Διπλωματική Εργασία με τίτλο:

“Μελέτη Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα”

Πανεπιστήμιο Πειραιά
Τμήμα Ψηφιακών Συστημάτων
Πρόγραμμα Μεταπτυχιακών Σπουδών στην Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων
Κατεύθυνση : Ασφάλεια Ψηφιακών Συστημάτων

Κωνσταντίνος Κουλούρης , Α.Μ ΜΤΕ 1620
Επιβλέπων Καθηγητής Κωνσταντίνος Λαμπρινουδάκης

ΟΚΤΩΒΡΙΟΣ 2018 ΠΕΙΡΑΙΑΣ

Περιεχόμενα

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμότατες ευχαριστίες μου στον επιβλέπων καθηγητή της παρούσας εργασίας κ. Κωνσταντίνο Λαμπρινουδάκη καθηγητή στο τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά. Χωρίς την πολύτιμη βοήθειά του σε επιστημονικά και διαδικαστικά ζητήματα, την συνεχή πρακτική και ηθική υποστήριξή του και την εμπιστοσύνη του, η πραγματοποίηση της παρούσας εργασίας θα ήταν αδύνατη.

Περίληψη

Η παρούσα εργασία έχει ως θέμα τον Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Γ.Κ.Π.Δ - GDPR) ο οποίος τέθηκε σε εφαρμογή στις 25 Μαΐου 2018 έχοντας καθολική ισχύ σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης καταργώντας την οδηγία 95/46/ΕΚ.

Συγκεκριμένα, η εργασία έχει ως κύριο θέμα την παρουσίαση της απαίτησης για διενέργεια μελέτης Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα από πλευράς οργανισμών οι οποίοι συλλέγουν και επεξεργάζονται περαιτέρω προσωπικά δεδομένα Ευρωπαίων Πολιτών.

Η συγκεκριμένη απαίτηση δεν είναι υποχρεωτική για όλους τους οργανισμούς αλλά μόνο για εκείνους οι οποίοι διενεργούν πράξεις επεξεργασίας που ενέχουν υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Η παρούσα εργασία έχει ως στόχο την παροχή όλων των απαραίτητων πληροφοριών σχετικά με τη νέα αυτή απαίτηση που εισάγει ο Κανονισμός. Συκεκριμένα παρουσιάζονται τα κριτήρια με βάση τα οποία θα πρέπει να λαμβάνεται η απόφαση για την διενέργεια ή όχι μιας μελέτης Εκτίμησης Αντικτύπου.Επίσης, αναλύονται τα βασικά στοιχεία που πρέπει να περιέχει μια Εκτίμηση Αντικτύπου όπως και τους βασικούς συμμετέχοντες που θα πρέπει να εμπλακούν στην διενέργεια της.

Τέλος, παρουσιάζεται μια μεθοδολογία για την διενέργειά της με αναλυτικά βήματα, η οποία βασίζεται στην ανάλογη μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Κεφάλαιο 1: Εισαγωγή

Ο Γενικός Κανονισμός για την προστασία των δεδομένων προσωπικού χαρακτήρα ΕΕ 679/2016 («GDPR») αποτελεί, από τις 25 Μαΐου 2018, το κύριο νομικό πλαίσιο σχετικά με την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση καταργώντας την ισχύουσα οδηγία 95/46 / ΕΚ. Ο Κανονισμός θα είναι άμεσα εφαρμόσιμος σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης και έχει ως στόχο την δημιουργία ενός συνεκτικού πλαισίου για την προστασία δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση.

Κύριος στόχος του νέου αυτού νομοθετικού πλαισίου είναι η θέσπιση ομοιόμορφων κανόνων και απαιτήσεων για την προστασία των δεδομένων προσωπικού χαρακτήρα σε όλη την Ευρωπαϊκή Ένωση.

Ο Κανονισμός θεσπίζει κανόνες για την προστασία των φυσικών προσώπων όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων και έχει ως βασική αρχή την προστασία θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων.

Ακόμη, εισάγει ορισμένες νέες αρχές και υποχρεώσεις για τους οργανισμούς οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, όπως η προστασία των δεδομένων εξ ορισμού και εκ σχεδιασμού.

Επιπρόσθετα, ενισχύει τα δικαιώματα των υποκειμένων των δεδομένων με την διατήρηση αυτών που υπήρχαν στην Οδηγία 95/46 / ΕΚ και την εισαγωγή νέων όπως το δικαίωμα διαγραφής (δικαίωμα στη λήθη) και το δικαίωμα της φορητότητας των δεδομένων κ.α.

