ΟΔΗΓΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΠΕΡΙΦΕΡΕΙΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

χειμάτη αντιδέσεις!

ΠΕΡΙΕΧΟΜΕΝΑ

ΟΔΗΓΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΙΚΑ

Η προστασία των δεδομένων προσωπικού χαρακτήρα των υποκειμένων αποτελεί συλλογική προσπάθεια και απαιτεί συνεργασία και καλή θέληση από όλους όσους συνδέονται με τις οργανωτικές δομές της Περιφέρειας Δυτικής Ελλάδας (εφεξής αναφερόμενης και ως «ΠΔΕ»), είτε ως όργανα διοίκησης είτε ως μέλη του ανθρώπινου δυναμικού. Ο Υπεύθυνος Προστασίας Δεδομένων (DPO), σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 (ΓΚΠΔ ή "GDPR"), συνδράμει σε αυτή τη διαδικασία, παρακολουθεί και εποπτεύει τη συμμόρφωση με τον πιο πάνω Κανονισμό. Ο παρών Οδηγός Συμμόρφωσης περιέχει τις βασικές αρχές και τις οδηγίες που θα βοηθήσουν στην αποτελεσματική συνεργασία όλων των εμπλεκόμενων μερών κατά το μέτρο της αρμοδιότητας του καθενός.

Η Περιφέρεια Δυτικής Ελλάδας έχει αναθέσει τις υπηρεσίες Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer – DPO) καθώς και τη συμμόρφωση της Περιφέρειας Δυτικής Ελλάδας με τον ΓΚΠΔ και τον Νόμο 4624/2019 για την προστασία των προσωπικών δεδομένων στην Εταιρεία "Privacy Advocate Συμβουλευτικές Υπηρεσίες ΙΚΕ". Με στόχο την καλύτερη και αμεσότερη συνεργασία του DPO με το προσωπικό της Περιφέρειας χρειάζεται να οριστούν τα αρμόδια πρόσωπα επικοινωνίας. Τα πρόσωπα αυτά αποτελούν τους λεγόμενους Data Champions και είναι τα σημεία επαφής του DPO, με σκοπό να προωθούν τα ερωτήματα και τους προβληματισμούς που καθημερινά προκύπτουν και αφορούν την επεξεργασία των προσωπικών δεδομένων των υποκειμένων αλλά και τα μέτρα για την προστασία τους. Συνεπώς, προτείνεται ο ορισμός ενός Data Champion τουλάχιστον σε κάθε Διεύθυνση της Περιφέρειας, ο οποίος θα βρίσκεται σε επικοινωνία με τον DPO για ενδεχόμενα ζητήματα που θα προκύπτουν.

2. Η ΥΠΟΧΡΕΩΣΗ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΚΠΔ

Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα, το οποίο περιγράφεται στο άρθρο 9 του Συντάγματος ως ατομικό δικαίωμα. Το δικαίωμα, όμως, αυτό δεν είναι απόλυτο. Πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα.

Το πλαίσιο προστασίας και οι όροι στάθμισης προβλέπονται και ορίζονται, μεταξύ άλλων, από τον ΓΚΠΔ. Ο ΓΚΠΔ τέθηκε σε ισχύ στις 25 Μαΐου 2016 και τέθηκε σε εφαρμογή στις 25 Μαΐου 2018. Τα κράτη μέλη, τα θεσμικά όργανα της Ε.Ε. και οι ιδιώτες πρέπει να συμμορφώνονται πλήρως με αυτόν. Σκοπός του είναι η διασφάλιση της ενιαίας εφαρμογής του δικαίου της Ένωσης σε όλα τα κράτη μέλη.

Επιπρόσθετα, στις 26-08-2019 ψηφίστηκε στην Βουλή ο Ν.4624/2019 για την εφαρμογή του GDPR στην ελληνική έννομη τάξη. Ο νόμος αυτός εξειδικεύει ρυθμίσεις του Κανονισμού στο βαθμό που ο τελευταίος το επιτρέπει.

3. ΣΥΝΤΟΜΟΣ ΚΑΤΑΛΟΓΟΣ ΟΡΩΝ

Οι ακόλουθοι εξειδικευμένοι όροι του ΓΚΠΔ χρησιμοποιούνται στον παρόντα Οδηγό.

- **ΓΚΠΔ**: 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 και την κατάργηση της οδηγίας 95/46/ΕΚ.

