# 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)

## Εκπαίδευση νεοεισερχομένων στην ΔΥ

Ειρήνη Λοϊζίδου Νικολαΐδου
Επίτροπος Προστασίας
Δεδομένων Προσωπικού Χαρακτήρα

Μάρτιος 2020

# Νομικό Πλαίσιο

- Κυρωτικοί Νόμοι της Σύμβασης 108 και του Πρόσθετου Πρωτοκόλλου

- Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (Ν. 125(Ι)/2018)

- **Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, Γενικός Κανονισμός για την Προστασία Δεδομένων**

## Ανάγκη αντικατάστασης του υφιστάμενου πλαισίου:

Η υφιστάμενη Οδηγία (95/46/ΕΚ), μετά από περίπου μια εικοσαετία, θεωρήθηκε ξεπερασμένη - δεν ανταποκρίνόταν 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 και διάθεσής τους σε παγκόσμιο επίπεδο

# Προσωπικά δεδομένα

- **Απλά δεδομένα** – δεδομένα θέσης και επιγραμμικά (on line) αναγνωριστικά στοιχεία ταυτότητας τα οποία παρέχονται από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα τους και διευκολύνουν τον εντοπισμό του φυσικού προσώπου π.χ.

  IP address, εντοπισμός θέσης μέσω GPS)

- **Ειδικές κατηγορίες δεδομένων**

  **- γενετικά δεδομένα:** τα χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν και τα οποία παρέχουν μοναδικές πληροφορίες για το εν λόγω φυσικό πρόσωπο π.χ. DNA

  **- βιομετρικά δεδομένα:** τα δεδομένα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία, η οποία επιτρέπει ή επιβεβαιώνει την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου

  π.χ. φωτογραφία, δακτυλικά αποτυπώματα, ίριδα, παλάμη, φωνή κτλ)

# Υπεύθυνος επεξεργασίας

Η δημόσια αρχή που καθορίζει τους σκοπούς της συλλογής και επεξεργασίας των προσωπικών δεδομένων, τα μέσα για την επίτευξη

# Εκτελών την επεξεργασία

Το φυσικό πρόσωπο ή νομική οντότητα που επεξεργάζεται δεδομένα εκ μέρους και για λογαριασμό του Υπουργείου/ Τμήματος/Υπηρεσίας κ.λ.π.

(π.χ. εταιρεία που συνάπτει σύμβαση με δημόσια αρχή για παροχή υπηρεσιών πληροφορικής)

Η σχετική ανάθεση γίνεται ΓΡΑΠΤΩΣ

# 1. Τήρηση των Αρχών νόμιμης επεξεργασίας

- 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
- Αρχής της Λογοδοσίας

# 2. Υποχρεώσεις δημόσιας αρχής/ τμήματος/ υπηρεσίας

- **Ενισχυμένη ασφάλεια και εφαρμογή πολιτικών ασφάλειας** π.χ. ψευδωνυμοποίηση και κρυπτογράφηση

- **Διενέργεια εκτίμησης αντικτύπου:** εκτίμηση των σχεδιαζόμενων πράξεων, για επεξεργασίες που παρουσιάζουν υψηλό κίνδυνο, σχετίζονται με αξιολόγηση προσωπικών πτυχών και αφορούν δεδομένα μεγάλης κλίμακας

- **Τήρηση αρχείου δραστηριοτήτων:**
  - Στην ιστοσελίδα του Γραφείου μου υπάρχει αναρτημένο «Δείγμα αρχείου δραστηριοτήτων», σύμφωνα με το άρθρο 30 του Κανονισμού, σε μορφή Πίνακα καθώς και Οδηγός για τη συμπλήρωσή του

- **Ορισμός Υπεύθυνου Προστασίας Δεδομένων:**
  - Αναλαμβάνει το ρόλο του θεματοφύλακα των προσωπικών δεδομένων
  - Διαθέτει επιστημονικές γνώσεις
  - Θα μπορεί να προλαμβάνει περιπτώσεις παραβίασης προσωπικών δεδομένων
  - Παρακολουθεί γενικά τη συμμόρφωση με τον Κανονισμό και έχει συμβουλευτικό ρόλο

