίστανται επεξεργασία για σκοπούς **επιστημονικής** ή ιστορικής **έρευνας** ή για στατιστικούς σκοπούς, εκτός εάν η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος

Παράδειγμα: Ξενοδοχείο έχει έννομο συμφέρον να διατηρεί προσωπικά δεδομένα πελατών του για στατιστικούς σκοπούς. Σε τέτοια περίπτωση πρώην πελάτης έχει δικαίωμα να εναντιωθεί

17

- **Δικαίωμα αντίρρησης σε αυτοματοποιημένη απόφαση περιλαμβανομένης της κατάρτισης προφίλ**

- Το υποκείμενο των δεδομένων έχει δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται με αυτοματοποιημένα μέσα, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία το επηρεάζει σημαντικά
- Ισχύει και για απόφαση που λαμβάνεται με μη αυτοματοποιημένα μέσα (Κατευθυντήριες Γραμμές Άρθρου 29)

18

Αυστηρότητες Υποχρεώσεις Υπεύθυνων Επεξεργασίας

1. Λήψη συγκατάθεσης για ανήλικους κάτω των 16 σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών

Για ανήλικους κάτω των 16 ετών δεν αρκεί η συγκατάθεση τους για την επεξεργασία προσωπικών τους δεδομένων αλλά χρειάζεται και η συγκατάθεση του γονέα / κηδεμόνα τους

2. Φέρει το βάρος της αποδείξεως όσον αφορά στην παροχή συγκατάθεσης

- Καταργείται η σιωπηρή συγκατάθεση
- Δήλωση συγκατάθεσης: σε απλή και κατανοητή γλώσσα
- Απόδειξη λήψης συγκατάθεσης

19

3. Υποχρέωση κατασκευαστών στο στάδιο του σχεδιασμού και εξ' ορισμού

Εφαρμογή τεχνικών και οργανωτικών μέτρων, π.χ. ψευδωνυμοποίηση ή ελαχιστοποίηση των δεδομένων, κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας και κατά τη στιγμή της επεξεργασίας που διασφαλίζουν ότι εξ ορισμού:

(α) υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας και (β) τα δεδομένα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων

4. Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας

Ο υπεύθυνος επεξεργασίας σε περίπτωση παραβίασης προσωπικών δεδομένων γνωστοποιεί αμέσως και όχι περὶ των **72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος, την παραβίαση στην ΑΠΔΠΧ, εκτός αν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο. Μετά τις 72 ώρες, λογοδοτεί στην ΑΠΔΠΧ

20

5. Υποχρέωση ανακοίνωσης παραβιάσεων ασφάλειας

- Η παραβίαση δεδομένων ανακοινώνεται αμέσως στο επηρεαζόμενο άτομο όταν υπάρχει ψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες του
- Περιγράφεται η φύση της παραβίασης και τα ληφθέντα μέτρα
- Η ανακοίνωση δεν απαιτείται, εάν:
 - (α) είχαν ήδη εφαρμοστεί κατάλληλα μέτρα προστασίας στα δεδομένα που αφορά η παραβίαση όπως π.χ. κρυπτογράφηση
 - (β) λήφθηκαν στη συνέχεια μέτρα που διασφαλίζουν ότι δεν υπάρχει κίνδυνος πλέον
 - (γ) προϋποθέτει δυσανάλογες προσπάθειες (γίνεται όμως δημόσια ανακοίνωση ή παρόμοιο μέτρο για ενημέρωση των επηρεαζόμενων προσώπων)

21

6. Υποχρέωση εκπροσώπησης υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ε.Ε.

- Υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία που ΔΕΝ είναι εγκατεστημένος στην ΕΕ ορίζει γραπτώς εκπρόσωπο του στην ΕΕ, που ενεργεί κατ' εντολή του υπεύθυνου/ εκτελούντα
- Ο εκπρόσωπος ενεργεί ως σημείο επαφής με την ΑΠΔΠΧ και με υποκείμενα των δεδομένων (one stop shop)
- Ο εκπρόσωπος εγκαθίσταται σε ΚΜ όπου βρίσκονται τα υποκείμενα των δεδομένων, των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία σε σχέση με προσφορά αγαθών ή υπηρεσιών ή των οποίων η συμπεριφορά παρακολουθείται

