ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΆ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΊΑ ΔΕΔΟΜΈΝΩΝ ΑΡΘΡ. 35 ΓΚΠΔ

Ιωάννης Ιγγλεζάκης
Αν. καθηγητής Νομ. Σχολής ΑΠΘ

Κανονισμός 2016/679/ΕΕ

- Τμήμα 3

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

- Άρθρο 35 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Τι είναι η Εκτίμηση Αντικτύπου Προστασίας δεδομένων (DPIA)

- Η διαδικασία που ακολουθείται για να περιγράψει την επεξεργασία δεδομένων, να αξιολογήσει την αναγκαιότητα και προσφορότητα της επεξεργασίας και να διαχειριστεί τους κινδύνους για τα δικαιώματα των προσώπων που προκύπτουν από την επεξεργασία των προσωπικών τους δεδομένων, αξιολογώντας τους κινδύνους αυτούς και βρίσκοντας μέτρα αντιμετώπισής τους.
- Εφαρμογή της αρχής της λογοδοσίας, αφού οι υπεύθυνοι επεξεργασίας όχι μόνο συμμορφώνονται με τον ΓΚΠΔ, αλλά και επιδεικνύουν ότι έλαβα μέτρα συμμόρφωσης.

Συνέπειες από την παράλειψη διενέργειας εκτίμησης αντικτύπου

- Άρθρο 82 ΓΚΠΔ – ευθύνη προς αποζημίωση για τη ζημία που προκαλείται, όταν δεν συμμορφώνεται με τον Κανονισμό
- Άρθρο 83 ΓΚΠΔ - 4. Παραβάσεις των ακόλουθων διατάξεων επισύρουν, σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 10 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο:
- α) οι υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία σύμφωνα με τα άρθρα 8, 11, *25 έως 39* και 42 και 43 …

Ιστορία του θεσμού της εκτίμησης αντικτύπου

- 1970s - Technology Assessment (TA) was created by the United States Office of Technology Assessment to determine the societal and social repercussions of new technologies. Similarly the Environmental Impact Assessments (EIA). The methodology of both of these impact assessments acted as precursors to the creation of the PIA.
- 1990s extensive PIAs started to be used more frequently by corporations and governments in the mid 1990s, and now are used by organizations all around the world, and by several governments including, New Zealand, Canada, Australia, and the United States Department of Homeland Security to assess privacy risk of their systems
- The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections

Προϋποθέσεις

- Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδια-ζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

Περιπτώσεις όπου απαιτείται η εκτίμηση αντικτύπου

- Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:
- α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματο-ποιημένη 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, β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Υποχρεωτικότητα

1

Η εκτίμηση αντικτύπου είναι υποχρεωτική μόνον όταν η επεξεργασία έχει ως αποτέλεσμα υψηλό κίνδυνο

2

Όταν δεν είναι σαφές αν πρέπει να γίνει, συνιστάται να διενεργείται, διότι είναι ένα χρήσιμο εργαλείο συμμόρφωσης

Εκτίμηση κινδύνων

- Κίνδυνοι είναι δυνατόν να προκύπτουν από την επεξεργασία δεδομένων η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη, ιδίως όταν η επεξεργασία μπορεί να οδηγήσει σε διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, βλάβη φήμης, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο, παράνομη άρση της ψευδωνυμοποίησης, ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα· όταν τα υποκείμενα των δεδομένων θα μπορούσαν να στερηθούν των δικαιωμάτων και ελευθεριών τους ή να εμποδίζονται από την άσκηση ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα· όταν υπόκεινται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα και γίνεται επεξεργασία γενετικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας· όταν αξιολογούνται προσωπικές πτυχές, ιδίως όταν επιχειρείται ανάλυση ή πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή μετακινήσεις, προκειμένου να δημιουργηθούν ή να χρησιμοποιηθούν προσωπικά προφίλ· όταν υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα ευάλωτων φυσικών προσώπων, ιδίως παιδιών· ή όταν η επεξεργασία περιλαμβάνει μεγάλη ποσότητα δεδομένων προσωπικού χαρακτήρα και επηρεάζει μεγάλο αριθμό υποκειμένων των δεδομένων.

