**Ενότητα 5η**

**ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΕΚΤΕΛΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ**

**ΑΣΦΑΛΕΙΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ**

**ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ**

1. Υποχρεώσεις υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία.
2. Ασφάλεια της επεξεργασίας.
3. Περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα.
4. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση.
5. Κώδικες δεοντολογίας – πιστοποίηση (αναφορά: περιορισμένη εφαρμογή στο δημόσιο τομέα, σε σύγκριση με τον ιδιωτικό).
6. **Υποχρεώσεις υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία** (άρθρα 24 - 29 ΓΚΠΔ και 60 ν. 4624/2019)

Ως προς τον υπεύθυνο επεξεργασίας

μεριμνά για την τήρηση των υποχρεώσεων που απορρέουν από το σύνολο κανονιστικό πλαίσιο σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ως προς τους εκτελούντες την επεξεργασία

* Ο υπεύθυνος επεξεργασίας μπορεί να αναθέσει την επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνο σε εκτελούντες την επεξεργασία
* Οι εκτελούντες την επεξεργασία οφείλουν, στο πλαίσιο σχετικής σύμβασης (έγγραφης ή ηλεκτρονικής) μεταξύ υπεύθυνου επεξεργασίας και εκτελούντος την επεξεργασία να εξασφαλίσουν με κατάλληλα τεχνικά μέσα ότι
	+ - * + η επεξεργασία διενεργείται σύμφωνα με τον νόμο
				+ διασφαλίζεται η προστασία των δικαιωμάτων των υποκειμένων επεξεργασίας

Περιεχόμενο της σύμβασης (μεταξύ εκτελούντος την επεξεργασία και υπευθύνου επεξεργασίας) : αντικείμενο, διάρκεια, φύση, σκοπός της επεξεργασίας, φύση των δεδομένων προσωπικού χαρακτήρα, κατηγορίες των υποκειμένων, δικαιώματα και υποχρεώσεις του υπεύθυνου προσώπου

**Υποχρεώσεις του εκτελούντος την επεξεργασία**

(α) ενεργεί κατ` εντολή και σύμφωνα με τις οδηγίες του υπεύθυνου επεξεργασίας,

(β) εγγυάται ότι τα πρόσωπα που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα οφείλουν να τηρούν την εμπιστευτικότητα

(γ) βοηθά με τα κατάλληλα μέσα τον υπεύθυνο επεξεργασίας για τη διασφάλιση των δικαιωμάτων του υποκειμένου των δεδομένων·

(δ) ευθύνεται για την επιστροφή ή διαγραφή των δεδομένων, μετά την ολοκλήρωση της παροχής των υπηρεσιών επεξεργασίας, κατά την κρίση του υπεύθυνου επεξεργασίας και καταστροφή των αντιγράφων

(ε) παρέχει στον υπεύθυνο επεξεργασίας όλες τις απαραίτητες πληροφορίες

(στ) συμβάλλει σε ελέγχους διενεργούμενους από τον υπεύθυνο επεξεργασίας

Προσοχή : Ο εκτελών την επεξεργασία μπορεί να αναθέσει την επεξεργασία σε άλλον, μόνο κατόπιν προηγούμενης έγγραφης άδειας του υπεύθυνου επεξεργασίας.

**Ευθύνη του εκτελούντος την επεξεργασία** (άρθρο 82 ΓΚΠΔ)

Κατά τα οριζόμενα στο άρθρο 82 παρ. 2 εδ. (β) ΓΚΠΔ : *«Ο εκτελών την επεξεργασία ευθύνεται για τη ζημία που προκάλεσε η επεξεργασία μόνο εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του παρόντος κανονισμού που αφορούν ειδικότερα τους εκτελούντες την επεξεργασία ή υπερέβη ή ενήργησε αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας»*.

Στη συνέχεια, προβλέπεται ότι *«ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία απαλλάσσεται από την ευθύνη … εάν αποδεικνύει ότι δε φέρει καμία ευθύνη για το γενεσιουργό γεγονός της ζημίας»* (άρθρο 82 παρ. 3 ΓΚΠΔ) (νόθος αντικειμενική ευθύνη)

Σημειωτέον πάντως, ότι στο πλαίσιο της αρχής της λογοδοσίας (accountability), υφίσταται διαρκής υποχρέωση του υπεύθυνου επεξεργασίας να αποδεικνύει ότι εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα και ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό» [άρθρο 24 παρ. 1 εδ. (β)]).