22

7. Υποχρέωση δέσμευσης του εκτελούντα την επεξεργασία με σύμβαση ή άλλη δεσμευτική πράξη

- Συνάπτεται συμφωνία/σύμβαση μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντα, η οποία καθορίζει τις υποχρεώσεις/ευθύνες του
- Ο εκτελών επεξεργάζεται τα δεδομένα μόνο βάσει καταγεγραμμένων εντολών του υπεύθυνου
- Θέτει στη διάθεση του υπεύθυνου κάθε απαραίτητη πληροφορία
- **Ο εκτελών:**
 - Τηρεί αρχείο καταγραφής δραστηριοτήτων επεξεργασίας
 - Συνεργάζεται με την ΑΠΔΠΧ
 - Λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της επεξεργασίας
 - Ενημερώνει τον υπεύθυνο επεξεργασίας σε περίπτωση παραβίασης
 - Διορίζει ΥΠΔ
 - Υπόκειται στον έλεγχο της εποπτικής αρχής και κυρώσεις

23

Παραδείγματα:

- ❖ Σύναψη συμφωνίας/σύμβασης μεταξύ τουριστικού/ταξιδιωτικού γραφείου και τρίτων, π.χ. ξενοδοχείων σε τρίτες χώρες, ξεναγών, συνοδών
- ❖ Σύναψη συμφωνίας/σύμβασης μεταξύ ξενοδοχείου και λογιστικού γραφείου που διαχειρίζεται το payroll των υπαλλήλων και τα έσοδα/έξοδα του

ΕΠΙΠΛΕΟΝ:

Τα τουριστικά/ταξιδιωτικά γραφεία στην Κύπρο οφείλουν να λάβουν την Άδεια της Επιτρόπου για να μπορούν να διαβιβάζουν δεδομένα των πελατών τους σε τρίτη χώρα

24

8. Τήρηση αρχείων των δραστηριοτήτων επεξεργασίας

- Ο υπεύθυνος επεξεργασίας και ο εκτελών **έχουν υποχρέωση να τηρούν εγγράφως ή ηλεκτρονικά** αρχείο δραστηριοτήτων
- Οι πληροφορίες στο εν λόγω αρχείο είναι αντίστοιχες με αυτές που περιλαμβάνει το υφιστάμενο έντυπο Γνωστοποίησης
- Το αρχείο τίθεται στη διάθεση της ΑΠΔΠΧ κατόπιν αιτήματος της για άσκηση των αρμοδιοτήτων της

ΠΑΡΑΔΕΙΓΜΑΤΑ

- Τα τουριστικά/ταξιδιωτικά γραφεία και ξενοδοχεία οφείλουν να τηρούν αρχείο δραστηριοτήτων για τους πελάτες τους αφού:
 - διενεργούν συνεχή επεξεργασία (*ΌΧΙ περιστασιακή*)
 - τα ξενοδοχεία επεξεργάζονται ειδικές κατηγορίες δεδομένων (*εθνικότητα*)

25

9. Υποχρέωση τήρησης της ασφάλειας της επεξεργασίας:

- Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία αξιολογεί τους κινδύνους της επεξεργασίας και εφαρμόζει μέτρα για τον μετριασμό τους π.χ. μέσω κρυπτογράφησης
- Γίνεται εκτίμηση του ενδεχόμενου επιπέδου ασφαλείας, λαμβάνοντας υπόψη τους κινδύνους που απορρέουν από την επεξεργασία (π.χ. από παράνομη καταστροφή, απώλεια, πρόσβαση στον εξυπηρετητή από hackers, κλοπή εγγράφων, διαρροή δεδομένων κ.λ.π.)
- Η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης είναι στοιχείο συμμόρφωσης

Παράδειγμα:

Τον Φεβρουάριο του 2017, κλάπηκαν προσωπικά δεδομένα 43.000 ατόμων λόγω παράνομης πρόσβασης από hackers στο σύστημα του Συνδέσμου Βρετανών Ταξιδιωτικών Πρακτόρων (Association of British Travel Agents)

26

10. Διενέργεια Εκτίμησης Αντικτύπου:

- Δεν απαιτείται σε κάθε πράξη επεξεργασίας **αλλά μόνο όταν υπάρχει υψηλός κίνδυνος (ιδίως με τη χρήση νέων τεχνολογιών) για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων** (περιλαμβανομένων και επεξεργασιών πριν τις 25.05.2018, δεδομένου ότι, ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων)

Π.χ. χρησιμοποιείται πλέον μια νέα τεχνολογία ή επειδή τα προσωπικά δεδομένα χρησιμοποιούνται για διαφορετικό σκοπό

- Διενεργείται πριν από την επεξεργασία (**δηλ. στο σχεδιασμό της πράξης επεξεργασίας**) και ενημερώνεται κάθε φορά που αλλάζει ο κίνδυνος ή κάθε 3 χρόνια

- **Κριτήρια υπολογισμού «υψηλού κινδύνου»:**

- αξιολόγηση προσωπικών πτυχών
- διαβιβάσεις
- μεγάλη κλίμακα (αρ. υποκειμένων, όγκος δεδομένων, διάρκεια, γεωγραφική έκταση, ευαίσθητα δεδομένα, διασύνδεση αρχείων κ.α.)²⁷

Η εκτίμηση αντικτύπου απαιτείται ιδίως:

- (α) για συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών που βασίζεται σε αυτοματοποιημένη επεξεργασία και προφίλ
- (β) για μεγάλη κλίμακα επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα
- (γ) για συστηματική παρακολούθηση δημόσιων χώρων

Παραδείγματα:

- Τα τουριστικά/ταξιδιωτικά γραφεία και ξενοδοχεία διενεργούν επεξεργασία σε μεγάλη κλίμακα (αρ. υποκειμένων, όγκος δεδομένων)
 - Επιπλέον, τα ξενοδοχεία συλλέγουν την εθνικότητα των πελατών τους (ειδική κατηγορία δεδομένων) σε μεγάλη κλίμακα (Κ.Δ.Π. 192/85 – Καν. 64)

Τι περιλαμβάνει η Εκτίμηση Αντικτύπου



29

11. Υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ):

- ΥΠΔ διορίζεται υποχρεωτικά:
- ❖ Όταν η επεξεργασία εκτελείται από δημόσια αρχή (συμπεριλαμβανομένων των νομικών προσώπων δημοσίου δικαίου)
- ❖ Όταν οι βασικές δραστηριότητες επεξεργασίας απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα (π.χ. τουριστικά / ταξιδιωτικά γραφεία) ή μεγάλης κλίμακας επεξεργασίας ειδικών κατηγοριών δεδομένων (π.χ. ξενοδοχεία)

30

12. Τήρηση κώδικα δεοντολογίας:

- Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπεύθυνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν υφιστάμενους

π.χ. ΠΑΣΥΞΕ, Σύνδεσμος Ταξιδιωτικών Πρακτόρων Κύπρου

- Η τήρηση του κώδικα είναι εθελοντική
- Το σχέδιο κώδικα δεοντολογίας υποβάλλεται στο Γραφείο μου για απόψεις και τελική έγκριση. Όταν εγκριθεί, το Γραφείο μου τον δημοσιεύει

31

13. Πιστοποίηση:

- Εάν επιθυμεί, ο υπεύθυνος επεξεργασίας / εκτελών την επεξεργασία θεσπίζει μηχανισμούς πιστοποίησης της προστασίας δεδομένων με σκοπό την απόδειξη συμμόρφωσης με τον Κανονισμό
- Μπορεί να είναι σφραγίδα ή σήμα προστασίας

32

14. Διαβιβάσεις σε τρίτες χώρες – διεθνείς οργανισμούς

Επιτρέπεται η διαβίβαση με Άδεια της ΑΠΔΠΧ:

- Εάν ο Οργανισμός επιλέξει ως νομική βάση για τη διαβίβαση συμβατικές ρήτρες που θα ετοιμάσει **και θα εγκριθούν από την ΑΠΔΠΧ**

Εάν από τη διαβίβαση επηρεάζονται και 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 ουσιαστικά σημαντικό αριθμό υποκειμένων των δεδομένων σε περισσότερα κμ.*