Ο Κανονισμός βασίζεται ρητά στην έννοια της προσέγγισης βάσει κινδύνου καθώς ορίζει σαφώς ότι τα μέτρα τα οποία καλούνται να υλοποιήσουν οι οργανισμοί που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα προκειμένου να παρέχουν ένα επαρκές επίπεδο ασφάλειας θα πρέπει να λαμβάνουν υπόψη τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Έτσι, ενσωματώνει μια προσέγγιση βασισμένη στον κίνδυνο για την προστασία των δεδομένων προσωπικού χαρακτήρα απαιτώντας από τους οργανισμούς να αξιολογήσουν την πιθανότητα και τη σοβαρότητα του κινδύνου που ενέχουν οι πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα όσον αφορά τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Αυτό το γεγονός θα πρέπει να τονίσουμε ότι δεν σημαίνει ότι η προστασία των δικαιωμάτων των υποκειμένων των δεδομένων όπως αυτά ορίζονται από τον Κανονισμό (π.χ. δικαίωμα ενημέρωσης, πρόσβασης, αντίρρησης ,διαγραφής κτλ.) εξαρτάται από το επίπεδο κινδύνου της εν λόγω επεξεργασίας.

Τα δικαιώματα των φυσικών προσώπων ισχύουν εξ ολοκλήρου ανεξάρτητα από το επίπεδο κινδύνου κατά την επεξεργασία των προσωπικών τους δεδομένων.

Ωστόσο, οι οργανισμοί θα πρέπει να τροποποιήσουν τη συμμόρφωσή τους όσον αφορά την προστασία των δεδομένων σύμφωνα με το επίπεδο κινδύνου που ενέχουν οι πράξεις επεξεργασίας όσον αφορά θεμελιώδη δικαιώματα και τις ελευθερίες των ατόμων.

Πολλοί οργανισμοί έχουν ήδη ακολουθήσει αυτή την προσέγγιση ως μέρος των εσωτερικών προγραμμάτων συμμόρφωσης με το ισχύον νομοθετικό πλαίσιο.

Ο Γενικός Κανονισμός όμως έρχεται να δώσει μια περαιτέρω ώθηση στην υιοθέτηση της εν λόγω προσέγγισης η οποία ορίζει πώς, οι διαδικασίες επεξεργασίας που ενέχουν χαμηλότερους κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων μπορούν γενικά να οδηγήσουν σε λιγότερες υποχρεώσεις συμμόρφωσης, ενώ οι διαδικασίες επεξεργασίας "υψηλού κινδύνου" θα δημιουργήσουν πρόσθετες υποχρεώσεις συμμόρφωσης για τους οργανισμούς οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα πολιτών της Ευρωπαϊκής Ένωσης.

Μια τέτοια νέα για τους οργανισμούς υποχρέωση η οποία εισάγεται με τον Κανονισμό και συγκεκριμένα στο Άρθρο 35, αποτελεί η διενέργεια μελέτης **Εκτίμησης Αντικτύπου** σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Η μελέτη για την διενέργεια της Εκτίμησης Αντικτύπου αποτελεί το θέμα της παρούσας εργασίας η οποία προσπαθεί να δώσει ορισμένες χρήσιμες πληροφορίες σχετικά με τη νέα αυτή υποχρέωση για του υπεύθυνους επεξεργασίας, να δώσει ορισμένες κατευθυντήριες γραμμές για τον τρόπο με τον οποίο θα πρέπει να διεξάγεται μια Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα αλλά και για τις πληροφορίες τις οποία θα πρέπει να περιέχει μια τέτοια μελέτη.

Απευθύνεται κυρίως προς τους υπεύθυνους επεξεργασίας οι οποίοι επιθυμούν να αποδείξουν τη συμμόρφωση τους με τις απαιτήσεις του Κανονισμού αλλά και να αποδείξουν παράλληλα ότι μια διαδικασία επεξεργασίας έχει αναπτυχθεί με απόλυτο σεβασμό στα δεδομένα προσωπικού χαρακτήρα .

Κεφάλαιο 2: Γενικές πληροφορίες σχετικά με την μελέτη Εκτίμησης Αντικτύπου

Όταν ένας οργανισμός συλλέγει, αποθηκεύει ,χρησιμοποιεί και εν γένει επεξεργάζεται δεδομένα προσωπικού χαρακτήρα , τα άτομα των οποίων τα δεδομένα τυγχάνουν επεξεργασίας είναι εκτεθειμένα σε κινδύνους.

Οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, είναι ποικίλης πιθανότητας και σοβαρότητας και είναι δυνατόν να προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη για τα υποκείμενα των δεδομένων, 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, ή οποιοδήποτε άλλη σημαντική οικονομική ή κοινωνική ζημία για τα υποκείμενα των δεδομένων .

Ακόμη, κίνδυνοι ενδέχεται να προκύψουν 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 ή 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.