Η ευθύνη του εκτελούντος την επεξεργασία βρίσκεται σε συνάρτηση με τις εντολές του υπεύθυνου επεξεργασίας, τον οποίο και οφείλει να συνδράμει στην υλοποίηση των υποχρεώσεών του σχετικά με την ασφάλεια των δεδομένων (άρθρο 28 παρ. 3).

Πάντως, οι εκτελούντες την επεξεργασία φέρουν ευθύνη για κάθε περίπτωση επεξεργασίας που αφορά υποκείμενα με διαμονή εντός ΕΕ, ανεξάρτητα από το εάν η επεξεργασία πραγματοποιείται εντός ή εκτός της ΕΕ (άρθρο 3) (βλ. την περίπτωση μηχανισμών αναζήτησης, κοινωνικής δικτύωσης, blogs κλπ που συνήθως εδρεύουν εκτός ΕΕ).

1. **Ασφάλεια της επεξεργασίας** (62 ν. 4624/2019)

Πρόκειται για σύνθετη υποχρέωση, νομικοτεχνικής φύσης, για την εκπλήρωση της οποίας απαιτούνται από κοινού σε οργανωμένο πλαίσιο, νομικές ρυθμίσεις, τεχνικές διαδικασίες και επαρκή μέτρα για την προστασία του πληροφορικού συστήματος.

Η κρισιμότητα του ζητήματος στην εποχή μας, συνδέεται με τις διαρκώς εξελισσόμενες απειλές σε σχέση με την ακεραιότητα των πληροφορικών συστημάτων. Η «ακεραιότητα» και η «εμπιστευτικότητα» περιλαμβάνονται κατά τις διατάξεις του ΓΚΠΔ, μεταξύ των αρχών που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα [άρθρο 5 παρ. 1 περ.(στ)]. Στο άρθρο 32 του κανονισμού απαριθμούνται ενδεικτικά, για τη διαμόρφωση του κατάλληλου επιπέδου ασφαλείας μια σειρά μέτρων, όπως η ψευδωνυμοποίηση, κρυπτογράφηση, τακτικές δοκιμές κοκ.

Ειδικότερα, τα μέτρα μεταξύ άλλων, πρέπει να διασφαλίζουν και :

(α) την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών που σχετίζονται με την επεξεργασία· και

(β) τη δυνατότητα, σε περίπτωση φυσικού ή τεχνικού συμβάντος, έγκαιρης αποκατάστασης της διαθεσιμότητας και πρόσβασης στα δεδομένα.

Ως προς την αυτοματοποιημένη επεξεργασία, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, μετά από αξιολόγηση των κινδύνων, εφαρμόζουν μέτρα που μεταξύ άλλων, έχουν ως σκοπό:

(α) τον έλεγχο πρόσβασης σε εξοπλισμό

(β) τον έλεγχο μέσων αποθήκευσης

(γ) τον έλεγχο αποθήκευσης

(δ) τον έλεγχο χρηστών

(ε) τον έλεγχο πρόσβασης στα δεδομένα

(στ) τον έλεγχο επικοινωνίας

(ζ) τον έλεγχο εισαγωγής

(η) τον έλεγχο διαβίβασης

(θ) τον έλεγχο αποκατάστασης

(ι) τον έλεγχο αξιοπιστίας και ακεραιότητας

(ια) τον έλεγχο διαθεσιμότητας κλπ

(ιβ) την εξασφάλιση ότι τα δεδομένα προσωπικού χαρακτήρα προστατεύονται από απώλεια και καταστροφή (έλεγχος της διαθεσιμότητας)·

(ιγ) τη δυνατότητα διαχωρισμού των συλλεγέντων δεδομένων

**(III) Υποχρεώσεις σε περιπτώσεις παραβίασης δεδομένων προσωπικού χαρακτήρα**

**(Α) Γνωστοποίηση στην εποπτική αρχή** (άρθρο 33 ΓΚΠΔ και 63 ν.4624/2019)

Ως παραβίαση δεδομένων προσωπικού χαρακτήρα νοείται κατά τους ορισμούς του ΓΚΠΔ, *«η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία»* (άρθρο 4 περ. 12)

Η υποχρέωση γνωστοποίησης της παραβίασης δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή αποτέλεσε κεντρικό ζήτημα, στο πλαίσιο των εργασιών για την εκπόνηση του ΓΚΠΔ. Δεδομένου ότι ένα τέτοιο γεγονός συνδέεται με τη φήμη και την αξιοπιστία των οργανισμών, καθώς επίσης και με ενδεχόμενες αποζημιωτικές υποχρεώσεις που θα γεννηθούν ως συνέπεια της παραβίασης, οι οργανισμοί – θύματα τέτοιων επιθέσεων δεν εμφανίζονται ιδιαίτερα πρόθυμοι να ενημερώσουν τους πελάτες τους.