**Τονίζεται ότι:**

- **Ο Κανονισμός δεν θέτει οποιαδήποτε νομική υποχρέωση για πιστοποίηση του ΥΠΔ, ούτε και οι σχετικές Κατευθυντήριες Γραμμές της Ομάδας Εργασίας Άρθρου 29** (Συμβουλευτικό όργανο της ΕΕ για θέματα προστασίας προσωπικών δεδομένων) ενθαρρύνουν κάτι τέτοιο

- **Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας:**

  στην ιστοσελίδα του Γραφείου μου είναι αναρτημένο το έντυπο Γνωστοποίησης Περιστατικών Παραβίασης Προσωπικών Δεδομένων

- **Υποχρέωση ανακοίνωσης παραβιάσεων ασφάλειας**

- **Επιλογή εκτελούντων την επεξεργασία** που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων

## 3. Δικαιώματα

- 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

# Διοικητικά πρόστιμα

- Αυστηρότατα πρόστιμα, με ανώτατο όριο: €10.000.000 ή 2% του παγκόσμιου κύκλου εργασιών για παραβιάσεις που αφορούν, μεταξύ άλλων:
  - στις υποχρεώσεις του υπεύθυνου επεξεργασίας σχετικά με την εκτέλεση καθηκόντων του Υπεύθυνου Προστασίας Δεδομένων

- 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 Αρχή Προστασίας Προσωπικών Δεδομένων, προκειμένου να είναι σε θέση να ασκήσει τις εποπτικές της αρμοδιότητες

# Θέματα που ενδιαφέρουν

# Παροχή πρόσβασης

Το Υπουργείο/Τμήμα/Υπηρεσία οφείλει να ικανοποιεί τα γραπτά αιτήματα πρόσβασης των υποκειμένων των δεδομένων *(π.χ. υπαλλήλων, πολιτών)* στα προσωπικά τους δεδομένα τα οποία περιλαμβάνονται σε έντυπα αρχεία ή ηλεκτρονικές βάσεις δεδομένων

- Δεν πληρώνεται οποιοδήποτε τέλος για άσκηση του δικαιώματος πρόσβασης
- Δικαίωμα παροχής αντιγράφου, νοουμένου ότι δεν επηρεάζει δυσμενώς τα δικαιώματα άλλων προσώπων *(δεν πληρώνεται οποιοδήποτε τέλος εκτός εάν το αίτημα είναι επαναλαμβανόμενο, ο υπεύθυνος επεξεργασίας μπορεί να ζητήσει τέλος για διοικητικά έξοδα)*

# Δικαίωμα πρόσβασης από υποψήφιους για πρόσληψη στο δημόσιο

- Οι υποψήφιοι που παρακάθησαν σε εξετάσεις που οργανώνονται από τη Δημόσια Υπηρεσία έχουν δικαίωμα να ζητούν και να λαμβάνουν πληροφορίες ως προς όλα τα προσωπικά δεδομένα που τους αφορούν, όπως το γραπτό τους, την κατάταξη και τη βαθμολογία τους

- **Απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), ημερ. 20.12.2017 στην υπόθεση C-434/16 Peter Nowak κατά Data Protection Commissioner:**
  - Οι γραπτές απαντήσεις και οι διορθώσεις του εξεταστή συνιστούν προσωπικά δεδομένα στα οποία ο υποψήφιος έχει δικαίωμα πρόσβασης
  - Το περιεχόμενο των διορθώσεων αποτελεί τη γνώμη ή την εκτίμηση του εξεταστή όσον αφορά στην επίδοση του εξεταζομένου

# Λήψη μέτρων για την ασφάλεια της επεξεργασίας

1. **Μέτρα Φυσικής ασφάλειας:** για προστασία από τυχαία/ αθέμιτη καταστροφή των δεδομένων