Επίσης, 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 τις μετακινήσεις, προκειμένου να δημιουργηθούν ή να χρησιμοποιηθούν προσωπικά προφίλ και επιπρόσθετα 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

Από την πλευρά των οργανισμών που αναπτύσσουν και λειτουργούν εφαρμογές πληροφορικής μέσω των οποίων επεξεργάζονται δεδομένα προσωπικού χαρακτήρα πελατών και εργαζομένων ένα σημαντικό πρόβλημα αποτελεί η προστασία αυτών των δεδομένων και η πρόληψη παραβιάσεων της ιδιωτικής ζωής. Η αποτυχία κατάλληλης αντιμετώπισης αυτού του προβλήματος μπορεί να οδηγήσει σε σημαντική ζημία στη φήμη της εταιρείας, σε οικονομικές απώλειες καθώς και αρνητικές επιπτώσεις για τους πελάτες ή τους εργαζόμενους (υποκείμενα των δεδομένων).

Οι κυριότερες δυσκολίες τις οποίες αντιμετωπίζουν οι οργανισμοί κατά την προσπάθεια συμμόρφωσης με τις απαιτήσεις του Κανονισμού είναι οι ακόλουθες:

- η ακριβής γνώση:

- για το ποια δεδομένα συλλέγουν και επεξεργάζονται περαιτέρω σε κάθε στάδιο των επιχειρηματικών τους δραστηριοτήτων,
- για το ποιοι εμπλέκονται στην επεξεργασία και με ποια εργαλεία και διαδικασίες λαμβάνει χώρα η επεξεργασία

- ο καθορισμός και ο διαχωρισμός των επιχειρησιακών αναγκών και των σκοπών της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ώστε να διασφαλίζονται όλες οι απαιτούμενες συγκαταθέσεις του υποκειμένου των δεδομένων και να μη γίνεται επεξεργασία για μη συμβατούς σκοπούς με του αρχικά δηλωθέντες.
- ο συστηματικός έλεγχος για την συμμόρφωση με τις απαιτήσεις του Κανονισμού σε κάθε στάδιο της επεξεργασίας των δεδομένων.
- η αξιολόγηση των κινδύνων που ενδέχεται να οδηγήσουν σε παραβίαση των προσωπικών δεδομένων
- η παρουσίαση των σημαντικότερων κινδύνων και των τρόπων αντιμετώπισής τους με πρακτικό τρόπο, ώστε να αποφασισθεί ένα ρεαλιστικό πλάνο αντιμετώπισης τους και να καθοριστεί ο προϋπολογισμός που απαιτείται για την ανάπτυξη των διαδικασιών συμμόρφωσης
- η λήψη αναλογικών, αποτελεσματικών και οικονομικών μέτρων για τον περιορισμό των κινδύνων, χωρίς να θίγονται οι επιχειρησιακές προτεραιότητες και η λειτουργικότητα των συστημάτων.

Ένα ιδιαιτέρως χρήσιμο εργαλείο τόσο για την αντιμετώπιση των προβλημάτων αυτών, όσο και εν γένει στην προσπάθεια συμμόρφωσης των οργανισμών με το νομοθετικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών της Ευρωπαϊκής Ένωσης αποτελεί η διενέργεια από πλευράς των οργανισμών μιας μελέτης Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.

2.1 Τι είναι μια μελέτη Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα

Όπως τονίσαμε ο Γενικός Κανονισμός για την προστασία των δεδομένων προσωπικού χαρακτήρα ο οποίος είναι από τις 25 Μαΐου 2018 το κύριο νομικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα έχοντας καθολική εφαρμογή σε όλες τις χώρες της ένωσης θεσπίζει ορισμένες νέες υποχρεώσεις για τους οργανισμούς οι οποίοι επεξεργάζονται προσωπικά δεδομένα.

Μία από αυτές τις νέες υποχρεώσεις αποτελεί η διενέργεια μιας μελέτης Εκτίμησης Αντικτύπου από πλευράς του οργανισμού ο οποίος καθορίζει τους σκοπούς και τα μέσα μιας πράξης επεξεργασίας και ο οποίος στα πλαίσια του Κανονισμού ονομάζεται υπεύθυνος επεξεργασίας.

Συγκεκριμένα, το **Άρθρο 35** του Κανονισμού εισάγει την έννοια της Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα αναφέροντας χαρακτηριστικά ότι:

'' 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 σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα''.

Η μελέτη Εκτίμησης Αντικτύπου αποτελεί μια διεργασία σχεδιασμένη προκειμένου να:

- περιγράψει μια διαδικασία επεξεργασίας
- αξιολογήσει την αναγκαιότητα και την αναλογικότητα της
- αναγνωρίσει τους κινδύνους που ενέχει
- βοηθήσει στην διαχείριση των κινδύνων αυτών για τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων

Αυτό το πετυχαίνει αξιολογώντας τους κινδύνους και προτείνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αντιμετώπιση των κινδύνων αυτών.

Η μελέτη Εκτίμησης Αντικτύπου συνιστά μια διαδικασία η οποία βοηθά έναν οργανισμό στον εντοπισμό και τη μείωση των κινδύνων που ενέχει ένα έργο, μια εφαρμογή ή μια μεμονωμένη πράξη επεξεργασίας όσον αφορά την προστασία των προσωπικών δεδομένων των φυσικών προσώπων που επηρεάζονται από αυτήν.