- **Δεδομένα προσωπικού χαρακτήρα (ή προσωπικά δεδομένα):** κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως, το όνομα, ο αριθμός ταυτότητας, τα δεδομένα θέσης, το επιγραμμικό (online) αναγνωριστικό ταυτότητας, ένας ή περισσότεροι παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική. Ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του φυσικού προσώπου.
- **Υποκείμενο δεδομένων:** το φυσικό πρόσωπο του οποίου τα δεδομένα προσωπικού χαρακτήρα υπόκεινται σε συλλογή ή/και επεξεργασία. Προσοχή: Ο Κανονισμός δεν εφαρμόζεται στη συλλογή και επεξεργασία δεδομένων θανόντων ή νομικών προσώπων. Για τις ανάγκες της Περιφέρειας, υποκείμενα δεδομένων αποτελούν οι πολίτες, οι ωφελούμενοι των υπηρεσιών της, οι εργαζόμενοι σε αυτήν, οι συνεργάτες και κάθε τρίτος για τον οποίο η Περιφέρεια συλλέγει και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα.
- **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. Επεξεργασία συνιστούν, μεταξύ άλλων, η συλλογή, η καταχώριση, η οργάνωση, η αποθήκευση, η προσαρμογή, η μεταβολή, η ανάκτηση, η αναζήτηση, η χρήση, η κοινολόγηση, η διαβίβαση, η διάδοση, ο συνδυασμός, η διαγραφή και η καταστροφή. Επεξεργασία προσωπικών δεδομένων αποτελεί κόμη και η απεικόνιση προσωπικών δεδομένων σε οθόνη υπολογιστή.
- **Αρχείο:** κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια. Το σύνολο μπορεί να είναι συγκεντρωμένο ή αποκεντρωμένο ή κατανεμημένο σε λειτουργική ή γεωγραφική βάση.
- **Υπεύθυνος επεξεργασίας:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία, ο φορέας, που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο επεξεργασίας δεδομένων προσωπικού χαρακτήρα (η ΠΔΕ εν προκειμένω).
- **Εκτελών την επεξεργασία:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία, ο φορέας, που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας. Ο Εκτελών λειτουργεί σύμφωνα με τις οδηγίες και τις υποδείξεις του Υπευθύνου Επεξεργασίας.
- **Αποδέκτης:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στον οποίο κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα είτε πρόκειται για τρίτο είτε όχι. Όμως, οι δημόσιες αρχές οι οποίες ζητούν, στη βάση εγγράφου αιτιολογημένου αιτήματος, και λαμβάνουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας για την εκπλήρωση της κύριας αποστολής τους, σύμφωνα με το δίκαιο της Ευρωπαϊκής Ένωσης ή εθνικής προέλευσης διατάξεις (πχ. ΕΦΚΑ, ΕΟΠΥΥ, ΥΠΕΔΥΦΚΑ, ΑΑΔΕ, ΔΟΥ, αστυνομικές, λιμενικές, στρατιωτικές ή άλλες δημόσιες αρχές στο πλαίσιο διενέργειας προκαταρκτικής εξέτασης ή προανάκρισης, δικαστικές αρχές ή εισαγγελικές στο πλαίσιο διενέργειας προανάκρισης ή τακτικής ανάκρισης), δεν θεωρούνται αποδέκτες των δεδομένων προσωπικού χαρακτήρα).
- **Παραβίαση προσωπικών δεδομένων:** η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, κοινολόγηση χωρίς άδεια, πρόσβαση χωρίς άδεια δεδομένων προσωπικού χαρακτήρα που υποβλήθηκαν με οποιοδήποτε τρόπο σε επεξεργασία.
-

4. ΠΑΡΟΥΣΙΑΣΗ ΒΑΣΙΚΩΝ ΑΡΘΡΩΝ ΤΟΥ ΓΚΠΔ

Στο παρόν Κεφάλαιο γίνεται παρουσίαση και ανάλυση βασικών άρθρων, εννοιών και υποχρεώσεων που ορίζονται στον Κανονισμό. Δεν περιγράφονται όλα τα άρθρα, αλλά όσα είναι κατ' αρχήν χρήσιμο να γνωρίζετε και στα οποία πρέπει να ανατρέχετε κάθε φορά που προκύπτει ζήτημα επεξεργασίας και προστασίας δεδομένων προσωπικού χαρακτήρα.

- Το άρθρο 1 ορίζει το αντικείμενο και τους στόχους του Κανονισμού. Θέτει τους βασικούς κανόνες εφαρμογής. Ο Κανονισμός προστατεύει τα φυσικά πρόσωπα έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και θέτει κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα. Επιδιώκει την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- Το άρθρο 2 προσδιορίζει το ουσιαστικό πεδίο εφαρμογής του Κανονισμού, το οποίο είναι η, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα και η μη αυτοματοποιημένη επεξεργασία των δεδομένων αυτών, τα οποία περιλαμβάνονται ή θα περιληφθούν σε αρχείο.
- Το άρθρο 3 προσδιορίζει το εδαφικό πεδίο εφαρμογής του Κανονισμού. Συγκκεριμένα, ο ΓΚΠΔ εφαρμόζεται στην επεξεργασία που λαμβάνει χώρα από Υπεύθυνους Επεξεργασίας εντός Ευρωπαϊκής Ένωσης, ή αφορά προσωπικά δεδομένα ευρωπαίων πολιτών, εντός και εκτός Ευρωπαϊκής Ένωσης. Επομένως, η μόνη περίπτωση που δεν εφαρμόζεται είναι όταν ένας οργανισμός εκτός ΕΕ επεξεργάζεται προσωπικά δεδομένα μη ευρωπαίων πολιτών.
- Το άρθρο 4 περιλαμβάνει όλους τους ορισμούς για την κατανόηση του κειμένου του Κανονισμού. Μερικοί από αυτούς δίνονται στο αμέσως προηγούμενο Κεφάλαιο του παρόντος.
- Το άρθρο 5 αποτελεί ένα από τα βασικότερα άρθρα του Κανονισμού. Περιγράφει τις αρχές που πρέπει να διέπουν την εκ μέρους σας συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Ως Υπεύθυνος Επεξεργασίας και σε εφαρμογή της αρχής της λογοδοσίας που θεσπίζει στο άρθρο αυτό ο Κανονισμός, η Περιφέρεια οφείλει να αποδεικνύει εγγράφως ότι τηρεί τις ακόλουθες αρχές:

- της νομιμότητας, της αντικειμενικότητας και της διαφάνειας: Σύμφωνα με τον Κανονισμό, υπάρχουν μόνο έξι (6) νομικές βάσεις επεξεργασίας απλών προσωπικών δεδομένων και δέκα (10) νομικές βάσεις επεξεργασίας ειδικών κατηγοριών προσωπικών δεδομένων. Η επεξεργασία πρέπει να είναι και νόμιμη και θεμιτή. Η επεξεργασία απαιτεί ενημέρωση του υποκειμένου των δεδομένων, η οποία να είναι πλήρης, συνοπτική, σαφής και κατανοητή, με απλή διατύπωση, διαρκής και εύκολα προσβάσιμη.
- του περιορισμού του σκοπού: Η επεξεργασία γίνεται για συγκεκριμένο σκοπό. Εξαιρείται η περαιτέρω επεξεργασία για αρχειοθέτηση προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας και για στατιστικούς σκοπούς (τεκμήριο συμβατότητας). Νόμιμη είναι η επεξεργασία για σκοπό συμβατό με τον αρχικό χωρίς να απαιτείται άλλη νομική βάση.
- της ελαχιστοποίησης των δεδομένων που συλλέγονται.
- της ακρίβειας των δεδομένων που συλλέγονται. Αν τα δεδομένα δεν είναι ακριβή, πρέπει να επικαιροποιούνται άμεσα.
- του περιορισμού (και εξ αρχής ορισμού) της περιόδου αποθήκευσης: Τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων τους μόνο για όσο χρονικό διάστημα αυτό είναι αναγκαίο για τον σκοπό της επεξεργασίας. Για μεγαλύτερο χρονικό διάστημα και εφόσον προβλέπεται από τον Κανονισμό ή το δίκαιο, θα πρέπει να επιλέγεται η ψευδωνυμοποίηση και η ανωνυμοποίηση[1]. Δεν θα πρέπει να φυλάσσονται έγγραφα (ιδιωτικά ή δημόσια) με προσωπικά δεδομένα

[1] Ανωνυμοποιημένα δεδομένα δεν θεωρούνται προσωπικά δεδομένα.

χωρίς λόγο. Κάθε Τμήμα/ Διεύθυνση θα πρέπει να λαμβάνει υπόψιν του την κείμενη νομοθεσία που ορίζει τον χρόνο τήρησης των δεδομένων ανά κατηγορία εγγράφων.

❖ της ακεραιότητας και της εμπιστευτικότητας: Τα δεδομένα υπόκεινται σε επεξεργασία κατά τρόπο ασφαλή, που εγγυάται την προστασία τους από παράνομη επεξεργασία, απώλεια, διάδοση ή κοινοποίηση, φθορά, κ.λπ. Δεν έχουν πρόσβαση όλοι οι εργαζόμενοι σε όλα τα δεδομένα, αλλά μόνο σε αυτά που τους είναι απαραίτητα για την άσκηση των καθηκόντων τους. Δεδομένα ειδικών κατηγοριών αποστέλλονται/κοινολογούνται με αυξημένα μέτρα προστασίας (κρυπτογράφηση, ενδείξεις απορρήτου και εμπιστευτικότητας).

- Το άρθρο 6 αποτελεί ένα από τα βασικότερα άρθρα του Κανονισμού. Αναφέρει τις έξι (6) μόνες νομικές βάσεις (προϋποθέσεις) που καθιστούν την επεξεργασία απλών δεδομένων προσωπικού χαρακτήρα νόμιμη. Συγκεκριμένα, προϋπόθεση – νομική βάση συνιστά:

(α) η συγκατάθεση του υποκειμένου των δεδομένων,
(β) η ανάγκη εκτέλεσης σύμβασης,
(γ) η ανάγκη συμμόρφωσης σε έννομη υποχρέωση του υπεύθυνου επεξεργασίας
(δ) η ανάγκη διαφύλαξης ζωτικού συμφέροντος φυσικού προσώπου,
(ε) η ανάγκη εκπλήρωσης καθήκοντος υπέρ του δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας και
(στ) η ανάγκη άσκησης των σκοπών των εννόμων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου (υπό τους όρους της διάταξης).
Η διάταξη της παρ. 4 του ίδιου άρθρου θεσπίζει τις αρχές που πρέπει να ακολουθηθούν σε περίπτωση που η ΠΔΕ επιθυμεί να προβεί σε επεξεργασία των δεδομένων που έχει συλλέξει για σκοπό διαφορετικό από τον αρχικώς ορισθέντα (έννοια της συμβατότητας των σκοπών).

Προσοχή:
(α) κατά κανόνα, δεν θα πρέπει να χρησιμοποιείται ως βάση η συγκατάθεση, π.χ. στα έντυπα ενημέρωσης των εργαζομένων, διότι η νομική βάση επεξεργασίας είναι αυτή του άρθρου 6 περ. β και 9 παρ. 2 β'.
(β) στα έντυπα ενημέρωσης δεν μπορούν να τεθούν πολλές ή εναλλακτικές νομικές βάσεις. Επιλέγεται μόνο μία, δηλαδή, αυτή που συμφωνεί με τη φύση των δεδομένων (απλά ή ειδικών κατηγοριών) και με τον σκοπό της συλλογής και επεξεργασίας.
(γ) στα έντυπα ενημέρωσης το υποκείμενο των δεδομένων θέτει την υπογραφή του υπό την ένδειξη «ενημερώθηκα» ή «έλαβα γνώση των ανωτέρω» και όχι «συναινώ» (φυσικά με ορισμένες εξαιρέσεις).

- Το άρθρο 7 αφορά την περίπτωση που η επεξεργασία των δεδομένων βασίζεται στη συγκατάθεση. Αναφέρονται οι προϋποθέσεις, που πρέπει να πληρούνται, προκειμένου η συγκατάθεση να είναι έγκυρη ως νομική βάση. Συγκεκριμένα, η συγκατάθεση θα πρέπει να αποτελεί ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη ένδειξη της συμφωνίας του υποκειμένου.
- Τα άρθρα 9 και 10 αποτελούν δύο από τα βασικότερα άρθρα του Κανονισμού. Αναφέρουν, το πρώτο, τις δέκα (10) μόνες νομικές βάσεις (προϋποθέσεις) και, το δεύτερο, τους όρους, που καθιστούν νόμιμη την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (παλιότερα αναφέρονταν ως ευαίσθητα προσωπικά δεδομένα).