Η υποχρέωση αυτή αφορά τόσο την εποπτική αρχή (γνωστοποίηση, άρθρο 33), όσο και τα υποκείμενα των δεδομένων (ανακοίνωση, άρθρο 34).

Ως προς την υποχρέωση γνωστοποίησης στην εποπτική αρχή (ΑΠΔΠΧ, στα καθ’ ημάς) :

* προθεσμία : αμελλητί, εντός μέγιστης προθεσμίας 72 ωρών, από τη στιγμή που ο υπεύθυνος επεξεργασίας αποκτά γνώση του γεγονότος – στην πραγματικότητα, εύλογο βαθμό βεβαιότητας για το συμβάν ασφαλείας που κατέληξε σε παραβίαση δεδομένων -.
* ελάχιστο περιεχόμενο γνωστοποίησης :

(α) φύση της παραβίασης,

(β) όνομα και στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων,

(γ) ενδεχόμενες συνέπειες της παραβίασης,

(δ) ληφθέντα ή προτεινόμενα μέτρα.

**(Β) Ανακοίνωση στα υποκείμενα των δεδομένων**

Η υποχρέωση αυτή, σε αντίθεση με τη γνωστοποίηση, υπάρχει μόνο σε περίπτωση που από την παραβίαση απορρέει «υψηλός κίνδυνος» για τα δικαιώματα και τις ελευθερίες των θιγόμενων προσώπων. Σ’ αυτή την περίπτωση, ο υπεύθυνος επεξεργασίας οφείλει να ανακοινώσει αμελλητί την παραβίαση στο υποκείμενο των δεδομένων.

Η ανακοίνωση έχει ως βασικό σκοπό την εξειδικευμένη ενημέρωση ως προς τα μέτρα που πρέπει να λάβουν τα υποκείμενα των δεδομένων για την προστασία τους.

Εξαίρεση από την υποχρέωση αυτή υπάρχει, όταν

1. ο υπεύθυνος επεξεργασίας είχε λάβει τα κατάλληλα οργανωτικά και τεχνικά μέτρα, με αποτέλεσμα τα παρανόμως παραβιασθέντα δεδομένα να μην είναι κατανοητά στους διαθέτοντες άδεια πρόσβασης πχ κρυπτογράφηση
2. υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα ικανά να αποτρέψουν την έλευση του υψηλού κινδύνου που αποτελεί προϋπόθεση της υποχρέωσης ανακοίνωσης
3. απαιτούνται δυσανάλογες προσπάθειες. Σε τέτοιες περιπτώσεις, γίνεται δημόσια ανακοίνωση ή υιοθετείται άλλο ανάλογο μέτρο.

**(Γ) Συνέπειες μη τήρησης της υποχρέωσης γνωστοποίησης και ανακοίνωσης**

Σε περιπτώσεις παραβίασης δεδομένων προσωπικού χαρακτήρα, η παράλειψη γνωστοποίησης στον αρμόδιο εποπτικό οργανισμό και ανακοίνωσης στα αφορώντα υποκείμενα, αντιστοίχως συνιστά παράβαση του ΓΚΠΔ. Επ’ αυτού, η αρμόδια Αρχή μπορεί να επιβάλλει διαρθρωτικά μέτρα (άρθρο 58 παρ. 2) και ταυτόχρονα διοικητικές κυρώσεις (άρθρο 83 παρ. 4).