Μια αποτελεσματική μελέτη Εκτίμησης Αντικτύπου θα πρέπει να χρησιμοποιείται καθ' 'όλη τη διάρκεια της ανάπτυξης και της εφαρμογής ενός έργου, επιτρέποντας σε έναν οργανισμό να αναλύει συστηματικά και διεξοδικά πώς ένα συγκεκριμένο έργο ή σύστημα θα επηρεάσει τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Η σημασία της διενέργειας μιας Εκτίμησης Αντικτύπου για τους οργανισμούς είναι διττή καθώς αποτελεί σημαντικό εργαλείο τόσο για τον εντοπισμό και την αντιμετώπιση των κινδύνων που ενέχει η επεξεργασία δεδομένων προσωπικού χαρακτήρα σε πρώιμο στάδιο, όσο και για την απόδειξη συμμόρφωσης του υπεύθυνου επεξεργασίας με τις απαιτήσεις τις οποίες θέτει ο Κανονισμός και εν γένει το νομοθετικό πλαίσιο περί προστασίας των δεδομένων προσωπικού χαρακτήρα.

2.2 Οφέλη από τη διενέργεια της Εκτίμησης Αντικτύπου

Τα κύρια οφέλη για τους υπεύθυνους επεξεργασίας από τη διενέργεια μιας Εκτίμησης Αντικτύπου είναι τα εξής:

- Απόδειξη συμμόρφωσης με τις απαιτήσεις του Κανονισμού και αποφυγή των προβλεπόμενων κυρώσεων.
- Μείωση των κινδύνων που σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.
- Μείωση του κόστους λειτουργίας του οργανισμού βελτιστοποιώντας τις ροές πληροφοριών στο πλαίσιο ενός έργου και εξαλείφοντας την περιττή συλλογή και επεξεργασία δεδομένων.

- Ενίσχυση του κύρους του οργανισμού και εγκαθίδρυση σχέσεων εμπιστοσύνης με τα υποκείμενα των δεδομένων που επηρεάζονται από τις διαδικασίες επεξεργασίας.
- Αύξηση της ευαισθητοποίησης του προσωπικού στο εσωτερικό του οργανισμού σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και την ασφάλεια πληροφοριών εν γένει.
- Ικανοποίηση των απαιτήσεων για "Προστασία των Δεδομένων ήδη από τον Σχεδιασμό" και "Προστασία των Δεδομένων εξ ορισμού" τις οποίες θέτει ο Κανονισμός στο Άρθρο 25 αλλά και των αρχών της διαφάνειας και της λογοδοσίας.

Συνεπώς, μπορούμε να πούμε ότι μια Εκτίμηση Αντικτύπου εκτελεί μια διπλή λειτουργία.

Από την μία πλευρά, μπορεί να λειτουργήσει ως μηχανισμός λογοδοσίας, ιδίως όταν υπάρχουν παραβιάσεις ή απώλειες δεδομένων υπό την έννοια ότι επιτρέπει στους υπεύθυνους επεξεργασίας να επιδεικνύουν την ευαισθητοποίησή τους σχετικά με τους κινδύνους που αφορούν την προστασία της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα και τη δέσμευσή τους να εξασφαλίσουν ένα αποτελεσματικό επίπεδο προστασίας των δεδομένων.

Από την άλλη πλευρά, δύναται να προωθήσει τη διασφάλιση της προστασίας των δικαιωμάτων της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα στην περίπτωση δημιουργίας νέων έργων, συστημάτων και υπηρεσιών που ενέχουν υψηλούς κινδύνους για την προστασία της ιδιωτικής ζωής, διότι απαιτεί από τον υπεύθυνο επεξεργασίας να εξετάζει συστηματικά την προβλεπόμενη πράξη επεξεργασίας δεδομένων, τους σχετικούς κινδύνους και τα μέτρα που πρέπει να ληφθούν για τον μετριασμό αυτών των κινδύνων ήδη από το αρχικό στάδιο της διαδικασίας επεξεργασίας.

Οι υπεύθυνοι οργανισμοί θα πρέπει να υιοθετήσουν την διενέργεια μελέτης Εκτίμησης Αντικτύπου ως μέρος των γενικών πρακτικών διαχείρισης κινδύνων ανεξάρτητα αν αποτελεί νομική υποχρέωση στα πλαίσια του Κανονισμού.

Τέλος, θα πρέπει να τονίσουμε ότι υπό το πρίσμα του Κανονισμού η μη συμμόρφωση με τις απαιτήσεις της Εκτίμησης Αντικτύπου επιφέρει την επιβολή προστίμων για τους υπεύθυνους επεξεργασίας από την Αρμόδια Εποπτική Αρχή.

