ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 16-10-2018

Αριθ. Πρωτ.: Γ/ΕΞ/8187/16-10-2018

**Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ**

*Νομική βάση*

Σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ, 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 δεδομένων (ΕΑΠΔ) δυνάμει της παρ. 1 και ανακοινώνει τον κατάλογο αυτό στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ).

Εάν ο κατάλογος αυτός περιλαμβάνει δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάσουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων στην Ένωση, εφαρμόζεται ο μηχανισμός συνεκτικότητας που αναφέρεται στο άρθρο 63.

*Πλαίσιο*

Η διενέργεια ΕΑΠΔ απαιτείται όταν ένα είδος επεξεργασίας, ιδίως με τη 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 (άρθρο 35 παρ. 1 του ΓΚΠΔ). Ενδεικτικές περιπτώσεις στις οποίες απαιτείται διενέργεια ΕΑΠΔ παρατίθενται στο άρθρο 35 παρ. 3 του ΓΚΠΔ.

Για την παροχή πιο συνεκτικού συνόλου πράξεων επεξεργασίας που απαιτούν τη διενέργεια ΕΑΠΔ λόγω του υψηλού κινδύνου που ενέχουν, η Ομάδα Εργασίας του Άρθρου 29 εξέδωσε τις κατευθυντήριες γραμμές με τίτλο «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679» (WP248 rev.01). Οι παραπάνω κατευθυντήριες γραμμές ορίζουν εννέα κριτήρια τα οποία πρέπει να χρησιμοποιούν οι υπεύθυνοι επεξεργασίας για να καθορίσουν κατά πόσον πρέπει να διενεργηθεί ή όχι ΕΑΠΔ.

*Ορισμός της μεγάλης κλίμακας*

Κατά τον προσδιορισμό του κατά πόσον η επεξεργασία τελείται σε μεγάλη κλίμακα συνιστάται να λαμβάνονται συγκεκριμένα υπόψη οι ακόλουθες παράμετροι βάσει των προαναφερθεισών κατευθυντήριων γραμμών WP248 καθώς και των κατευθυντήριων γραμμών με τίτλο «Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων» (WP243):

α. ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού·

β. ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία·

γ. η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων·

δ. το γεωγραφικό εύρος της δραστηριότητας επεξεργασίας.

*Πράξεις επεξεργασίας που υπόκεινται σε απαίτηση ΕΑΠΔ*

Ο παρών κατάλογος ομαδοποιεί και εξειδικεύει περαιτέρω τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια ΕΑΠΔ με παράθεση και ενδεικτικών παραδειγμάτων. Ο εν λόγω κατάλογος δεν είναι εξαντλητικός και δεν αίρεται ούτε μεταβάλλεται η υποχρέωση να διενεργείται ΕΑΠΔ σε κάθε περίπτωση συνδρομής των προϋποθέσεων του άρθρου 35 παρ. 1 του ΓΚΠΔ. Ο εν λόγω κατάλογος βασίζεται στο άρθρο 35 του ΓΚΠΔ και ιδίως στις παρ. 1 και 3 αυτού καθώς και στις κατευθυντήριες γραμμές για την εκτίμηση αντικτύπου (WP248), τις οποίες συμπληρώνει και εξειδικεύει περαιτέρω.

Τα κριτήρια για την διενέργεια ΕΑΠΔ ομαδοποιούνται στις παρακάτω τρεις κατηγορίες:

- *1η κατηγορία:* με βάση τα είδη και τους σκοπούς επεξεργασίας.
- *2η κατηγορία:* με βάση το είδος των δεδομένων και/ή τις κατηγορίες των υποκειμένων.
- *3η κατηγορία:* με βάση τα πρόσθετα χαρακτηριστικά και/ή τα χρησιμοποιούμενα μέσα της επεξεργασίας.

Η διενέργεια ΕΑΠΔ κρίνεται υποχρεωτική όταν πληρούται τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας. Είναι επίσης υποχρεωτική όταν συντρέχει ένα τουλάχιστον κριτήριο ως προς την 3η κατηγορία και η επεξεργασία αφορά είδη και σκοπούς επεξεργασίας της 1ης κατηγορίας, ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της 2ης κατηγορίας.

*1η κατηγορία: είδη και σκοποί της επεξεργασίας*

1.1 Συστηματική αξιολόγηση, βαθμολόγηση, πρόβλεψη, πρόγνωση και κατάρτιση προφίλ, ιδίως πτυχών που αφορούν την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή τις κινήσεις ή την πιστοληπτική ικανότητα των υποκειμένων των δεδομένων.