33

- **Επιτρέπεται η διαβίβαση χωρίς Άδεια** όταν τρίτη χώρα:
 - Εξασφαλίζει ικανοποιητικό επίπεδο προστασίας (με Απόφαση της Ευρωπαϊκής Επιτροπής)
 - Δεν εξασφαλίζει μεν ικανοποιητικό επίπεδο προστασίας αλλά υπάρχουν επαρκείς εγγυήσεις:
 - (α) νομικά δεσμευτικό μέσο μεταξύ δημόσιων αρχών π.χ. πολυμερής συμφωνία, FATCA ή
 - (β) δεσμευτικούς εταιρικούς κανόνες (για ομίλους επιχειρήσεων) **που εγκρίνονται από την αρμόδια εποπτική αρχή** ή
 - (γ) τυποποιημένες ρήτρες που εκδίδονται από την Επιτροπή ή
 - (δ) τυποποιημένες ρήτρες που **εκδίδονται από το Γραφείο μου και εγκρίνονται από την Επιτροπή** ή
 - (ε) κώδικα δεοντολογίας, **ο οποίος εγκρίνεται από το Γραφείο μου** ή από το Συμβούλιο Προστασίας Δεδομένων, εάν αφορά διάφορα κμ
 - (στ) μηχανισμό πιστοποίησης, **ο οποίος εγκρίνεται από το Γραφείο μου** ή τον εθνικό οργανισμό πιστοποίησης ή και από τους δύο

34

- **ΔΕΝ** εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, **ΔΕΝ** υπάρχουν επαρκείς εγγυήσεις, αλλά πληρούνται συγκεκριμένες προϋποθέσεις
Π.χ. για λόγους δημοσίου συμφέροντος, για άσκηση νομικών αξιώσεων, για προστασία ζωτικού συμφέροντος κλπ

ΣΗΜ: Όταν η διαβίβαση ελλοχεύει κινδύνους για τα υποκείμενα των δεδομένων, ο Οργανισμός διενεργεί εκτίμηση αντικτύπου και αν δεν υπάρχουν μέτρα μετριασμού του κινδύνου ή αν τα προβλεπόμενα μέτρα δεν μετριάζουν τον κίνδυνο επαρκώς, ο οργανισμός διαβουλεύεται τη διαβίβαση με την ΑΠΔΠΧ

35

Διοικητικά πρόστιμα

- Αυστηρότατα πρόστιμα, **με ανώτατο όριο: €10.000.000 ή 2% του παγκόσμιου κύκλου εργασιών** για παραβιάσεις που αφορούν, μεταξύ άλλων:
 - ❖ στις υποχρεώσεις σχετικά με την συγκατάθεση ανηλίκων
 - ❖ στις υποχρεώσεις του υπεύθυνου επεξεργασίας σχετικά με την εκτέλεση καθηκόντων του ΥΠΔ
 - ❖ στην προστασία των προσωπικών δεδομένων από τον σχεδιασμό και εξ ορισμού
- **Το ανώτατο όριο είναι €20.000.000 ή 4% του παγκόσμιου κύκλου εργασιών** για παραβιάσεις των υποχρεώσεων που σχετίζονται, μεταξύ άλλων:
 - ❖ με τις βασικές αρχές επεξεργασίας
 - ❖ τα δικαιώματα των φυσικών προσώπων
 - ❖ την μη παροχή πρόσβασης στην ΑΠΔΠΧ, προκειμένου να είναι σε θέση να ασκήσει τις εποπτικές της αρμοδιότητες,

36

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 4 χρόνια)*

37

Εξουσίες Επιτρόπου (Άρθρο 58)

➤ Εισάγονται αυξημένες εξουσίες

π.χ.

- Εγκρίνει πιστοποιητικά και κριτήρια πιστοποίησης
- Προβαίνει σε επανεξέταση των πιστοποιήσεων
- Παρέχει διαπίστευση σε φορείς πιστοποίησης
- Εκδίδει γνώμες για σχέδια κωδίκων δεοντολογίας και τα εγκρίνει
- Εγκρίνει δεσμευτικούς εταιρικούς κανόνες
- Εγκρίνει τυποποιημένες ρήτρες

➤ Επιβάλλει αυξημένα διοικητικά πρόστιμα (Άρθρο 83)

38

Άλλα σημαντικά θέματα και ορθές πρακτικές που αφορούν στα Τουριστικά/Ταξιδιωτικά Γραφεία / Ξενοδοχεία