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα:

- Φυλετική ή εθνοτική καταγωγή
- Πολιτικά φρονήματα
- Θρησκευτικές και φιλοσοφικές πεποιθήσεις
- Συμμετοχή σε συνδικαλιστική οργάνωση

- Γενετικά και βιομετρικά δεδομένα (αδιαμφισβήτητη ταυτοποίηση προσώπου)
- Υγεία
- Σεξουαλική ζωή / γενετήσιος προσανατολισμός
- Ειδικές προβλέψεις για τα ποινικά μητρώα.

Νομικές βάσεις σύννομης επεξεργασίας:
(α) η συγκατάθεση,
(β) η ανάγκη εκτέλεσης υποχρεώσεων και άσκησης δικαιωμάτων του υπεύθυνου επεξεργασίας στους τομείς του εργατικού δικαίου, του δικαίου κοινωνικής ασφάλισης και του δικαίου κοινωνικής προστασίας,
(γ) η ανάγκη διαφύλαξης ζωτικού συμφέροντος φυσικού προσώπου,
(δ) η επεξεργασία στο πλαίσιο δραστηριοτήτων ιδρύματος κλπ με στόχο πολιτικό, φιλοσοφικά κ.α. (υπό τους όρους της διάταξης),
(ε) η προηγούμενη δημοσιοποίηση των δεδομένων από το υποκείμενό,
(στ) η άσκηση νομικών αξιώσεων
(ζ) λόγοι ουσιαστικού δημοσίου συμφέροντος ανάλογου προς τον επιδιωκόμενο σκοπό (υπό τους όρους της διάταξης),
(η) η ανάγκη εξυπηρέτησης συγκεκριμένων ιατρικών σκοπών,
(θ) λόγοι δημοσίου συμφέροντος στον τομέας της δημόσιας υγείας (υπό τους όρους της διάταξης) και
(ι) σκοποί αρχειοθέτησης προς το δημόσιο συμφέρον, σκοποί επιστημονικής και ιστορικής έρευνας και σκοποί στατιστικοί (υπό τους όρους της διάταξης).

- Τα άρθρα 12 έως και 23 περιγράφουν τα δικαιώματα των υποκειμένων των δεδομένων.
- Στα άρθρα 24 έως και 31 αναλύονται οι γενικές υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία.

Βασικό άρθρο είναι το άρθρο 24, που ουσιαστικά περιγράφει την αρχή της λογοδοσίας *(«ο υπεύθυνος επεξεργασίας (ΠΔΕ) εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό»*). Το άρθρο 25 καθορίζει τις υποχρεώσεις του υπευθύνου επεξεργασίας για τη λήψη μέτρων τόσο κατά τη στιγμή καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, όπως, ψευδωνυμοποίηση, ελαχιστοποίηση των δεδομένων, εγγυήσεις απορρήτου (προστασία από τον σχεδιασμό και εξ ορισμού). Πολύ σημαντικό είναι και το άρθρο 30, που θεσπίζει την υποχρέωση των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία να τηρούν **έγγραφη και ηλεκτρονική τεκμηρίωση των πράξεων επεξεργασίας (Αρχείο Δραστηριοτήτων Επεξεργασίας)**. Είναι το κύριο εργαλείο απόδειξης τήρησης της αρχής της λογοδοσίας και αντικαθιστά την παλιά διαδικασία κοινοποίησης/γνωστοποίησης επεξεργασίας δεδομένων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής ΑΠΔΠΧ).

- Τα άρθρα 32 έως και 36 αναφέρονται στην ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Βασικό άρθρο είναι το άρθρο 32 που ορίζει την υποχρέωση του υπεύθυνου επεξεργασίας (αλλά και του εκτελούντα) να τηρούν μέτρα ασφάλειας της επεξεργασίας. Τα άρθρα 33 και 34 θεσπίζουν την υποχρέωση γνωστοποίησης στην ΑΠΔΠΧ και ανακοίνωσης στα υποκείμενα των δεδομένων παραβιάσεων των δεδομένων προσωπικού χαρακτήρα. Το άρθρο 35 επιβάλλει τη διενέργεια εκτίμησης επιπτώσεων (DPIA) εφόσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα πουπρόκειται να γίνει, εγκυμονεί κινδύνους για τα δικαιώματα των υποκειμένων.

- Τα άρθρα 37 και 38 αναφέρονται στον ορισμό Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer – Κατσίκης Μαυράκη & Συνεργάτες). Η θέση του στην οργάνωση της Περιφέρειας και οι αρμοδιότητές του καθορίζονται ειδικώς στα άρθρα 38 και 39. Ειδικότερα, σύμφωνα με το άρθρο 39, προβλέπεται ότι ο Υπεύθυνος Προστασίας Δεδομένων: *«α) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον*

εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων, β) παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35, δ) συνεργάζεται με την εποπτική αρχή, ε) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα».