Σχετικά παραδείγματα είναι η περίπτωση, κατά την οποία χρηματοπιστωτικό ίδρυμα ελέγχει τους πελάτες του με βάση δεδομένα πιστοληπτικής ικανότητας ή δεδομένα για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας ή δεδομένα για εγκλήματα απάτης, ή η περίπτωση, κατά την οποία εταιρεία βιοτεχνολογίας παρέχει απευθείας στους καταναλωτές γενετικές δοκιμές για να εκτιμήσει και να προβλέψει τους κινδύνους νόσου/υγείας.

1.2 Συστηματική επεξεργασία δεδομένων που αποσκοπεί στη λήψη αυτοματοποιημένων αποφάσεων, οι οποίες παράγουν έννομα αποτελέσματα σχετικά με τα υποκείμενα των δεδομένων ή επηρεάζουν σημαντικά τα υποκείμενα των δεδομένων κατά ανάλογο τρόπο και μπορούν να οδηγήσουν σε αποκλεισμό ή διακρίσεις σε βάρος του φυσικού προσώπου.

Σχετικά παραδείγματα είναι η αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση (αιτ. 71 του ΓΚΠΔ) ή η αυτόματη άρνηση ασφαλιστικής παροχής.

1.3 Συστηματική επεξεργασία δεδομένων που ενδέχεται να εμποδίζει το υποκείμενο να ασκήσει τα δικαιώματά του ή να χρησιμοποιήσει μια υπηρεσία ή σύμβαση, ιδίως όταν λαμβάνονται υπόψη δεδομένα που συλλέγονται από τρίτους.

Σχετικά παραδείγματα είναι η περίπτωση, κατά την οποία τράπεζα ελέγχει τους πελάτες της χρησιμοποιώντας μια βάση δεδομένων πιστοληπτικής ικανότητας για να αποφασίσει αν θα τους χορηγήσει δάνειο ή όχι, η καταχώρηση του υποκειμένου σε «μαύρη» λίστα, όπως η λίστα των παρόχων κινητής τηλεφωνίας (τηλέγνους), η καταχώριση του υποκειμένου σε whistleblowing συστήματα.

1.4 Συστηματική επεξεργασία δεδομένων που αφορά την κατάρτιση προφίλ για το σκοπό της προώθησης προϊόντων και υπηρεσιών εφόσον τα δεδομένα συνδυάζονται με δεδομένα που συλλέγονται από τρίτους.

1.5 Συστηματική και σε μεγάλη κλίμακα επεξεργασία για την παρακολούθηση, την παρατήρηση ή τον έλεγχο των φυσικών προσώπων με χρήση δεδομένων που συλλέγονται μέσω συστημάτων βιντεοεπιτήρησης ή μέσω δικτύων ή με οποιοδήποτε άλλο μέσο σε δημόσιο χώρο, δημοσίως προσβάσιμο χώρο ή ιδιωτικό χώρο προσιτό σε απεριόριστο αριθμό προσώπων. Περιλαμβάνει την παρακολούθηση των κινήσεων ή της τοποθεσίας/γεωγραφικής θέσης σε πραγματικό ή μη χρόνο ταυτοποιημένων ή ταυτοποιήσιμων φυσικών προσώπων.

Σχετικά παραδείγματα είναι η χρήση καμερών σε εμπορικό κέντρο ή σε σταθμούς μέσων μαζικής μεταφοράς, ή η επεξεργασία δεδομένων θέσης των επιβατών σε αεροδρόμιο ή σε μέσα μαζικής μεταφοράς. Επίσης, η παρακολούθηση μέσω wi-fi συστημάτων (wi-fi tracking) επισκεπτών σε εμπορικά κέντρα ή επεξεργασία δεδομένων μέσω drones.

1.6 Μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία και τη δημόσια υγεία για σκοπούς δημοσίου συμφέροντος,

όπως η εισαγωγή και χρήση συστημάτων ηλεκτρονικής συνταγογράφησης και η εισαγωγή και χρήση ηλεκτρονικού φακέλου ή ηλεκτρονικής κάρτας υγείας.

1.7 Μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό την εισαγωγή, οργάνωση, παροχή και έλεγχο της χρήσης υπηρεσιών ηλεκτρονικής διακυβέρνησης, όπως ορίζονται στο άρθρο 3 του ν.3979/2011 όπως ισχύει.

*2η κατηγορία: είδος δεδομένων ή/και κατηγορίες υποκειμένων*

2.1 Μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων (περιλαμβανομένων των γενετικών και των βιομετρικών με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου) που αναφέρονται στο άρθρο 9 παρ. 1 και των δεδομένων που αναφέρονται στο άρθρο 10 του ΓΚΠΔ.