Όπως προσφυώς επισημαίνει η καθ. Λίλιαν Μήτρου[[1]](#footnote-1): «*Η δημοσιότητα που ενδέχεται να προκύψει, κυρίως ως αποτέλεσμα της ανακοίνωσης της παραβίασης στα υποκείμενα των δεδομένων έχει επιπτώσεις στην αξιοπιστία και τη φήμη ενός οργανισμού, στοιχεία ιδιαίτερης (της περιουσιακής συμπεριλαμβανομένης) σημασίας για την ίδια την ύπαρξη ενός οργανισμού ιδίως στο πλαίσιο του ιδιωτικού τομέα. Εκτιμάται ότι ο κίνδυνος της αρνητικής δημοσιότητας μπορεί να ενισχύσει τη συνειδητοποίηση των προβλημάτων και των απαιτήσεων ασφάλειας πληροφοριακών συστημάτων και πληροφοριών αλλά και των επιπτώσεων της παραβίασής τους. Καθώς θεωρείται ότι ο φόβος για τις συνέπειες μιας τέτοιας «αποκάλυψης» ως προς τη φήμη του οργανισμού θα ωθήσει τους υπεύθυνους επεξεργασίας σε μια συνεπέστερη αξιολόγηση των κινδύνων, εκτιμάται ότι το μέτρο αυτό θα ενισχύσει το επίπεδο ασφάλειας αλλά και τη γενικότερη συμμόρφωση προς τις επιταγές της νομοθεσίας*» (σελ. 227-228, συλλογή άρθρων)

**(ΙV) Εκτίμηση αντικτύπου και προηγούμενη διαβούλευση** (άρθρο 35 - 36 ΓΚΠΔ)

Ορισμός: πρόκειται για επαναλαμβανόμενο σύνολο ενεργειών, οι οποίες αντιστοιχούν σε υποχρέωση του υπεύθυνου επεξεργασίας, στις περιπτώσεις επεξεργασιών υψηλού κινδύνου, ιδίως με τη χρήση νέων τεχνολογιών.

Περιεχόμενο της ανάλυσης : εδώ, εμπίπτουν η ανάλυση

* της φύσης,
* του πεδίου εφαρμογής και
* των σκοπών της επεξεργασίας.

Στο πλαίσιο της αρχής της αναλογικότητας, αξιολογείται

* η σοβαρότητα των επαπειλούμενων κινδύνων για τα δικαιώματα και τις ελευθερίες των ατόμων,
* η πιθανότητα έλευσης του κινδύνου.

Στόχος : λήψη των οργανωτικών και τεχνικών μέτρων που απαιτούνται προκειμένου να εναρμονιστούν οι υποχρεώσεις του υπεύθυνου επεξεργασίας με τις προβλέψεις του ΓΚΠΔ.

**Πώς συνδέεται η εκτίμηση αντικτύπου με την ενίσχυση συμμόρφωσης προς τον ΓΚΠΔ**

Όταν οι πράξεις επεξεργασίας ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, είναι σημαντικό ο υπεύθυνος επεξεργασίας να έχει προηγουμένως αποτυπώσει τις εκτιμήσεις του σε σχέση με τους επικείμενους κινδύνους (προέλευση, φύση, πιθανότητα, σοβαρότητα του κινδύνου). Το αποτέλεσμα της εκτίμησης θα πρέπει να συνεκτιμάται κατά την πρόταση περί λήψης των αναγκαίων μέτρων ώστε η επεξεργασία να είναι σύμφωνη με τις αρχές του ΓΚΠΔ

Πότε διενεργείται:

Kατά τα στάδια

* ανάλυσης απαιτήσεων, καθορισμού προδιαγραφών, αναλυτικής σχεδίασης.
* επικύρωσης
* επαλήθευσης

**Ενδεικτικές περιπτώσεις, όπου απαιτείται η εκτίμηση αντικτύπου:**

* συστηματική αξιολόγηση προσωπικών πτυχών που αφορούν φυσικά πρόσωπα (αυτοματοποιημένη επεξεργασία, προφίλ), η οποία αποτελεί τη βάση για τη λήψη αποφάσεων που επηρεάζουν σημαντικά το φυσικό πρόσωπο.
* ευρείας κλίμακας επεξεργασία δεδομένων ειδικών κατηγοριών (πχ σχετικά με ποινικές καταδίκες)
* συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

**Κριτήρια ως προς την υπαγωγή μιας κατηγορίας δεδομένων στις περιπτώσεις, όπου απαιτείται η εκτίμηση αντικτύπου λόγω υψηλής επικινδυνότητας για τα δικαιώματα και τις ελευθερίες των ατόμων:**

