Νέος Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 (εφεξής «ο Κανονισμός») - Προετοιμασία και Υποχρεώσεις Δημοσίων Αρχών -

<u>Δημόσιες Αρχές για τους σκοπούς του Κανονισμού:</u>

Θεωρούνται οι **Αρχές του Δημόσιου και ευρύτερου Δημόσιου τομέα** συμπεριλαμβανομένων *όλων των ανεξάρτητων Αρχών και των Αρχών τοπικής αυτοδιοίκησης, Δικαστικές Αρχές όταν δεν ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας και Βουλή των Αντιπροσώπων.*

1. Ποιος είναι ο υπεύθυνος επεξεργασίας:

Με βάση την ερμηνεία του όρου «υπεύθυνος επεξεργασίας» στο **άρθρο 4(7)** του Κανονισμού:

«7) «υπεύθυνος επεξεργασίας» είναι το φυσικό ή νομικό πρόσωπο, **η δημόσια αρχή,** η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους,».

Υπεύθυνος επεξεργασίας θεωρείται δηλαδή η νομική οντότητα (συλλογικό όργανο/ Υπουργείο/Τμήμα /Υπηρεσία/ Ανεξάρτητο Γραφείο) π.χ Η ΕΔΥ ως ανεξάρτητη στη Δημοκρατία Αρχή, συλλογικό όργανο και νομική οντότητα θεωρείται, για τους σκοπούς του οικείου Κανονισμού «υπεύθυνος επεξεργασίας» σχετικά με όλες τις επεξεργασίες σε αυτοματοποιημένη ή μη μορφή που εκτελούνται σε προσωπικά δεδομένα.

2. Όλες οι Δημόσιες Αρχές διενεργούν και /ή εκτελούν επεξεργασία προσωπικών δεδομένων:

Με βάση την ερμηνεία του όρου «επεξεργασία» στο **άρθρο 4(2)** του Κανονισμού:

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

3. Τι αλλάζει με το νέο Γενικό Κανονισμό:

Οι απορρέουσες, από τον ανωτέρω Κανονισμό, υποχρεώσεις, έκαστου υπεύθυνου επεξεργασίας είναι αρκετές, κοινό σημείο όλων είναι η προαγωγή της διαφάνειας, η ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων, η ενισχυμένη ασφάλεια των προσωπικών δεδομένων η εισαγωγή της αρχής της λογοδοσίας στην αρμόδια Εποπτική Αρχή (Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) με την έννοια της απόδειξης της συμμόρφωσης με τις πρόνοιες του Κανονισμού και οι ενισχυμένες και αποτρεπτικές διοικητικές κυρώσεις.

4. Προετοιμασία για τον Κανονισμό:

4.1 Ως σημείο εκκίνησης της διαδικασίας συμμόρφωσης με τον Κανονισμό για όλες τις Δημόσιες Αρχές είτε υπέχουν ιδιότητα υπεύθυνου επεξεργασίας είτε εκτελούντος την επεξεργασία είναι ο ορισμός υπεύθυνου προστασίας δεδομένων **(άρθρα 37, 38 και 39)** κύρια καθήκοντα του οποίου είναι να ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία κατά περίπτωση, να παρακολουθεί τη συμμόρφωση με τον παρόντα Κανονισμό, να συνεργάζεται και να ενεργεί ως σημείο επικοινωνίας με την εποπτική αρχή. Κατά την ενάσκηση των καθηκόντων του θα πρέπει να διασφαλίζεται η πλήρης ανεξαρτησία του καθώς και ότι δεν λαμβάνει εντολές, και λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή εκτελούντα την επεξεργασία, κατά περίπτωση.

4.2 Αρχείο δραστηριοτήτων (άρθρο 30 του Κανονισμού)

Το περιεχόμενο του αρχείου δραστηριοτήτων καθορίζουν οι διατάξεις του **άρθρου 30** του Κανονισμού. Στο αρχείο αυτό καταγράφονται επακριβώς οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα, που τυγχάνουν επεξεργασίας (συλλογή, καταχώριση, φύλαξη, διαβίβαση, κλπ.), από κάθε Δημόσια Αρχή είτε υπέχει θέση υπεύθυνου επεξεργασίας είτε εκτελούντος την επεξεργασία, καθώς επίσης και τα συστήματα αρχειοθέτησης (αρχεία) που τηρούνται. Το Γραφείο της ΕΠΔΠΧ,