- Τα άρθρα 37 έως και 43 του Κανονισμού προβλέπουν τη σύνταξη κωδίκων δεοντολογίας και τη λήψη πιστοποίησης, σε σχέση με υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία.
- Τα άρθρα 44 έως 50 του Κανονισμού αναφέρονται στις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς. Είναι χρήσιμη η ανάγνωση των ειδικών αυτών άρθρων, αλλά και η συμβουλή του Υπεύθυνου Προστασίας Δεδομένων για την αντιμετώπιση αιτήματος διαβίβασης προσωπικών δεδομένων, καθώς υπάρχει ειδικός κατάλογος χωρών για τις οποίες η Ευρωπαϊκή Ένωση έχει λάβει απόφαση «επάρκειας» σχετικά με τη διαβίβαση δεδομένων προσωπικού χαρακτήρα. Περαιτέρω, το άρθρο 48 ορίζει ποιες διαβιβάσεις ή κοινοποιήσεις δεν επιτρέπονται από το δίκαιο της Ένωσης.
- Τα άρθρα 51 έως 59 του Κανονισμού αφορούν στις ανεξάρτητες εποπτικές αρχές, που για την Ελλάδα είναι η ΑΠΔΠΧ. Τα άρθρα 55-58 ορίζουν την αρμοδιότητα, τα καθήκοντα και τις εξουσίες της εποπτικής αρχής.
- Τα άρθρα 77 έως 84 του Κανονισμού καθορίζουν τις διαδικασίες προσφυγών και το καθεστώς κυρώσεων σε βάρος των Υπευθύνων Επεξεργασίας και των εκτελούντων την επεξεργασία. Ειδικότερα, σύμφωνα με το άρθρο 77 κάθε υποκειμένο δεδομένων έχει δικαίωμα να υποβάλει καταγγελία (προσφυγή) στην ΑΠΔΠΧ, σε περίπτωση που θεωρεί ότι είναι παράνομη η επεξεργασία των προσωπικών του δεδομένων. Το άρθρο 78 ορίζει τα ένδικα μέσα (ενώπιον δικαστηρίου) κατά της απόφασης της ΑΠΔΠΧ. Το άρθρο 79 αφορά το δικαίωμα δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, ενώ το άρθρο 82 ορίζει δικαίωμα αποζημίωσης του υποκειμένου δικαιώματος από τον υπεύθυνο επεξεργασίας σε περίπτωση παραβίασης των δικαιωμάτων του. Οι κυρώσεις, που ορίζει ο Κανονισμός (άρθρα 83 επ.) είναι: Κύρωση έως € 10,000,000 ή, σε περίπτωση ανάληψης υποχρέωσης, 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (όποιο εκ των δύο είναι μεγαλύτερο) για παραβίαση των άρθρων 8 (συγκατάθεση ανηλίκου), 11 (επεξεργασία χωρίς αναγνώριση), 25 (προστασία δεδομένων λόγω σχεδιασμού και εξ' ορισμού), 26 (κοινοί εκτελούντες την επεξεργασία), 27 (αντιπρόσωποι υπευθύνων επεξεργασίας που δεν εδρεύουν στην Ε.Ε.), 26 – 29 & 30 (επεξεργασία δεδομένων), 31 (συνεργασία με την εποπτική αρχή), 32 (ασφάλεια δεδομένων), 33 (αναφορά παραβιάσεων στην εποπτική αρχή), 34 (ενημέρωση των υποκειμένων δεδομένων για παραβιάσεις), 35 (εκτίμηση επιπτώσεων προστασίας δεδομένων), 36 (πρότερη διαβούλευση), 37-39 (Υπεύθυνοι Προστασίας Δεδομένων), 41(4) (επίβλεψη κώδικα δεοντολογίας), 42 – 43 (πιστοποίηση) Κύρωση έως € 20,000,000 ή, σε περίπτωση ανάληψης υποχρέωσης, 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (όποιο εκ των δύο είναι μεγαλύτερο) για παραβίαση των άρθρων: 5 (αρχές που σχετίζονται με την επεξεργασία προσωπικών δεδομένων), 6 (νομιμότητα της επεξεργασίας), 7 (συνθήκες συγκατάθεσης), 9 (επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων), 12-22 (δικαιώματα των υποκειμένων των δεδομένων), 44-49: διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες, 58 (1): Προϋπόθεση να παρέχεται πρόσβαση στην εποπτεύουσα αρχή, 58(2): Εντολές / περιορισμοί στην επεξεργασία ή διακοπή της ροής δεδομένων.

Ποινικές κυρώσεις μπορούν και θα καθοριστούν από το εθνικό δίκαιο. Τα άρθρα 85 έως 91 του Κανονισμού αφορούν ειδικές περιπτώσεις επεξεργασίας.

5. ΤΑ ΟΚΤΩ ΔΙΚΑΙΩΜΑΤΑ των ΥΠΟΚΕΙΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ

Προσοχή:
- Πάντα επαληθεύουμε την ταυτότητα του αιτούντος την άσκηση δικαιώματός του, και
- Πάντα απαντάμε εγγράφως μέσα στις προθεσμίες που ορίζει ο Κανονισμός. Σύμφωνα με το άρθρο 12 παρ. 3 και 4 ΓΚΠΔ τα αιτήματα απαντώται, κατά περίπτωση, είτε άμεσα εντός ενός (1) μήνα, είτε μέσα σε δύο (2) μήνες εάν το αίτημα είναι ιδαίτερα περίπλοκο ή απαιτεί περισσότερο χρόνο. Στην περίπτωση που δεν έχουμε προβεί σε ενέργεια, τότε μέσα σε ένα (1) μήνα ενημερώνουμε γιατί δεν προβήκαμε σε ενέργεια και πότε προβλέπεται η απάντηση.

1. Δικαίωμα ενημέρωσης (άρθρο 12):
Ο Κανονισμός θεσπίζει μία διαφανή πολιτική ενημέρωσης των υποκειμένων δεδομένων, ώστε το κάθε υποκείμενο να μπορεί να ασκεί τα δικαιώματά του αποτελεσματικά. Κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία προσωπικών δεδομένων πρέπει να είναι εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή γλώσσα, γλώσσα καθημερινή, ανάλογα με το μορφωτικό επίπεδο και την ηλικία του ατόμου. Να αποφεύγεται η υπερπληροφόρηση. Οι πληροφορίες δίνονται γραπτώς ή με ηλεκτρονική μορφή. Όταν οι πληροφορίες δίνονται προφορικώς, πρέπει να αποδεικνύεται εγγράφως η πληροφόρηση. Η προθεσμία για παροχή ενημέρωσης είναι ένας μήνας και μπορεί να παραταθεί για δύο μήνες ανάλογα με την πολυπλοκότητα. Κάθε αίτηση ενημέρωσης δεν συνεπάγεται και υποχρέωση για ενέργεια. Πρέπει, όμως, να ενημερωθεί το υποκείμενο δεδομένων για τους λόγους που δεν ενήργησε και τη δυνατότητα προσφυγής στην εποπτική αρχή και στα δικαστήρια. Προσοχή στα καταχρηστικά αιτήματα.