2.2 Συστηματική και σε μεγάλη κλίμακα επεξεργασία δεδομένων ιδιαίτερης σημασίας ή εξαιρετικού χαρακτήρα όπως

2.2.1 δεδομένα κοινωνικής πρόνοιας (δεδομένα σχετικά με τη φτώχεια, την ανεργία, την κοινωνική εργασία κλπ.),

2.2.2 δεδομένα ηλεκτρονικών επικοινωνιών, περιλαμβανομένων των δεδομένων περιεχομένου όπως του ηλεκτρονικού ταχυδρομείου, μεταδεδομένων και των δεδομένων γεωγραφικής θέσης/τοποθεσίας, με εξαίρεση την καταγραφή τηλεφωνικών συνδιαλέξεων σύμφωνα με το άρθρο 4 παρ. 3 του ν.3471/2006,

2.2.3 δεδομένα που αφορούν εθνικό αριθμό ταυτότητας ή άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής ή αλλαγή των προϋποθέσεων και όρων επεξεργασίας και χρήσης αυτών και των συναφών με αυτά δεδομένων προσωπικού χαρακτήρα,

2.2.4 δεδομένα που περιλαμβάνονται σε προσωπικά έγγραφα, ημερολόγια, σημειώσεις από ηλεκτρονικό αναγνώστη (e-reader) και σε εφαρμογές καταγραφής βίου (life logging), που προσφέρουν δυνατότητες τήρησης σημειώσεων και πολύ προσωπικών πληροφοριών,

2.2.5 δεδομένα που συλλέγονται ή παράγονται από συσκευές (όπως αυτές με αισθητήρες) ιδίως μέσω των εφαρμογών του 'διαδικτύου των πραγμάτων - IoT' (όπως έξυπνες τηλεοράσεις, έξυπνες οικιακές συσκευές, συνδεδεμένα παιχνίδια, έξυπνες πόλεις, έξυπνοι μετρητές ενέργειας κλπ) και/ή με τη χρήση άλλων μέσων.

2.3 Συστηματική παρακολούθηση – εφόσον είναι επιτρεπτή – της θέσης/τοποθεσίας καθώς και του περιεχομένου και των μεταδεδομένων των επικοινωνιών των εργαζομένων με εξαίρεση τα αρχεία καταγραφής για λόγους ασφάλειας εφόσον η επεξεργασία περιορίζεται στα απολύτως απαραίτητα δεδομένα και είναι ειδικά τεκμηριωμένη. Σχετικό παράδειγμα που εμπίπτει στην υποχρέωση διενέργειας ΕΑΠΔ αποτελεί η χρήση συστημάτων DLP.

Συστηματική επεξεργασία βιομετρικών δεδομένων των εργαζομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου καθώς και γενετικών δεδομένων των εργαζομένων.

*3η κατηγορία: πρόσθετα χαρακτηριστικά ή/και χρησιμοποιούμενα μέσα της επεξεργασίας*

3.1 Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογιών ή οργανωτικών λύσεων, οι οποίες μπορεί να περιλαμβάνουν νέες μορφές συλλογής και χρήσης δεδομένων, με ενδεχόμενο υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όπως η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης, ή εφαρμογές mhealth ή άλλες «έξυπνες» εφαρμογές, από τις οποίες δημιουργείται προφίλ των χρηστών (π.χ. καθημερινές συνήθειες), ή εφαρμογές τεχνητής νοημοσύνης ή τεχνολογίες δημόσια προσπελάσιμων blockchain που περιλαμβάνουν προσωπικά δεδομένα.

3.2 Συνδυασμό και/ή συσχέτιση προσωπικών δεδομένων από πολλαπλές πηγές ή τρίτους, από δύο ή περισσότερες πράξεις επεξεργασίας που υλοποιούνται για διαφορετικούς σκοπούς ή/και από διαφορετικούς υπευθύνους επεξεργασίας με τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων.

3.3 Σε περίπτωση που η επεξεργασία αφορά δεδομένα, τα οποία δεν έχουν συλλεγεί από το υποκείμενο και η ενημέρωση των υποκειμένων σύμφωνα με το άρθρο 14 ΓΚΠΔ αποδεικνύεται αδύνατη ή θα προϋπέθετε δυσανάλογη προσπάθεια ή είναι πιθανό να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας.

*Αναθεώρηση του καταλόγου*

Ο ανωτέρω κατάλογος υπόκειται σε τακτική αναθεώρηση κάθε δύο έτη ή σε έκτακτη αναθεώρηση σε περίπτωση σημαντικών εξελίξεων σε τεχνολογικό επίπεδο ή στα επιχειρησιακά μοντέλα, καθώς και σε περίπτωση μεταβολής των σκοπών της επεξεργασίας εφόσον οι νέοι αυτοί σκοποί συνεπάγονται υψηλό κίνδυνο.