ανήρτησε για σκοπούς διευκόλυνσης των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία αλλά και για σκοπούς ομοιόμορφου και ενιαίου ελέγχου των αρχείων αυτών, ολοκληρωμένο **δείγμα αρχείου δραστηριοτήτων σε μορφή excel** με λεπτομερή **Οδηγό συμπλήρωσης**. Το αρχείο αυτό συμπληρώνουν και διατηρούν στις εγκαταστάσεις τους οι υπεύθυνοι επεξεργασίας **σε έγγραφη και ηλεκτρονική μορφή**.

Το αρχείο τίθεται στη διάθεση της ΕΠΔΠΧ ύστερα από σχετικό αίτημά της.

4.3 Παραδείγματα Συστημάτων Αρχειοθέτησης και επεξεργασιών που διενεργούν Δημόσιες Αρχές με βάση τη νομοθεσία και την αποστολή τους: π.χ ΕΔΥ:

1. Αρχείο και επεξεργασία για σκοπούς πλήρωσης θέσεων στη Δημόσια Υπηρεσία. (υποψήφιοι για πρόσληψη / επιλεγέντες για διορισμό / μη επιλεγέντες για διορισμό).
2. Φάκελοι δικαστικού ελέγχου/προσφυγών για σκοπούς υπεράσπισης.
3. Φάκελοι για σκοπούς εκτέλεσης αποσπάσεων και μεταθέσεων.
4. Φάκελοι γνωματεύσεων, δικαστικών αποφάσεων και επανεξετάσεων.
5. Φάκελοι αδειών.
6. Προσωπικοί φάκελοι Δημοσίων Υπαλλήλων.
7. Φάκελοι Υπηρεσιακών Εκθέσεων Δημοσίων Υπαλλήλων.
8. Πειθαρχικοί Φάκελοι.
9. Φάκελοι καταγγελιών εναντίον Δημοσίων Υπαλλήλων (15.30.007).

4.4 Με το πέρας της καταγραφής και της συμπλήρωσης του αρχείου δραστηριοτήτων η Δημόσια Αρχή είτε υπό την ιδιότητά της ως υπεύθυνος επεξεργασίας είτε ως εκτελών την επεξεργασία θα πρέπει να είναι σε θέση να αποτιμήσει τα αποτελέσματα της καταγραφής και να προβεί σε προγραμματισμό όλων των απαραίτητων ενεργειών που απαιτούνται με σκοπό την καθολική συμμόρφωσή της με τις υποχρεώσεις του Κανονισμού ξεκινώντας από τις βασικές αρχές της επεξεργασίας προσωπικών δεδομένων, **άρθρο 5** του Κανονισμού.

4.5 Βασικές Αρχές της επεξεργασίας προσωπικών δεδομένων: η πεμπτουσία της προστασίας των προσωπικών δεδομένων (άρθρο 5)

(α) Νομιμότητα /Αντικειμενικότητα και Διαφάνεια.
(β) Περιορισμός του σκοπού και μη υποβολή σε περαιτέρω επεξεργασία ασύμβατη με τον αρχικό σκοπό της συλλογής.

(γ) Ελαχιστοποίηση των δεδομένων (συλλέγονται μόνο τα απολύτως απαραίτητα σε σχέση με τον επιδιωκόμενο σκοπό).
(δ) Ακρίβεια, επικαιροποίηση, διόρθωση ή διαγραφή ανακριβών προσωπικών δεδομένων.
(ε) Περιορισμός της περιόδου αποθήκευσης: επιτρεπτή η ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που εξυπηρετεί τους σκοπούς της επεξεργασίας.
(στ) Ακεραιότητα και εμπιστευτικότητα με τη λήψη όλων των κατάλληλων τεχνικών, οργανωτικών και μέτρων φυσικής ασφάλειας.

Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις ανωτέρω αρχές («**λογοδοσία**»).