39

Συγκατάθεση

- ❖ Η συλλογή πληροφοριών πελατών για την πραγματοποίηση μιας κράτησης είναι απαραίτητο στοιχείο της παροχής της υπηρεσίας και δεν απαιτεί περαιτέρω λήψη συγκατάθεσης
- ❖ **Απαιτείται η λήψη ξεχωριστής, ρητής συγκατάθεσης από τους πελάτες όταν τα δεδομένα θα χρησιμοποιηθούν για διαφορετικό σκοπό από τον αρχικό. Παραδείγματα:**
 - (α) προώθηση προϊόντων και υπηρεσιών
 - (β) ενημερωτικά δελτία / προσφορές
 - (γ) αποστολή ευχετήριας κάρτας μέσω ταχυδρομείου ή αποστολή ευχετήριου ηλεκτρονικού μηνύματος
 - (δ) έρευνα
 - (ε) στατιστικούς σκοπούς
 - (στ) ταξιδιωτικές συμβουλές
- Το έντυπο συγκατάθεσης που δίνεται στους πελάτες, πρέπει να περιλαμβάνει ξεχωριστά τετραγωνίδια για κάθε τύπο συγκατάθεσης

40

Επεξεργασία αρ. δελτίου ταυτότητας πελατών και υπαλλήλων

- ❖ Τα ξενοδοχεία και τα τουριστικά/ταξιδιωτικά γραφεία δικαιούνται να συλλέγουν τον αρ. δελτίου ταυτότητας / διαβατηρίου των πελατών και υπαλλήλων τους αλλά **ΔΕΝ** δικαιούνται να φωτοτυπούν/διατηρούν αντίγραφο τους
- ❖ Οι περί Ξενοδοχείων και Τουριστικών Καταλυμάτων Κανονισμοί του 1985 (Καν. 64) προβλέπουν **ότι ο πελάτης «παραδίδει το διαβατήριό του εφόσον του ζητηθεί από τον ξενοδόχο»**

41

Παροχή αντιγράφων συμβολαίων Ξενοδόχο-υπαλλήλων σε Επιθεωρητές του Υπουργείου Εργασίας, Πρόνοιας και Κοινωνικών Ασφαλίσεων

Είναι υποχρέωση των μελών του ΠΑΣΥΞΕ να παρέχουν σε Επιθεωρητές των ΥΚΑ αντίγραφα των συμβολαίων των υπαλλήλων τους βάσει του άρθρου 70 του περί Κοινωνικών Ασφαλίσεων Νόμου του 2010

42

Ηχογράφηση τηλεφωνικών συνδιαλέξεων

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

43

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

44

Εγκατάσταση Κλειστού Κυκλώματος Βιντεοπαρακολούθησης (ΚΚΒΠ)

- Επιτρέπεται μόνο αν δεν υπάρχει λιγότερο παρεμβατικός τρόπος για την πραγματοποίηση του σκοπού π.χ. για προστασία του χώρου από διαρρήξεις και κλοπές.
- **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

45

➤ 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
 - διαδρόμους που οδηγούν στα δωμάτια του ξενοδοχείου
 - εισόδους των κατ' ιδίαν δωματίων
 - τουαλέτες
 - χώροι όπου πραγματοποιούνται δραστηριότητες αναψυχής (όπως πισίνες, γυμναστήρια, χώροι άθλησης, αποδυτήρια κλπ.)
 - παιδότοποι
 - μέσα στο ασανσέρ
 - εξωτερικές κάμερες που λαμβάνουν εικόνες από χώρους εκτός του ξενοδοχείου π.χ. 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)

46

- Απαραίτητη η σήμανση με ευδιάκριτα γράμματα για ενημέρωση των πελατών πριν από την είσοδό τους στο ξενοδοχείο / τουριστικό γραφείο ή σε κάθε όροφο
- Οι υπάλληλοι ενημερώνονται μέσω εγκυκλίου
- Δεν επιτρέπεται η μυστική παρακολούθηση

47

Εγκατάσταση συστημάτων δακτυλικών αποτυπωμάτων για σκοπούς ελέγχου της ώρας προσέλευσης/ αναχώρησης των υπαλλήλων από την εργασία

(Το Γραφείο μου ενημερώθηκε από διάφορα ξενοδοχεία για την πρόθεση τους να εγκαταστήσουν τέτοιο σύστημα ή για το σύστημα που έχουν ήδη προβεί – το θέμα παρακολουθείται)