2.3 Παράγοντες επιτυχίας μιας Εκτίμησης Αντικτύπου

Οι ακόλουθοι παράγοντες μπορούν να συμβάλουν στη διενέργεια μιας επιτυχούς Εκτίμησης Αντικτύπου από πλευράς των οργανισμών.

Μια μελέτη Εκτίμησης Αντικτύπου θα πρέπει:

- να αποτελεί αναπόσπαστο μέρος της διαδικασίας διαχείρισης κινδύνων και να έχει διαρθρωτικό ρόλο σε έργα, προγράμματα ή διαδικασίες του οργανισμού. Δεν θα πρέπει να συνιστά μια ad-hoc ή τυχαία διαδικασία αλλά μια καλά οργανωμένη διαδικασία.
- να εκτελείται σε πρώιμο στάδιο κατά προτίμηση κατά τη διάρκεια σχεδιασμού νέων εφαρμογών ή συστημάτων.

- κατά τη διάρκεια της διενέργειας της Εκτίμησης Αντικτύπου να συμμετέχουν ενεργά εσωτερικοί και εξωτερικοί ενδιαφερόμενοι φορείς. (π.χ. εργαζόμενοι, υποκείμενα των δεδομένων, εξωτερικοί συνεργάτες, ίδιοι εμπειρογνώμονες)
- να εκτελείται κατά προτίμηση από μια διεπιστημονική ομάδα εμπειρογνωμόνων στην οποία να συμμετέχουν τόσο νομικοί όσο και επιστήμονες πληροφορικής. Η ομάδα υλοποίησης της Εκτίμησης Αντικτύπου θα πρέπει να περιλαμβάνει άτομα τα οποία να έχουν γνώσεις σχετικά με το έργο / πρόγραμμα όσο και γνώσεις σχετικές με τη νομοθεσία αλλά και την ασφάλεια πληροφοριών.
- να υπόκειται σε μια τακτική (τυπική ή ανεπίσημη) διαδικασία για τον έλεγχο των αποτελεσμάτων της.
- να μην χρησιμοποιείται ως στατικό έγγραφο αλλά να αναθεωρείται τακτικά και να προσαρμόζεται κατά τη διάρκεια ενός έργου (ειδικά όταν οι κίνδυνοι μεταβάλλονται)
- να διενεργείται με την ενεργή συμμετοχή και την ένθερμη υποστήριξη της διοίκησης του οργανισμού

Κεφάλαιο 3: Οργάνωση της διενέργειας της μελέτης Εκτίμησης Αντικτύπου

Η έννοια της διενέργειας μελέτης Εκτίμησης Αντικτύπου από τον υπεύθυνο επεξεργασίας αποτελεί μια νέα απαίτηση την οποία εισάγει ο Κανονισμός σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Η νέα όμως αυτή απαίτηση δεν είναι υποχρεωτική για όλους τους υπεύθυνους επεξεργασίας σύμφωνα με τον Κανονισμό. Αποτελεί νομική υποχρέωση υπό το πρίσμα του Κανονισμού σύμφωνα με το Άρθρο 35 παράγραφός 1 'όταν : ''η προβλεπόμενη επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων"

Το πρώτο βήμα λοιπόν για τη διεξαγωγή μιας Εκτίμησης Αντικτύπου είναι ο καθορισμός για το κατά πόσον αποτελεί νομική υποχρέωση για έναν οργανισμό ο οποίος υλοποιεί ή σχεδιάζει να υλοποιήσει μια συγκεκριμένη πράξη ή ένα σύνολο πράξεων επεξεργασίας.

3.1 Διαδικασία Αρχικής Αξιολόγησης

Όπως αναφέρθηκε παραπάνω, δεν απαιτούν όλες οι πράξεις επεξεργασίας την διενέργεια Εκτίμησης Αντικτύπου.

Συνεπώς, για το λόγο αυτό κρίνεται απαραίτητο οι οργανισμοί να διεξάγουν μια πρώτη αξιολόγηση πριν από την διενέργεια μιας Εκτίμησης Αντικτύπου για να καθορίσουν εάν είναι υποχρεωτική για αυτούς ή όχι.

Η διαδικασία αυτή αποτελεί μια πιο ήπια εκτίμηση για να διαπιστωθεί κατά πόσον οι διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα ενέχουν υψηλούς κινδύνους για τα υποκείμενα των δεδομένων

Ανεξάρτητα από την τελική απόφαση για την διεξαγωγή ή όχι μιας Εκτίμησης Αντικτύπου ο υπεύθυνος επεξεργασίας θα πρέπει να τηρεί ένα αρχείο με την αρχική αυτή αξιολόγηση των πράξεων επεξεργασίας. Στο αρχείο αυτό ο υπεύθυνος επεξεργασίας θα πρέπει να καταγράφει όλα εκείνα τα στοιχεία τα οποία έλαβε υπόψη του κατά τη λήψη της απόφασης για το αν θα προβεί σε διενέργεια Εκτίμησης Αντικτύπου ή όχι