4.6 Νομική βάση επεξεργασίας προσωπικών δεδομένων από Δημόσιες Αρχές:

Τηρουμένων των αρμοδιοτήτων και εξουσιών των Δημοσίων Αρχών όπως ενδεχομένως απονέμονται από το Σύνταγμα της Κυπριακής Δημοκρατίας, τις εθνικές, εναρμονιστικές, κυρωτικές νομοθεσίες, τις πρωτογενείς και τις συναφείς δευτερογενείς νομοθεσίες και την αποστολή τους οι Δημόσιες Αρχές προβαίνουν σε συλλογή και επεξεργασία (σε ηλεκτρονική και έντυπη μορφή) και διατήρηση συστημάτων αρχειοθέτησης (αρχεία) προσωπικών δεδομένων ήτοι των διοικούμενων, πολιτών, υπαλλήλων τους, αιτητών κ.α.

Η νομική βάση και /ή νομιμότητα των επεξεργασιών που εκτελούν Δημόσιες Αρχές θα πρέπει να αναζητείται κυρίως στα στοιχεία **(γ) ή (ε)** της **παρ.1** του **άρθρου 6** του Κανονισμού με βάση το οποίο:

«Άρθρο 6

Νομιμότητα της επεξεργασίας

1. Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Το στοιχείο στ) του πρώτου εδαφίου δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

2. Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν πιο ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού όσον αφορά την επεξεργασία για τη συμμόρφωση με την παράγραφο 1 στοιχεία γ) και ε), καθορίζοντας ακριβέστερα ειδικές απαιτήσεις για την επεξεργασία και άλλα μέτρα προς εξασφάλιση σύννομης και θεμιτής επεξεργασίας, μεταξύ άλλων για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX.

3. Η βάση για την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχεία γ) και ε) ορίζεται σύμφωνα με:

α) το δίκαιο της Ένωσης, ή

β) το δίκαιο του κράτους μέλος στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας.

Ο σκοπός της επεξεργασίας καθορίζεται στην εν λόγω νομική βάση ή, όσον αφορά την επεξεργασία που αναφέρεται στην παράγραφο ***1 στοιχείο ε), είναι η αναγκαιότητα της επεξεργασίας για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Η εν λόγω νομική βάση μπορεί να περιλαμβάνει ειδικές διατάξεις για την προσαρμογή της***

εφαρμογής των κανόνων του παρόντος κανονισμού, μεταξύ άλλων: τις γενικές προϋποθέσεις που διέπουν τη σύννομη επεξεργασία από τον υπεύθυνο επεξεργασίας· τα είδη των δεδομένων που υποβάλλονται σε επεξεργασία· τα οικεία υποκείμενα των δεδομένων· τις οντότητες στις οποίες μπορούν να κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα και τους σκοπούς αυτής της κοινοποίησης· τον περιορισμό του σκοπού· τις περιόδους αποθήκευσης· και τις πράξεις επεξεργασίας και τις διαδικασίες επεξεργασίας, συμπεριλαμβανομένων των μέτρων για τη διασφάλιση σύννομης και θεμιτής επεξεργασίας, *όπως εκείνα για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX. Το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους ανταποκρίνεται σε σκοπό δημόσιου συμφέροντος και είναι ανάλογο προς τον επιδιωκόμενο νόμιμο σκοπό.».*

Ιδιαίτερη έμφαση θα πρέπει να δοθεί στην **παρ.(3) του άρθρου 6** του Κανονισμού με βάση την οποία ενδεχομένως να πρέπει να γίνουν σχετικές τροποποιήσεις στις οικείες νομοθεσίες με βάση τις οποίες αποδίδονται υποχρεώσεις συλλογής και επεξεργασίας για σκοπούς προσαρμογής τους με τον Κανονισμό.

4.7 Η επεξεργασία ειδικών κατηγοριών (ευαίσθητων) προσωπικών δεδομένων γίνεται μόνο υπό προϋποθέσεις που καθορίζει το **άρθρο 9** του Κανονισμού (π.χ δεδομένα υγείας).

4.8 Ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων **άρθρα 12-22 Κανονισμού.**

Κάθε Δημόσια Αρχή υπέχει υποχρέωση να ενημερώσει το προσωπικό και να καθιερώσει μηχανισμούς, να οργανώσει κατάλληλα την υπηρεσία με την απονομή ρόλων ώστε να διευκολύνεται η άσκηση των δικαιωμάτων των διοικούμενων τα οποία απορρέουν από τον Κανονισμό π.χ δικαίωμα ενημέρωσης, πρόσβασης κλπ αλλά και να επιτευχθεί σε κάθε περίπτωση η συμμόρφωση με τον Κανονισμό σε κάθε επίπεδο εντός της Δημόσιας Αρχής.