- **Έλεγχος φυσικής πρόσβασης:** π.χ ηλεκτρονικός εξοπλισμός και απόρρητα έγγραφα σε δωμάτια ασφαλείας με ελεγχόμενη και περιορισμένη πρόσβαση, φάκελοι σε φωριαμούς που κλειδώνουν και μηχανισμοί ελέγχου πρόσβασης
- **Ασφάλεια από φυσικές καταστροφές ή κακόβουλες πράξεις:** π.χ συστήματα συναγερμού και πυρανίχνευσης
- **Προστασία φορητών μέσων αποθήκευσης / Κλειδαριές ασφαλείας**
- **Καλή πρακτική:** τήρηση επικαιροποιημένου καταλόγου με τα δικαιώματα φυσικής πρόσβασης του προσωπικού *(ανάλογα με το επίπεδο πρόσβασής τους π.χ κωδικοί, κλειδιά,)*

## 2. Τεχνικά μέτρα ασφάλειας

**Έλεγχος πρόσβασης /Ασφάλεια συστημάτων**

- Antivirus /ασφάλεια επικοινωνιών και λογισμικού
- Firewalls
- Backups (να φυλάσσονται σε ασφαλές μέρος)
- Επίπεδα πρόσβασης (need-to-know basis)
- Αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας (audit trails / log files)
- Χρήση κρυπτογράφησης (ειδικές κατηγορίες δεδομένων)
- Απομακρυσμένη πρόσβαση (remote access) μέσω ασφαλών καναλιών και κρυπτογράφησης.

⇨ **Καλή πρακτική:** Να έχει προηγηθεί μελέτη για εκτίμηση κινδύνων και λήψη ανάλογων μέτρων ασφάλειας

# 3. Προσωπικό που εργοδοτείται σε Υπουργείο/Τμήμα/Υπηρεσία

- Προσόντα, τεχνικές γνώσεις, εκπαίδευση
- Απόρρητο της επεξεργασίας
- Πρόσβαση στα αρχεία – μόνο σε εξουσιοδοτημένο προσωπικό. Τα προσωπικά δεδομένα των πολιτών δεν διατίθενται σε αναρμόδια πρόσωπα / οργανισμούς π.χ. σε συγγενικά τους πρόσωπα
  - Απαγορευμένη διάδοση – έστω και σε φιλικό επίπεδο, μεταξύ συναδέλφων
  - Ετοιμασία γραπτής πολιτικής
  - Διενέργεια εσωτερικών ελέγχων

# 4. Ορθή χρήση αρχείου του προσωπικού

- Οι προσωπικοί φάκελοι των υπαλλήλων (που περιέχουν προσόντα και ατομικές εκθέσεις), θα πρέπει να διατηρούνται σε ασφαλές μέρος (σε χώρους που κλειδώνουν)

- Πρόσβαση στους προσωπικούς φακέλους να έχει μόνο εξουσιοδοτημένο προσωπικό

- Απαγορεύεται η διάδοση προσωπικών δεδομένων που αφορούν ένα υπάλληλο σε άλλο

# 5. Ορθή χρήση αδειών ασθενείας του προσωπικού

- Οι άδειες ασθενείας να μην καταχωρούνται στον προσωπικό φάκελο του υπαλλήλου αλλά να καταχωρούνται σε ένα ξεχωριστό φάκελο που να ονομάζεται «Φάκελος Αδειών». Σε αυτόν, μπορούν επίσης να καταχωρούνται οι άδειες ανάπαυσης του
- Περιορισμένη πρόσβαση: μόνο από άτομα που έχουν εξουσιοδοτηθεί 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

## Αναθεώρηση των εντύπων που δίνονται στα υποκείμενα με τα οποία ενημερώνονται για τις πληροφορίες που προβλέπονται στα άρθρα 13 και 14