Παραδείγματα

- Scoring από τράπεζες, δημιουργία προφίλ στο μάρκετινγκ
- Αυτόματο profiling που οδηγεί σε διακρίσεις
- Συστηματική παρακολούθηση, π.χ.:
  - Χρήση συστήματος βιντεοσκόπησης για την παρακολούθηση της οδικής συμπεριφοράς σε αυτοκινητοδρόμους (έξυπνο σύστημα ανάλυσης βίντεο που απομονώνει τα οχήματα και αναγνωρίζει αυτόματα τις πινακίδες τους).
  - Εταιρεία που παρακολουθεί συστηματικά τις δραστηριότητες των εργαζομένων της, καθώς και τον σταθμό εργασίας τους, τη δραστηριότητά τους στο διαδίκτυο κ.ο.κ.
- Δεδομένα μεγάλης κλίμακας
  - συλλογή δεδομένων στα social media για την κατάρτιση προφίλ

Παραδείγματα

- Επεξεργασία ευαίσθητων δεδομένων (ιατρικά αρχεία ασθενών που τηρεί ένα γενικό νοσοκομείο ή τα προσωπικά στοιχεία παραβατών που τηρεί ένας πράκτορας ιδιωτικών ερευνών)
- Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων (παιδιά, εργαζόμενοι, ασθενείς, ψυχικά νοσούντες, αιτούντες άσυλο κοκ)
- Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων (συνδυασμένη χρήση δακτυλικών αποτυπωμάτων, αναγνώριση προσώπου)

Παραδείγματα

Οργανισμός που δημιουργεί εθνική βάση δεδομένων αξιολόγησης της πιστοληπτικής ικανότητας ή υποθέσεων απάτης.

Αποθήκευση για λόγους αρχείου ψευδωνυμοποιημένων ευαίσθητων δεδομένων προσωπικού χαρακτήρα που αφορούν ευάλωτα υποκείμενα δεδομένων σε ερευνητικά έργα ή κλινικές δοκιμές.

Παραδείγματα όπου δεν απαιτείται εκτίμηση αντικτύπου

- Ηλεκτρονικό περιοδικό που χρησιμοποιεί κατάλογο ηλεκτρονικών διευθύνσεων για να αποστέλλει γενικές ημερήσιες συνόψεις στους συνδρομητές του.
  - Δεδομένα μεγάλης κλίμακας επεξεργασίας.
- Δικτυακός τόπος ηλεκτρονικού εμπορίου που διαφημίζει ανταλλακτικά αυτοκινήτων-αντικών και περιλαμβάνει περιορισμένη κατάρτιση προφίλ βάσει των αντικειμένων που έχουν προβληθεί ή αγοραστεί στον δικτυακό του τόπο.
  - Αξιολόγηση ή βαθμολόγηση.

Περιπτώσεις όπου απαιτείται η εκτίμηση αντικτύπου

- Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

Κατάλογοι

- Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.
- Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

Τι ισχύει για τις ήδη υφιστάμενες πράξεις επεξεργασίας;

Η απαίτηση διενέργειας ΕΑΠΔ ισχύει σε υφιστάμενες πράξεις επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και στις οποίες έχει επέλθει μεταβολή των κινδύνων, λαμβανομένης υπόψη της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας.

Δεν απαιτείται ΕΑΠΔ σε πράξεις επεξεργασίας που έχουν ελεγχθεί από εποπτική αρχή ή τον υπεύθυνο υπάλληλο προστασίας δεδομένων, σύμφωνα με το άρθρο 20 της οδηγίας 95/46/ΕΚ, και υλοποιούνται χωρίς καμία μεταβολή από τον προηγούμενο έλεγχο

Πότε θα πρέπει να διενεργείται η ΕΑΠΔ

Η ΕΑΠΔ θα πρέπει να διενεργείται «*πριν από την επεξεργασία*» (άρθρο 35 παράγραφος 1 και άρθρο 35 παράγραφος 10, αιτιολογικές σκέψεις 90 και 93). Τούτο συνάδει με τις αρχές της εξ ορισμού και της εκ σχεδιασμού προστασίας των δεδομένων (άρθρο 25 και αιτιολογική σκέψη 78). Η ΕΑΠΔ θα πρέπει να αντιμετωπίζεται ως εργαλείο που βοηθά στη λήψη αποφάσεων σε σχέση με την επεξεργασία.

η ΕΑΠΔ ενδέχεται να χρειαστεί επικαιροποίηση μετά την έναρξη της επεξεργασίας

Η ΕΑΠΔ αποτελεί διαρκή διαδικασία και όχι πράξη που διενεργείται άπαξ

Ποιος οφείλει να διενεργεί την ΕΑΠΔ

Ο υπεύθυνος επεξεργασίας είναι αρμόδιος. Μπορεί να πραγματοποιηθεί από άλλο πρόσωπο, εντός ή εκτός του οργανισμού, ωστόσο ο υπεύθυνος επεξεργασίας παραμένει ο τελικός υπεύθυνος.