Αυτή η αρχική αξιολόγηση θα πρέπει να περιλαμβάνει τις ακόλουθες πληροφορίες:

- Μια σύντομη περιγραφή του συστήματος εφόσον πρόκειται για ένα νέο σύστημα ή μια περιγραφή των τυχόν αλλαγών σε ένα ήδη υπάρχον σύστημα
- Πληροφορίες σχετικά με τις πράξεις επεξεργασίας που περιλαμβάνει το συγκεκριμένο σύστημα όπως:
- Μια σύντομη περιγραφή των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας (όπως όνομα, διεύθυνση, ημερομηνία γέννησης, πληροφορίες για την υγεία κ.λπ.)
- Πληροφορίες σχετικές με τις βασικές αρχές της προστασίας δεδομένων προσωπικού χαρακτήρα όπως:

- τους γενικούς σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για το συγκεκριμένο σύστημα
- τη νομική βάση στην οποία στηρίζεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα

- Τις απόψεις των κύριων συμμετεχόντων στην διαδικασία επεξεργασίας σχετικά με τους κινδύνους που ενδέχεται να ενέχει η εν λόγω επεξεργασία για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων
- Μια περιγραφή του τρόπου με τον οποίο αξιολογήθηκαν και αντιμετωπίστηκαν ή πρόκειται να αντιμετωπιστούν πιθανοί κίνδυνοι που ενέχει η πράξη επεξεργασίας.
- Την απόφαση για το αν θα προβεί ο υπεύθυνος επεξεργασίας τελικά σε διενέργεια Εκτίμησης Αντικτύπου.
- Η απόφαση αυτή θα πρέπει να προκύπτει από τεκμηριωμένα στοιχεία τα οποία θα πρέπει να καταγράφονται αναλυτικά .
- Τα στοιχεία του ατόμου ή της ομάδας που είναι υπεύθυνη για την διενέργεια της αρχικής αυτής αξιολόγησης αλλά και όλων των συμμετεχόντων στη διαδικασία αυτή.

3.1.1 Η έννοια του υψηλού κινδύνου

Όπως ορίζει ο Κανονισμός η διενέργεια Εκτίμησης Αντικτύπου απαιτείται όταν η πράξη επεξεργασίας ενέχει υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Ο Κανονισμός όμως δεν ορίζει ρητά την έννοια του υψηλού κινδύνου. Ωστόσο, ορισμένες ενδείξεις σχετικά με την έννοια αυτή μπορούν να βρεθούν σε αρκετές αιτιολογικές σκέψεις και άρθρα του.

Ενδεικτικά, στο άρθρο 35 παράγραφος 3 στοιχείο α) του Κανονισμού φαίνεται να καταγράφονται ορισμένες κατηγορίες υψηλού κινδύνου που απαιτούν την διενέργεια Εκτίμησης Αντικτύπου στο πλαίσιο του Κανονισμού, όπως:

- Η συστηματική και εκτενής αξιολόγηση 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 πρόσωποΗ μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα ,δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας
- Η συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

Επίσης, ορισμένες δραστηριότητες οι οποίες ενδέχεται να ενέχουν υψηλούς κινδύνους είναι οι ακόλουθες:

- Πράξεις επεξεργασίας μεγάλης κλίμακας που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο, για παράδειγμα λόγω της ευαισθησίας τους
- Πράξεις επεξεργασίας κατά τις οποίες χρησιμοποιείται μια νέα τεχνολογία σε ευρεία κλίμακα ,σύμφωνα με τα υφιστάμενα επίπεδα τεχνολογικής γνώσης , μια νέα τεχνολογία σε ευρεία κλίμακα
- Πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα ευάλωτων φυσικών προσώπων, ιδίως παιδιών

3.1.2 Κριτήρια για το εάν απαιτείται η διενέργεια Εκτίμησης Αντικτύπου

Σε μια περαιτέρω προσπάθεια για την κατανόηση των προϋποθέσεων σύμφωνα με τις οποίες είναι απαραίτητη η διενέργεια μιας Εκτίμησης Αντικτύπου στα πλαίσια του Κανονισμού και προκειμένου να παρασχεθεί ένα πιο συμπαγές σύνολο πράξεων επεξεργασίας που απαιτούν τη διενέργεια της λόγω του εγγενούς υψηλού κινδύνου τους κρίνεται απαραίτητη η θέσπιση κριτηρίων σύμφωνα με τα οποία θα καθορίζεται εάν η εκπόνηση μελέτης Εκτίμησης Αντικτύπου αποτελεί νομική υποχρέωση για τους υπεύθυνους επεξεργασίας η ομάδα εργασίας του Άρθρου 29 της Ευρωπαϊκής Ένωσης λαμβάνοντας υπόψη τα στοιχεία του άρθρου 35 παράγραφος 1 και του άρθρου 35 παράγραφος 3 στοιχεία α) έως γ αλλά και τις αιτιολογικές σκέψεις 71, 75 και 91 του Κανονισμού έχει καθορίσει τα ακόλουθα κριτήρια:

Κριτήριο	Επεξήγηση	Παραδείγματα
Επεξεργασία που οδηγεί σε κατάρτιση προφίλ με στόχο την αξιολόγηση ή την βαθμολόγηση	Η επεξεργασία αυτή περιλαμβάνει την «κατάρτιση προφίλ» που αποτελείται από οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση προσωπικών πτυχών σχετικά με ένα φυσικό πρόσωπο. Ιδίως σχετίζεται με την ανάλυση ή την πρόβλεψη πτυχών που αφορούν: τις επιδόσεις στην εργασία, την οικονομική κατάσταση την υγεία, προσωπικές προτιμήσεις ή ενδιαφέροντα την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του υποκειμένου των δεδομένων στον βαθμό που παράγει νομικά αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο.	Μια τράπεζα που θα καταγράφει τους πελάτες της σε μια βάση δεδομένων και θα παρακολουθεί τις πιστώσεις τους Μια εταιρεία βιοτεχνολογίας που θα παρέχει γενετικές εξετάσεις απευθείας στους καταναλωτές προκειμένου να εκτιμήσει και να προβλέψει τους κινδύνους για την υγεία τους ή Ένα εταιρικό προφίλ συμπεριφοράς
Επεξεργασία που οδηγεί σε Αυτοματοποιημένη λήψη αποφάσεων	Επεξεργασία η οποία έχει ως στόχο τη λήψη απόφασης αποκλειστικά βάσει αυτοματοποιημένης διαδικασίας και η οποία παράγει έννομα αποτελέσματα έναντι του υποκειμένου των δεδομένων ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο Για παράδειγμα, η	Αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης από ένα χρηματοπιστωτικό ίδρυμα Πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση.

Κριτήριο	Επεξήγηση	Παραδείγματα
	επεξεργασία μπορεί να οδηγήσει στον αποκλεισμό ή τη διάκριση ατόμων	
Επεξεργασία που οδηγεί σε Συστηματική Παρακολούθηση	Επεξεργασία που πραγματοποιείται για την παρατήρηση, την παρακολούθηση ή τον έλεγχο των υποκειμένων των δεδομένων, μέσω "συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα." Αυτός ο τύπος παρακολούθησης ενέχει υψηλούς κινδύνους διότι τα δεδομένα προσωπικού χαρακτήρα ενδέχεται να συλλέγονται σε περιπτώσεις όπου τα υποκείμενα των δεδομένων δεν είναι σε θέση να γνωρίζουν ποιος συλλέγει τα δεδομένα τους, για ποιόν σκοπό και με ποιόν τρόπο αυτά θα χρησιμοποιηθούν. Επιπλέον, ενδέχεται να είναι αδύνατο για τα υποκείμενα των δεδομένων να αποφεύγουν να υποβάλλονται σε τέτοια επεξεργασία σε συχνά δημόσιους (ή προσβάσιμους στο κοινό)χώρους).	Παρακολούθηση δημόσια προσπελάσιμων χώρων(οδοί, πλατείες, άλση, αιγιαλός, παραλία, λιμάνια, όχθες λιμνών και ποταμών, δημόσια δάση κτλ.) σε μεγάλη κλίμακα, ιδίως όταν χρησιμοποιούνται οπτικοακουστικές συσκευές
Επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα	Περιλαμβάνει την επεξεργασία ειδικών κατηγοριών δεδομένων όπως αυτά ορίζονται στο άρθρο 9 όπως δεδομένα τα οποία αποκαλύπτουν: φυλετική ή εθνοτική καταγωγή πολιτικά φρονήματα θρησκευτικές ή φιλοσοφικές πεποιθήσεις	Γενικό νοσοκομείο ή κλινική που κρατά τα ιατρικά αρχεία των ασθενών Ένας ιδιωτικός ερευνητής ο οποίος κρατά στοιχεία σχετικά με καταδίκες των πελατών του. Δεδομένα που υποβάλλονται σε επεξεργασία από φυσικό πρόσωπο κατά τη διάρκεια καθαρά προσωπικών ή οικιακών