**Για παράδειγμα:**

- ✓ στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων
- ✓ νομική βάση για την επεξεργασία
- ✓ χρονικό διάστημα διατήρησης των δεδομένων
- ✓ τα δικαιώματα που μπορούν να ασκήσουν
- ✓ δικαίωμα υποβολής παραπόνου στο Γραφείο μου
- ✓ σε περίπτωση που η συγκατάθεση είναι η νομική βάση της επεξεργασίας, να γνωρίζουν ότι μπορούν να την ανακαλέσουν ανά πάσα στιγμή
- ✓ σε περίπτωση συλλογής των δεδομένων, όχι από το ίδιο το υποκείμενο, την πηγή/προέλευση τους

## Εκπαίδευση και ευαισθητοποίηση του προσωπικού:

Όσοι επεξεργάζονται προσωπικά δεδομένα θα πρέπει να εκπαιδεύονται και ενημερώνονται για νέες νομοθεσίες και τεχνολογίες και να λαμβάνουν τα απαραίτητα μέτρα για ορθή και νόμιμη διαχείριση και επεξεργασία των προσωπικών δεδομένων. π.χ. πρέπει να γνωρίζουν πότε υπάρχει παραβίαση προσωπικών δεδομένων

# Εγκατάσταση και Λειτουργία Κ.Κ.Β.Π.

- Κατά κανόνα απαγορεύεται ενόψει της απουσίας νομοθετικής ρύθμισης
- Επιτρέπεται σε δημόσιους χώρους όταν το έννομο συμφέρον της δημόσιας αρχής 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:

- 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

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

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

- Δεν επιτρέπεται η μυστική παρακολούθηση

# Ανακοίνωση αποτελεσμάτων γραπτών εξετάσεων

Τα αποτελέσματα (βαθμολογία και σειρά κατάταξης) πρέπει να δημοσιεύονται για παράδειγμα με αρ. ταυτότητας ή αρ. κοινωνικών ασφαλίσεων (ΟΧΙ ονομαστικώς)

# Δεδομένα που πρέπει να περιλαμβάνονται σε έντυπο/αίτηση

- Μόνο αυτά που είναι **απαραίτητα** για το σκοπό που επιδιώκεται στη συγκεκριμένη περίπτωση.
- Π.χ. Στο Έντυπο Γεν. 6G (Αίτηση για διορισμό ή προαγωγή στη Δ.Υ.) αφαιρέθηκαν:

Διεύθυνση κατοικίας αιτητή, Άγαμος /έγγαμος κ.λ.π., Στοιχεία συζύγου (π.χ. όνομα, υπηκοότητα, επάγγελμα, ημερ. Γέννησης), Αριθμός και ηλικίες τέκνων ,Στοιχεία πατέρα και μητέρας (π.χ. όνομα, επάγγελμα, τόπος γέννησης, διεύθυνση, τηλ.), Φωτογραφία

# Ορθή τηλεξυπηρέτηση κοινού

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

## Αποστολή πληροφοριών (π.χ. μισθοδοτικών / συνταξιοδοτικών πληροφοριών) μέσω fax / ταχυδρομείου

Οι πληροφορίες θα πρέπει να αποστέλλονται μόνο στον αρ. φαξ ή στη διεύθυνση που έχει δηλώσει ο πολίτης **νοουμένου ότι έχει δηλώσει ότι επιθυμεί να στέλλονται οι πληροφορίες μέσω του συγκεκριμένου φαξ/διεύθυνσης**

# Αιτήματα δημοσιογράφων για παράθεση μισθοδοτικών/συνταξιοδοτικών στοιχείων κρατικών υπαλλήλων / αξιωματούχων

Τα δεδομένα που αφορούν μισθοδοσία / σύνταξη κρατικών υπαλλήλων / αξιωματούχων **και προβλέπονται στον Κρατικό Προϋπολογισμό**, μπορούν να δίνονται σε δημοσιογράφους

# Έλεγχος της ώρας προσέλευσης/αναχώρησης 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)*

- Η δημόσια αρχή 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

# 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**