4.9 Απαιτείται να σχεδιαστούν και να τεθούν σε λειτουργία συστήματα διαχείρισης πληροφοριών και διαδικασίες που να αποσκοπούν στη διασφάλιση ενός υψηλού επιπέδου ασφάλειας των προσωπικών δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (data protection by design and by default) **(άρθρο 25)** αυστηρά προσαρμοσμένα στις βασικές αρχές της επεξεργασίας δεδομένων. Αναφορικά με το επίπεδο ασφάλειας των συστημάτων σε κάθε περίπτωση θα πρέπει να

εφαρμόζονται, μεταξύ άλλων, τα προβλεπόμενα στο **(άρθρο 32)** τεχνικά και οργανωτικά μέτρα ασφάλειας τα οποία να εξασφαλίζουν επίπεδο ασφάλειας των προσωπικών δεδομένων ανάλογο με τους κινδύνους στους οποίους εκτίθενται οι επεξεργασίες δεδομένων.

4.10 Ανάθεση επεξεργασίας σε εκτελών την επεξεργασία γίνεται με **έγγραφη ανάθεση** σύμφωνα με το περιεχόμενο του **άρθρου 28**.

Αποτελεί πάγια και θεσμοθετημένη πολλές φορές πρακτική και /ή διαδικασία η ανάθεση εργολαβίας από Δημόσιες Αρχές σε ιδιωτικούς οργανισμούς. Όταν η εργολαβία αφορά στη συλλογή ή σε οποιασδήποτε μορφής επεξεργασία προσωπικών δεδομένων από τον εκτελών την επεξεργασία εκ μέρους και για λογαριασμό του υπεύθυνου επεξεργασίας η επιλογή του πρώτου θα πρέπει να γίνεται με κριτήρια που αφορούν στην αξιοπιστία του όσον αφορά τη διασφάλιση της ασφάλειας των προσωπικών δεδομένων με τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων ασφάλειας και την καθιέρωση διαδικασιών ώστε να διασφαλίζεται η προστασία των δικαιωμάτων των υποκειμένων των δεδομένων.

Η σχετική ανάθεση διέπεται υποχρεωτικά από γραπτή σύμβαση ή άλλη νομική πράξη του ενωσιακού ή εθνικού δικαίου αμφότερες οι οποίες θα πρέπει απαραίτητα να περιλαμβάνουν τα στοιχεία της **παρ. 3 του άρθρου 28**.

Η γραπτή σύμβαση ανάθεσης της επεξεργασίας μπορεί να αποτελεί μέρος ευρύτερης σύμβασης εργολαβίας.

4.11 Γνωστοποίηση παραβιάσεων προσωπικών δεδομένων στην ΕΠΔΠΧ εντός αποκλειστικής προθεσμίας σύμφωνα με τα οριζόμενα στα **άρθρα 33 και 34** του Κανονισμού.

Καθιέρωση μηχανισμών και πλάνου άμεσης επικοινωνίας για σκοπούς έγκαιρης ανταπόκρισης στις υποχρεώσεις γνωστοποίησης της παραβίασης στην εποπτική Αρχή και στα υποκείμενα των δεδομένων. Η επικαιροποίηση των στοιχείων επαφής των υποκειμένων των δεδομένων κατά τακτά χρονικά διαστήματα συνδράμει θετικά τόσο στη διατήρηση ακριβών και έγκυρων πληροφοριών όσο και στην επικοινωνία μαζί τους σε περίπτωση που λάβει χώρα περιστατικό ασφάλειας το οποίο συνεπάγεται την παραβίαση προσωπικών δεδομένων.

4.12 Εφόσον διαπιστωθεί η διενέργεια επεξεργασιών, από τις οποίες ενδέχεται να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, σχετικός κατάλογος συναφών επεξεργασιών έχει αναρτηθεί στην ιστοσελίδα του Γραφείου της ΕΠΔΠΧ,

ο υπεύθυνος επεξεργασίας διενεργεί εκτίμηση αντικτύπου των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας σύμφωνα με τα οριζόμενα στο **άρθρο 35** του Κανονισμού.

17/5/2018