* αξιολόγηση, βαθμολόγηση, κατάρτιση προφίλ, πρόγνωση συναρτώμενη ιδίως με την οικονομική κατάσταση του ατόμου, υγεία, εργασιακή απόδοση, αξιοπιστία κλπ πχ επεξεργασία προσωπικών δεδομένων από τραπεζικούς οργανισμούς σε σχέση με την πιστοληπτική ικανότητα
* αυτοματοποιημένη λήψη αποφάσεων με έννομες συνέπειες, αφορώσες τον αποκλεισμό ή τη δυσμενή διάκριση των υποκειμένων
* συστηματική παρακολούθηση με στόχο παρακολούθηση ή έλεγχο ατόμων ενδεχομένως και εν αγνοία τους, με ενδεχόμενο κίνδυνο τη δυσμενή διάκρισή τους
* δεδομένα ειδικών κατηγοριών ή ειδικής προσωπικής φύσης – εδώ εμπίπτουν και τα ευαίσθητα δεδομένα πχ φυλετική καταγωγή, πολιτικές πεποιθήσεις, υγεία κ.λπ.
* επεξεργασία δεδομένων μεγάλης κλίμακας πχ ευρείς γεωγραφικές περιφέρειες και ιδίως, όταν από τις πράξεις επεξεργασίας εξαρτάται η άσκηση δικαιωμάτων των δεδομένων των υποκειμένων
* διασύνδεση ή αντιστοίχιση δεδομένων προερχόμενων από επεξεργασία κατά τρόπο μη αναμενόμενο από τα υποκείμενα
* δεδομένα που αφορούν σε ευάλωτα άτομα ή ομάδες, κυρίως, παιδιά, εργαζόμενοι, σωματικώς ή ψυχικώς ασθενείς
* χρήση νέων τεχνολογιών
* επεξεργασίες που στόχο έχουν να επιτρέψουν ή να αποτρέψουν την άσκηση δικαιώματος πχ έλεγχος βάσης δεδομένων πιστοληπτικής ικανότητας πριν τη χορήγηση δανείου

**Η εποπτική αρχή ανακοινώνει στο Συμβούλιο Προστασίας Δεδομένων του άρθρου 68**

(α) κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων

(β) κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων – τον κατάλογο αυτό η αρχή καταρτίζει και ανακοινώνει προαιρετικά

**Σε ποιες επεξεργασίες δεν απαιτείται εκτίμηση αντικτύπου**

Ενδεικτικά :

(α) σε περιπτώσεις που δεν εμπίπτουν στα προαναφερθέντα κριτήρια

(β) σε νέες επεξεργασίες, των οποίων το πλαίσιο, η φύση, ο σκοπός είναι παρόμοια με άλλης επεξεργασίας περί της οποίας έχει πραγματοποιηθεί ήδη εκτίμηση αντικτύπου

**Η εκτίμηση αντικτύπου απαιτείται ιδίως, σε περιπτώσεις:**

1. συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,
2. μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών ευαίσθητων δεδομένων (άρθρο 9 παρ. 1) ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα (άρθρο 10) ή
3. συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

O υπεύθυνος επεξεργασίας, ο οποίος φέρει την ευθύνη για τις πράξεις επεξεργασίας που πραγματοποιεί

(α) ζητά τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί.

(β) ζητά τις απόψεις των υποκειμένων των δεδομένων, εκτός αν υπάρχει ειδικός λόγος (πχ διαφύλαξη εμπιστευτικών πληροφοριών)

(γ) ζητά απόψεις ειδικών στην προστασία δεδομένων (νομικών, τεχνικών κλπ) ή ειδικών σε θέματα ηθικής ή πχ εκείνων που εμπλέκονται με τον καθορισμό των επιχειρηματικών σχεδίων.

Για την εκπόνηση της εκτίμησης αντικτύπου υπάρχουν σχετικά διεθνή πρότυπα ISO.

**Περιεχόμενο της εκτίμησης κινδύνου**

Η εκτίμηση περιέχει τουλάχιστον:

1. συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, με αναφορά στο έννομο συμφέρον, την ικανοποίηση του οποίου επιδιώκει ο υπεύθυνος επεξεργασίας,
2. παραβολή της αναγκαιότητας και αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς της επεξεργασίας,
3. εκτίμηση των κινδύνων που διατρέχουν τα δικαιώματα και οι ελευθερίες των αφορώντων υποκειμένων
4. τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων – εγγυήσεις, μέτρα, μηχανισμοί ασφάλειας, με στόχο

(i) προστασία των δεδομένων προσωπικού χαρακτήρα

(ii) συμμόρφωση προς τον ΓΚΠΔ, συνεκτιμώντας τα δικαιώματα και έννομα συμφέροντα των αφορώντων υποκειμένων και άλλων ενδιαφερόμενων προσώπων.

Εξυπακούεται ότι το αποτέλεσμα της εκτίμησης θα πρέπει να λαμβάνεται υπόψη κατά τον καθορισμό των ενδεικνυόμενων μέτρων ώστε να διασφαλισθεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι σύμφωνη με τον ΓΚΠΔ.