Ο υπεύθυνος επεξεργασίας πρέπει επίσης να ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων (ΥΠΔ), εφόσον έχει οριστεί και η γνώμη του και οι αποφάσεις του υπεύθυνου επεξεργασίας πρέπει να τεκμηριώνονται στην ΕΑΠΔ. Ο ΥΠΔ θα πρέπει επίσης να παρακολουθεί την υλοποίηση της ΕΑΠΔ

Ο εκτελών την επεξεργασία θα πρέπει να συνδράμει τον υπεύθυνο επεξεργασίας στη διενέργεια της ΕΑΠΔ και να παράσχει κάθε αναγκαία πληροφορία

Περιεχόμενο (κατ' ελάχιστον)

α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (εγγυήσεις, μέτρα και μηχανισμοί ασφάλειας, για τη διασφάλιση προστασίας των δεδομένων και απόδειξη της συμμόρφωσης προς τον κανονισμό

Αξιολόγηση κινδύνων

- 1. Αμελητέος κίνδυνος: όταν δεν είναι πιθανό να επέλθει κίνδυνος στα προστατευόμενα αγαθά (π.χ., να συμβεί κλοπή εγγράφων που φυλάσσονται σε ένα δωμάτιο το οποίο προστατεύεται με μηχανισμό ελέγχου με κάρτα και με κωδικό πρόσβασης)
- 2. Περιορισμένος κίνδυνος: όταν φαίνεται δύσκολο είναι να επέλθει κίνδυνος στα προστατευόμενα αγαθά (π.χ., να συμβεί κλοπή εγγράφων που φυλάσσονται σε ένα δωμάτιο με μηχανισμό ελέγχου με κάρτα)
- 3. Σημαντικός κίνδυνος: όταν είναι πιθανό να επέλθει κίνδυνος στα προστατευόμενα αγαθά (π.χ., κλοπή εγγράφων από ένα γραφείο στο οποίο πρόσβαση υπάρχει μόνο μετά αφού περάσει κανείς από τη reception.
- 4. Μέγιστος κίνδυνος: όταν είναι πολύ εύκολο να επισυμβεί κίνδυνος (π.χ., να κλαπούν έγγραφα που φυλάσσονται στην αίθουσα αναμονής).

Μέτρα προστασίας

Protection goal	Component	Measure
Ensuring availability	Data, systems, processes	Redundancy, protection, repair strategies
Ensuring integrity	Data	Comparing hash values
	Systems	Limitation of write permissions, regular integrity checks
	Processes	Setting references values (min/max), control of regulation
Ensuring confidentiality	Data, systems	Encryption
	Processes	Rights and roles concepts
Ensuring unlinkability through definitions of purposes	Data	Anonymity, pseudonymity, attribute-based credentials
	Systems	Separation (isolation) of stored data, systems and processes
	Processes	Identity management, anonymity infrastructures, audits
Ensuring unlinkability through definitions of purposes	Data	Documentation, logging
	Systems	System documentation, logging of configuration changes
	Processes	Documentation of procedures, logging
Ensuring intervenability through anchor points	Data	Access of persons concerned to their data (information, rectification, blocking, deletion)
	Systems	Off-switch
	Processes	Helpdesk/single point of contact for modification/deletion, change management

παραδείγματα

- Π.χ., στην αποθήκευση δεδομένων προσωπικού χαρακτήρα σε φορητούς υπολογιστές για τη μείωση κινδύνου να γίνεται χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας (αποτελεσματική πλήρης κρυπτογράφηση δίσκου, ισχυρή διαχείριση κλειδιών, κατάλληλος έλεγχος πρόσβασης, ασφαλή εφεδρικά αντίγραφα κ.ο.κ.) πλέον των υφιστάμενων πολιτικών (ειδοποίηση, συναίνεση, δικαίωμα πρόσβασης, δικαίωμα εναντίωσης κ.ο.κ.).
- Όταν τα υποκείμενα των δεδομένων μπορεί να υποστούν σημαντικές, ή ακόμη και μη αναστρέψιμες, επιπτώσεις τις οποίες ενδέχεται να μην ξεπεράσουν (π.χ.: αθέμιτη πρόσβαση σε δεδομένα που ενέχει απειλή για τη ζωή των υποκειμένων των δεδομένων, απόλυση, οικονομική διακινδύνευση) και/ή όταν καθίσταται προφανές ότι θα επέλθει ο κίνδυνος (π.χ.: όταν δεν είναι δυνατή η μείωση του αριθμού των προσώπων που έχουν πρόσβαση στα δεδομένα λόγω των τρόπων διαμοιρασμού, χρήσης ή διανομής ή όταν δεν καλύπτεται ένα ήδη γνωστό τρωτό σημείο).