- **Είναι βιομετρικό δεδομένο:** καθολικό, μοναδικό, μόνιμο δεδομένο όπως είναι φωτογραφία, DNA, ίριδα, παλάμη, φωνή κτλ
- **Επιτρέπεται ΜΟΝΟ** σε κτίρια υψίστης ασφάλειας και χώρους με ιδιαίτερες απαιτήσεις ασφαλείας και εφόσον δεν υπάρχει άλλο λιγότερο επαχθές μέσο για την επίτευξη των σκοπών ασφάλειας των εγκαταστάσεων / εξοπλισμού / προσώπων (π.χ. στρατιωτικές /αμυντικές εγκαταστάσεις, εργαστήρια υψηλού κινδύνου, χώροι αεροδρομίων, κ.α)
- Ο υπεύθυνος επεξεργασίας 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

48

Ορθή χρήση αδειών ασθενείας και δεδομένων υγείας του προσωπικού

Νόμιμη επεξεργασία: Συγκατάθεση ή Άδεια Επιτρόπου

- Οι άδειες ασθενείας (περιλαμβάνουν ευαίσθητα δεδομένα) θα πρέπει να καταχωρούνται όχι στον προσωπικό φάκελο του υπαλλήλου αλλά να σε ξεχωριστό φάκελο που να ονομάζεται «Φάκελος Αδειών». Σε αυτόν, μπορούν επίσης να καταχωρούνται οι άδειες ανάπαυσης του
- Περιορισμένη πρόσβαση: μόνο από άτομα που έχουν επιλεγεί και εξουσιοδοτηθεί ειδικά από τον εργοδότη.
- Αν τα δεδομένα υγείας ενός εργοδοτούμενου πρόκειται να κοινοποιηθούν σε τρίτους, ο εργοδοτούμενος πρέπει να ενημερώνεται εκ των προτέρων για τους σκοπούς και τους αποδέκτες της κοινοποίησης

49

- Η επεξεργασία δεδομένων υγείας πρέπει να περιορίζεται στις περιπτώσεις όπου αυτή είναι απαραίτητη για να ικανοποιηθούν συγκεκριμένοι σκοποί όπως π.χ.:
- ❖ όταν η επεξεργασία είναι απαραίτητη για να κριθεί κατά πόσο ένας εργοδοτούμενος είναι ικανός να εκπληρώσει μία παρούσα ή μελλοντική εργασία
- ❖ όταν η επεξεργασία είναι απαραίτητη για σκοπούς πρόληψης και προστασίας της υγείας των εργοδοτούμενων στους χώρους εργασίας
- ❖ όταν η επεξεργασία είναι απαραίτητη, για να παρασχεθούν στον εργοδοτούμενο δικαιώματα ασθενείας ή κοινωνικών ασφαλίσεων
- ❖ όταν τα καθήκοντα της θέσης επιβάλλουν την υποβολή του εργοδοτούμενου σε συγκεκριμένους υγειονομικούς ή ιατρικούς ελέγχους

50

Διαγραφή / καταστροφή προσωπικών δεδομένων πελατών

- Τα δεδομένα θα πρέπει να διατηρούνται **μόνο κατά τη διάρκεια της περιόδου που απαιτείται** για την πραγματοποίηση των σκοπών της συλλογής /επεξεργασίας
- Μετά τη λήξη οποιασδήποτε οικονομικής διαφοράς, θα πρέπει να οριστεί χρονικό διάστημα διατήρησης των δεδομένων που διατηρούνται από ξενοδοχεία και τουριστικά/ταξιδιωτικά γραφεία **ιδιαίτερα όσον αφορά στον αριθμό πιστωτικής κάρτας, αριθμό ταυτότητας/διαβατηρίου και εθνικότητας**
- Εάν ο πελάτης συγκατατέθηκε για επεξεργασία προσωπικών του δεδομένων για άλλους σκοπούς π.χ. αποστολή ενημερωτικών προσφορών, θα πρέπει να διατηρούνται μόνο τα απολύτως απαραίτητα στοιχεία π.χ. ονοματεπώνυμο, email, διεύθυνση αλληλογραφίας και αρ. τηλεφώνου

51

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

52