2. Δικαίωμα πρόσβασης (άρθρα 13 -15):
Το υποκείμενο δεδομένων έχει δικαίωμα να ελέγξει τον τρόπο επεξεργασίας των προσωπικών του δεδομένων (νομιμότητα) ώστε να ασκήσει τα υπόλοιπα δικαιώματά του (όπως, το δικαίωμα διόρθωσης, το δικαίωμα εναντίωσης κ.α.). Το δικαίωμα (και ο λόγος άσκησής του) δεν χρήζει αιτιολόγησης. Πρώτα πρέπει να εξετασθεί αν υπάρχουν δεδομένα του υποκειμένου στον φορέα. Σε θετική περίπτωση, το υποκείμενο δεδομένων έχει πρόσβαση στις ακόλουθες πληροφορίες (α) σκοπό επεξεργασίας, (β) κατηγορίες δεδομένων, (γ) αποδέκτες, (δ) χρονικό διάστημα διατήρησης, (ε) ύπαρξη δικαιώματος υποβολής αιτήματος για διορθωση, διαγραφή κλπ, (στ) δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή, (ζ) προέλευσή τους.

3. Δικαίωμα διόρθωσης (άρθρο 16):
Το υποκείμενο δεδομένων έχει δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών του δεδομένων, την επικαιροποίηση των δεδομένων του και τη συμπλήρωση ελλιπών δεδομένων[2].

4. Δικαίωμα διαγραφής («δικαίωμα στη λήθη») (άρθρο 17):
Το υποκείμενο δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή των δεδομένων του, όταν συντρέχουν συγκεκριμένοι λόγοι. Οι λόγοι είναι οι εξής:
(α) τα δεδομένα δεν είναι πλέον αναγκαία για τους σκοπούς της επεξεργασίας,
(β) το υποκείμενο δεδομένων έχει ανακαλέσει τη συγκατάθεσή του ως νομική βάση επεξεργασίας και δεν υπάρχει άλλη νομική βάση για τη συνέχεια της επεξεργασίας,
(γ) το υποκείμενο δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί λόγοι για αυτή,
(δ) τα δεδομένα έτυχαν επεξεργασίας παράνομα,
(ε) τα δεδομένα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση,
(στ) τα δεδομένα συλλέχθηκαν σε σχέση με την προσφορά υπηρεσιών της κοινωνίας της πληροφορίας

[2] Ελλιπή είναι τα δεδομένα που οδηγούν σε παραπλάνηση ή παρεξήγηση.

Κρίσιμη είναι η διάταξη της παρ. 3 του ίδιου άρθρου, καθώς τα παραπάνω δεν εφαρμόζονται στο βαθμό που επεξεργασία είναι απαραίτητη, μεταξύ άλλων (α) για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία κατά το δίκαιο ή για την εκπλήρωση καθήκοντος υπέρ του δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, β) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και (γ) για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
Δεν απαιτείται επίκληση ζημίας.

5. Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18):

Το υποκείμενο δεδομένων έχει δικαίωμα να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας των δεδομένων του σε συγκεκριμένες περιπτώσεις. Ειδικότερα:
α) η ακρίβεια των δεδομένων αμφισβητείται από το υποκείμενο για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να τα επαληθεύσει,
β) η επεξεργασία είναι παράνομη, το υποκείμενο αντιτάσσεται στη διαγραφή και ζητά περιορισμό,
γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πια τα δεδομένα, τα χρειάζεται όμως το υποκείμενο για άσκηση νομικών αξιώσεων,
δ) το υποκείμενο δεδομένων έχει αντιρρήσεις για την επεξεργασία και εν αναμονή του ελέγχου βασιμότητας των αντιρρήσεών του.
Πρέπει να υπάρξει ενημέρωση του υποκειμένου των δεδομένων για την άρση του περιορισμού.

6. Δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20):

Το υποκείμενο δεδομένων έχει δικαίωμα να λάβει ή να ζητήσει τη μεταφορά των δεδομένων του, σε μηχαναγνώσιμη μορφή, από έναν υπεύθυνο επεξεργασίας σε άλλον, υπό συγκεκριμένες προϋποθέσεις. Αφορά σε δεδομένα που λήφθηκαν με βάση τη νομική βάση της συγκατάθεσης και μόνο όταν η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα. Δεν αφορά σε έγχαρτα αρχεία δεδομένων. Η διαβίβαση των δεδομένων γίνεται από υπεύθυνο επεξεργασίας προς υπεύθυνο επεξεργασίας. Αφορά μόνο στα προσωπικά δεδομένα και όχι σε εργασία (στοιχεία αξιολόγησης) του φορέα, που συνοδεύει ή αφορά τα δεδομένα.

7. Δικαίωμα εναντίωσης στην επεξεργασία (άρθρο 21):

Το υποκείμενο δεδομένων έχει δικαίωμα να αντιτάσσεται στην επεξεργασία των δεδομένων του ανά πάσα στιγμή και για λόγους που αφορούν στην διαίτερη κατάστασή του, συμπεριλαμβανομένης της κατάρτισης «προφίλ».Ιδιαίτερη κατάσταση είναι οι ειδικές περιστάσεις της ζωής του κάθε ανθρώπου, νομικές, κοινωνικές, οικογενειακές καταστάσεις ανάγκης.