**Πότε είναι αναγκαία η διαβούλευση με την εποπτική αρχή (άρθρο 36 παρ.1)**

(i) αν η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι οι πράξεις επεξεργασίας συνεπάγονται υψηλό κίνδυνο και

(ii) ο υπεύθυνος επεξεργασίας δε μπορεί να μετριάσει με τα κατάλληλα μέτρα από άποψη διαθέσιμης τεχνολογίας και κόστους εφαρμογής,

(iii) τότε, θα πρέπει της επεξεργασίας, να πραγματοποιείται διαβούλευση με την αρχή ελέγχου.

Στο πλαίσιο αυτής της διαβούλευσης με την εποπτική αρχή, ο υπεύθυνος επεξεργασίας παρέχει στην εποπτική αρχή:

1. κατά περίπτωση, τις αντίστοιχες αρμοδιότητες του υπευθύνου επεξεργασίας, των από κοινού υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία που συμμετέχουν στις εργασίες, ιδίως όσον αφορά επεξεργασία εντός ομίλου επιχειρήσεων,
2. τους σκοπούς και τα μέσα της σχεδιαζόμενης επεξεργασίας,
3. τα μέτρα και τις εγγυήσεις για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σύμφωνα με τον παρόντα κανονισμό,
4. κατά περίπτωση, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων,
5. την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων που προβλέπεται στο άρθρο 35, και
6. κάθε άλλη πληροφορία που ζητεί η εποπτική αρχή.

**(V) ΚΩΔΙΚΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ** (άρθρα 40-41 ΓΚΠΔ)

Ο ΓΚΠΔ ενθαρρύνει την κατάρτιση κωδίκων δεοντολογίας, με στόχο την ορθή εφαρμογή του κανονισμού. Ορίζει δε ότι «ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας» προκειμένου να εξειδικεύουν την εφαρμογή του κανονισμού στο θεματικό πεδίο των αρμοδιοτήτων τους (ενδεικτικά : διαδικασία θεμιτής και διαφανούς επεξεργασίας, συλλογή δεδομένων προσωπικού χαρακτήρα, ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα, άσκηση δικαιωμάτων των υποκειμένων των δεδομένων κλπ).

Οι Κώδικες δεοντολογίας μπορούν να υποβληθούν στην αρμόδια αρχή, η οποία γνωμοδοτεί επί του σχεδίου και προχωρεί σε έγκριση, εφόσον παρέχονται οι αναγκαίες από τον ΓΚΠΔ εγγυήσεις. Υπάρχει επίσης, η δυνατότητα να αποκτήσουν γενική ισχύ εντός της Ένωσης, μετά την έκδοση εκτελεστικής πράξης (άρθρο 40 παρ. 9).

**ΜΗΧΑΝΙΣΜΟΙ ΠΙΣΤΟΠΟΙΗΣΗΣ** (άρθρα 42 – 43 ΓΚΠΔ)

Ο ΓΚΠΔ προτρέπει επίσης για τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων. Ειδικότερα : σφραγίδες, σήματα, τεχνικά πρότυπα, με σκοπό την απόδειξη τήρησης των υποχρεώσεων που απορρέουν από τον ΓΚΠΔ.

Πάντως, πρόκειται για εθελοντική, μη δεσμευτική διαδικασία, η οποία δεν περιορίζει την ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για συμμόρφωση προς τον παρόντα κανονισμό, ούτε θίγει τις αρμοδιότητες των εποπτικών αρχών.

Το μεγαλύτερο όφελος από τη χρήση των μηχανισμών πιστοποίησης συνίσταται στην ασφαλή απόδειξη περί συμμόρφωσης του υπεύθυνου επεξεργασίας με τις επιταγές του ΓΚΠΔ.

Η πιστοποίηση χορηγείται για μέγιστη περίοδο μέχρι τρία έτη και εφόσον πληρούνται οι προϋποθέσεις, μπορεί να ανανεωθεί με τους ίδιους όρους. Ομοίως, η πιστοποίηση ανακαλείται όταν παύουν να πληρούνται οι αναγκαίες προϋποθέσεις.

Το σύνολο των μηχανισμών πιστοποίησης υπάρχει διαθέσιμο σε ειδικό μητρώο που τηρείται στο Συμβούλιο Προστασίας Δεδομένων.

1. Υποχρεώσεις του υπεύθυνου επεξεργασίας [↑](#footnote-ref-1)