Δημοσίευση

Η δημοσίευση της ΕΑΠΔ δεν συνιστά νομική απαίτηση του ΓΚΠΔ και αποτελεί απόφαση του υπεύθυνου επεξεργασίας. Ωστόσο, οι υπεύθυνοι επεξεργασίας θα πρέπει να εξετάζουν το ενδεχόμενο δημοσίευσης τουλάχιστον αποσπασμάτων αυτής, όπως σύνοψη ή συμπέρασμα της ΕΑΠΔ τους.

Σκοπός η προαγωγή της εμπιστοσύνης στις πράξεις επεξεργασίας του υπεύθυνου επεξεργασίας και η απόδειξη της διαφάνειας και της εκπλήρωσης της υποχρέωσης λογοδοσίας.

Ορθή πρακτική η δημοσίευση της ΕΑΠΔ σε πράξη επεξεργασίας που επηρεάζει το κοινό, ιδίως σε περίπτωση διενέργειας ΕΑΠΔ από δημόσια αρχή.

Συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων

- Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

Κώδικες Δεοντολογίας

- Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας που αναφέρονται στο άρθρο 40 από τους σχετικούς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

Διαβούλευση με τα υποκείμενα των δεδομένων

- Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

Εξαίρεση από την υποχρέωση διενέργειας εκτίμησης αντικτύπου

- Όταν η επεξεργασία δυνάμει του άρθρου 6 παράγραφος 1 στοιχείο γ) ή ε) έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης, οι παράγραφοι 1 έως 7 δεν εφαρμόζονται, εκτός εάν τα κράτη μέλη κρίνουν απαραίτητη τη διενέργεια της εν λόγω εκτίμησης πριν από τις δραστηριότητες επεξεργασίας

Επανεξέταση

- Όπου απαιτείται, ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας.

Προηγούμενη διαβούλευση

- Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη της εποπτικής αρχής πριν από την επεξεργασία, όταν η δυνάμει του άρθρου 35 εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας.
- *(με άλλη διατύπωση)* Όταν οι υπολειπόμενοι κίνδυνοι είναι υψηλοί.

Προηγούμενη διαβούλευση (συνέχεια)

- Όταν η εποπτική αρχή φρονεί ότι η σχεδιαζόμενη επεξεργασία που αναφέρεται στην παράγραφο 1 παραβαίνει τον παρόντα κανονισμό, ιδίως εάν ο υπεύθυνος επεξεργασίας δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο, η εποπτική αρχή παρέχει γραπτώς συμβουλές στον υπεύθυνο επεξεργασίας εντός προθεσμίας μέχρι οκτώ εβδομάδων από την παραλαβή του αιτήματος διαβούλευσης, και, όπου απαιτείται, στον εκτελούντα την επεξεργασία, ενώ δύναται να χρησιμοποιήσει οποιαδήποτε από τις εξουσίες της που αναφέρονται στο άρθρο 58. Η εν λόγω προθεσμία μπορεί να παραταθεί κατά έξι εβδομάδες, λόγω της πολυπλοκότητας που χαρακτηρίζει τη σχεδιαζόμενη επεξεργασία. Η εποπτική αρχή ενημερώνει τον υπεύθυνο επεξεργασίας και, όπου απαιτείται, τον εκτελούντα την επεξεργασία για την εν λόγω παράταση εντός ενός μηνός από την παραλαβή του αιτήματος διαβούλευσης, καθώς και για τους λόγους της καθυστέρησης. Οι εν λόγω προθεσμίες μπορούν να αναστέλλονται έως ότου η εποπτική αρχή λάβει τις πληροφορίες που ζήτησε για τους σκοπούς της διαβούλευσης.

Ο υπεύθυνος επεξεργασίας παρέχει στην εποπτική αρχή

- Κατά τη διαβούλευση με την εποπτική αρχή: α) 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, β) τους σκοπούς και τα μέσα της σχεδιαζόμενης επεξεργασίας, γ) τα μέτρα και τις εγγυήσεις για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σύμφωνα με τον παρόντα κανονισμό, δ) κατά περίπτωση, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, ε) την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων που προβλέπεται στο άρθρο 35, και στ) κάθε άλλη πληροφορία που ζητεί η εποπτική αρχή.