8. Δικαίωμα στην ανθρώπινη παρέμβαση (άρθρο 22):

Το υποκείμενο δεδομένων έχει δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά με αυτοματοποιημένη επεξεργασία, χωρίς, δηλαδή, να λαμβάνονται υπόψιν τα προσωπικά χαρακτηριστικά του από ένα φυσικό πρόσωπο/χειριστή.

6. ΣΥΓΚΑΤΑΘΕΣΗ ΥΠΟΚΕΙΜΕΝΟΥ ΔΙΚΑΙΩΜΑΤΩΝ [ΑΡΘΡΑ 4 & 7]

Στις περιπτώσεις, που η επεξεργασία των προσωπικών δεδομένων θα γίνεται επί τη βάσει της συγκατάθεσης, ισχύουν τα ακόλουθα:
Συγκατάθεση του υποκειμένου των δεδομένων: κάθε ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη ένδειξη της συμφωνίας 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.
Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε στην επεξεργασία.
Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης που αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση (π.χ. με tickbox).

Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε σε αυτήν προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.
Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.
Προσοχή: Προηγείται η πλήρης ενημέρωση και έπεται η συγκατάθεση.

7. ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ [ΑΡΘΡΟ 13]

Όταν δεδομένα προσωπικού χαρακτήρα υποκειμένου δεδομένων συλλέγονται από το ίδιο το υποκείμενο, η Περιφέρεια, μέσω των Τμημάτων και των Διευθύνσεών της, κατά τη λήψη των δεδομένων, θα παρέχει και εγγράφως στο υποκείμενο όλες τις ακόλουθες πληροφορίες:

- την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας,
- τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων,
- τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,
- εάν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο,
- τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,
- κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό,
- τον χρόνο διατήρησης των δεδομένων,
- τη δυνατότητα άσκησης δικαιωμάτων,
- τυχόν κινδύνους από την επεξεργασία των δεδομένων.

8. ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ [ΑΡΘΡΟ 14]

Όταν τα δεδομένα προσωπικού χαρακτήρα υποκειμένου δεδομένων, δεν έχουν συλλεγεί από το ίδιο το υποκείμενο, αλλά λαμβάνονται από άλλο φορέα, που τα συνέλεξε σύννομα (άλλως δεν λαμβάνονται), η ΠΔΕ παρέχει στο υποκείμενο τις ακόλουθες πληροφορίες:

- την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας,
- τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων,
- τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,
- τις σχετικές κατηγορίες προσωπικών δεδομένων,
- τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,
- κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό,
- τον χρόνο διατήρησης των δεδομένων,
- τη δυνατότητα άσκησης δικαιωμάτων,
- τη δυνατότητα ανάκλησης της συγκατάθεσής του,

- το δικαίωμα υποβολής καταγγελίας στην ΑΠΔΠΧ,
- την πηγή από την οποία προέρχονται τα δεδομένα,
- την ύπαρξη αυτοματοποιημένης λήψης απόφασης,
- τυχόν κινδύνους από την επεξεργασία των δεδομένων.

9. ΕΞΑΙΡΕΣΕΙΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ ΣΤΗΝ ΑΣΚΗΣΗ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Πότε παρέχει η Περιφέρεια τις πιο πάνω πληροφορίες:

- ✓ εντός εύλογης προθεσμίας από την απόκτηση και το αργότερο μέσα σε ένα μήνα,
- ✓ κατά την πρώτη επικοινωνία με το υποκείμενο, όταν τα δεδομένα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο,
- ✓ κατά την γνωστοποίηση σε άλλο αποδέκτη, όταν τα δεδομένα γνωστοποιούνται **πρώτη** φορά.

Πότε δεν απαιτείται να τηρηθούν όλα τα παραπάνω:

- ✓ όταν το υποκείμενο έχει όλες τις πληροφορίες,
- ✓ όταν η παροχή των πιο πάνω πληροφοριών είναι αδύνατη ή δυσανάλογα δύσκολη (ιδίως, στην περίπτωση αρχειοθέτησης υπέρ δημοσίου συμφέροντος, έρευνας και στατιστικής). Στην περίπτωση αυτή, πρέπει να ληφθούν μέτρα προστασίας και ασφάλειας,
- ✓ όταν η απόκτηση ή κοινολόγηση προβλέπεται από νομοθεσία, που παρέχει προστασία των εννόμων συμφερόντων του υποκειμένου,
- ✓ όταν τα δεδομένα πρέπει να μείνουν εμπιστευτικά λόγω υποχρέωσης τήρησης απορρήτου.

10. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ [ΑΡΘΡΑ 25 & 32]

Το άρθρο 25 περιγράφει τις υποχρεώσεις του υπεύθυνου επεξεργασίας για τήρηση (τεχνικών και οργανωτικών) μέτρων ασφάλειας και προστασίας πριν ακόμα την έναρξη συλλογής και επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (data protection by design / data protection by default). Ανεξάρτητα αν η επεξεργασία είναι ηλεκτρονική ή έγχαρτη. Ειδικότερα, στο άρθρο προβλέπεται ότι ο υπεύθυνος πεξεργασίας, αφού λάβει υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα. Τέτοια μέτρα είναι η ψευδωνυμοποίηση, η ελαχιστοποίηση των δεδομένων, και η ενσωμάτωση εγγυήσεων στην επεξεργασία ώστε να πληρούνται οι απαιτήσεις του Κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

Στο άρθρο 32 τα μέτρα ασφάλειας και προστασίας ορίζονται ειδικότερα σε:

- ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα,
- διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων,
- δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση συμβάντος,
- διασφάλιση διαδικασιών για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.
- τήρηση κώδικα δεοντολογίας.

Πέρα από τους ορισμούς του συγκεκριμένου άρθρου, στην Περιφέρεια θα πρέπει:

- να προσδιορίζεται εγγράφως, με βάση τα καθηκοντολόγιά και τις αρμοδιότητές της, ποια πρόσωπα (ονομαστικά) είναι εξουσιοδοτημένα για συγκεκριμένες πράξεις
- να τηρούνται αντίγραφα ασφαλείας αρχείων με δεδομένα προσωπικού χαρακτήρα,
- να χρησιμοποιεί κάθε υπάλληλος δικό του, ξεχωριστό κωδικό πρόσβασης στον υπολογιστή του,
- να μη γίνεται χρήση εξωτερικών αποθηκευτικών μέσων και να μην εξάγονται αρχεία για εργασία στο σπίτι (εκτός συγκερκιμένων περιπτώσεων που θα καταγράφονται ρητά από τη Διεύθυνση Πληροφορικής)
- να μην παραμένουν οι χώροι αφύλακτοι και ανοιχτοί, όταν λείπουν οι υπάλληλοι από αυτούς,
- να τηρείται η αρχή του "clean desk" και να μην μπορούν να δουν μη εξουσιοδοτημένοι τρίτοι έγγραφα και αρχεία με δεδομένα προσωπικού χαρακτήρα
- να επικαιροποιούνται τα λογισμικά και, ιδίως, τα λογισμικά για προστασία των υπολογιστών από ιούς.
- να καταστρέφονται – με την τήρηση του νόμου και των διαδικασιών ασφαλείας – όλα τα αρχεία δεδομένων μετά το πέρας του χρόνου τήρησής τους.

Τα πιο πάνω μέτρα πρέπει να υφίστανται και στους εκτελούντες την επεξεργασία για λογαριασμό της Περιφέρειας. Πριν την έναρξη μίας τέτοιας συνεργασίας θα πρέπει να λαμβάνεται σχετική βεβαίωση από τους εκτελούντες την επεξεργασία και να υπογράφεται η απαραίτητη από το άρθρο 25 του ΓΚΠΔ Σύμβασης Επεξεργασίας Δεδομένων.

11. ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ [ΑΡΘΡΟ 30]

Αποτελεί το βασικό εργαλείο απόδειξης τήρησης της αρχής της λογοδοσίας. Ποιες πληροφορίες περιλαμβάνει:
α) το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων.
β) τους σκοπούς της επεξεργασίας,
γ) περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,
δ) τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,
ε) όπου συντρέχει περίπτωση, τις διαβιβάσεις προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό
στ) όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων,
ζ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας

12. ΒΑΣΙΚΕΣ ΣΚΕΨΕΙΣ ΠΡΙΝ ΤΗΝ ΣΥΛΛΟΓΗ ΚΑΙ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Πριν τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να τίθενται τα ακόλουθα ερωτήματα:
i. Τα δεδομένα προσωπικού χαρακτήρα, που προτίθεμαι να επεξεργαστώ, είναι τα αναγκαία; Μπορώ να αρκεστώ σε λιγότερα;
ii. Για τα δεδομένα προσωπικού χαρακτήρα που μου έχουν ζητηθεί από το ίδιο το υποκείμενο, έχει γίνει αίτηση; Έχω κάνει την αναγκαία ταυτοποίηση; Αν έχουν ζητηθεί από τρίτο, έχει γίνει αίτηση; Έχω ελέγξει τη νομιμοποίησή του, συμπεριλαμβανομένων των κατάλληλων δικαιολογητικών εγγράφων;

iii. Μπορώ να κάνω χρήση των δεδομένων με ανωνυμοποίηση ή ψευδωνυμοποίηση και να πετύχω τους ίδιους σκοπούς;
iv. Τα δεδομένα που προτίθεμαι να επεξεργαστώ είναι απλά ή ειδικών κατηγοριών;
v. Ποια είναι η κατάλληλη νομική βάση σύννομης επεξεργασίας για τα δεδομένων που θα συλλέξω;
vi. Για ποιους σκοπούς θα επεξεργαστώ τα προσωπικά δεδομένα; Τους έχω συμπεριλάβει όλους στο έντυπο ενημέρωσης;
vii. Από ποιους θα συλλέξω τα δεδομένα; Από τα ίδια τα υποκείμενα (άρθρο 13 του Κανονισμού) ή από τρίτους (άρθρο 14) ώστε να τηρήσω τους αντίστοιχους όρους ενημέρωσης;
viii. Πόσο χρόνο θα τηρήσω τα δεδομένα;
ix. Τα δεδομένα που θα επεξεργαστώ θα τα αποστείλω/κοινοποιήσω/διαβιβάσω σε τρίτες χώρες ή άλλους αποδέκτες;
x. Πώς θα ενημερώσω το υποκείμενο δεδομένων για την επεξεργασία στην οποία προτίθεμαι να προβώ με όλες τις πιο πάνω πληροφορίες;
xi. Ενημέρωσα το υποκείμενο των δεδομένων εγγράφως;
xii. Ποια μέτρα πρέπει να λάβω ή να εφαρμόσω ή να τηρήσω προκειμένου τα δεδομένα που θα επεξεργαστώ να είναι ασφαλή; Τηρώ την κρυπτογράφηση ή άλλες μεθόδους ενδεδειγμένες για την ασφάλεια των δεδομένων;
xiii. Αν πρόκειται να γίνει επεξεργασία πολλών δεδομένων ή αν τίθεται κίνδυνος λόγω της επεξεργασίας στα δικαιώματα των υποκειμένων τους, συμβουλεύτηκα τον Υπεύθυνο Προστασίας Δεδομένων;