Κριτήριο	Επεξήγηση	Παραδείγματα
	συμμετοχή σε συνδικάτα δεδομένων που αφορούν την υγεία Βιομετρικά δεδομένα δεδομένων που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας Περιλαμβάνονται επίσης στοιχεία τα οποία γενικότερα μπορούν να θεωρηθούν ότι αυξάνουν τον πιθανό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, όπως τα δεδομένα ηλεκτρονικής επικοινωνίας, τα δεδομένα θέσης και κίνησης, τα οικονομικά δεδομένα (που μπορούν να χρησιμοποιηθούν για απάτες πληρωμών).	δραστηριοτήτων (όπως υπηρεσίες cloud computing για προσωπική διαχείριση εγγράφων, υπηρεσίες ηλεκτρονικού ταχυδρομείου, ημερολόγια, ηλεκτρονικές συσκευές ανάγνωσης, εφαρμογές καταγραφής που μπορεί να περιέχουν πολύ προσωπικές πληροφορίες)
Επεξεργασία δεδομένων τα υποκείμενα των οποίων λογίζονται ως ευάλωτα.	Η επεξεργασία τέτοιου είδους δεδομένων ενέχει υψηλούς κινδύνους λόγω της αυξημένης ανισορροπίας στη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας δεδομένων, πράγμα που σημαίνει ότι το άτομο μπορεί να αδυνατεί να συναινέσει ή να αντιταχθεί στην επεξεργασία των προσωπικών του δεδομένων	Οι εργαζόμενοι αντιμετωπίζουν συχνά σοβαρές δυσκολίες για να αντιταχθούν στην επεξεργασία που πραγματοποιεί ο εργοδότης τους. Τα παιδιά κάτω των 15 ετών θεωρείται ότι δεν είναι σε θέση να αντιταχθούν ή να παρέχουν συνειδητή και ρητή συγκατάθεση στην επεξεργασία των δεδομένων τους.

Κριτήριο	Επεξήγηση	Παραδείγματα
		Ευάλωτες κατηγορίες του πληθυσμού που χρήζουν ειδικής προστασίας, όπως για παράδειγμα οι ψυχικά ασθενείς, οι αιτούντες άσυλο ή οι ηλικιωμένοι.
Η επεξεργασία κατά την οποία πραγματοποιείται καινοτόμος χρήση ή η εφαρμογή νέων τεχνολογιών	Η επεξεργασία ενέχει υψηλούς κινδύνους διότι η χρήση μιας τέτοιας τεχνολογίας μπορεί να περιλαμβάνει νέες μορφές συλλογής και χρήσης δεδομένων, ενδεχομένως με υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Πράγματι, οι προσωπικές και κοινωνικές συνέπειες της ανάπτυξης μιας νέας τεχνολογίας μπορεί να είναι άγνωστες. Μια Εκτίμηση Αντικτύπου θα βοηθήσει τον υπεύθυνο επεξεργασίας δεδομένων να κατανοήσει και να αντιμετωπίσει αυτούς τους κινδύνους.	Εφαρμογές "Διαδικτύου των Πραγμάτων ΄΄ (Internet of things) θα μπορούσαν να έχουν σημαντικό αντίκτυπο στην καθημερινή ζωή και την ιδιωτική ζωή των ατόμων Εφαρμογές που χρησιμοποιούν βιομετρικά δεδομένα όπως για παράδειγμα ο συνδυασμός της χρήσης του δακτυλικού αποτυπώματος και της αναγνώρισης προσώπου για βελτιωμένο έλεγχο της φυσικής πρόσβασης.
Επεξεργασία δεδομένων σε μεγάλη κλίμακα	Ισχύει ιδίως για πράξεις επεξεργασίας που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο, για παράδειγμα λόγω της ευαισθησίας τους.	Επεξεργασία μεγάλης κλίμακας: Επεξεργασία δεδομένων ασθενών από ένα νοσοκομείο ή κλινική Επεξεργασία δεδομένων κίνησης των πολιτών μέσω των συστημάτων των Μέσων Μαζικής Μεταφοράς (π.χ. Προσωποποιημένη Κάρτα Μετακινήσεων) Επεξεργασία δεδομένων πελατών στα πλαίσια των επιχειρηματικών δραστηριοτήτων από μία τράπεζα ή μια ασφαλιστική εταιρεία Επεξεργασία δεδομένων για στοχευμένη διαφήμιση

Κριτήριο	Επεξήγηση	Παραδείγματα
	Πρέπει να λαμβάνονται υπόψη, ιδίως, οι ακόλουθοι παράγοντες κατά τον καθορισμό του κατά πόσον η επεξεργασία πραγματοποιείται σε μεγάλη κλίμακα: Ο αριθμός των υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό του σχετικού πληθυσμού · Ο όγκος δεδομένων ή / και το εύρος των διαφόρων στοιχείων δεδομένων που υφίστανται επεξεργασία · Η διάρκεια ή τη μονιμότητα της δραστηριότητας επεξεργασίας δεδομένων · Η γεωγραφική έκταση της δραστηριότητας επεξεργασίας	από μια μηχανή αναζήτησης Επεξεργασία δεδομένων (κίνησης ή γεωγραφικής θέσης) από έναν πάροχο κινητής ή σταθερής τηλεφωνίας και Διαδικτύου Επεξεργασία η οποία δεν λογίζεται ως ευρείας κλίμακας Επεξεργασία ιατρικών δεδομένων από έναν ιδιώτη ιατρό Επεξεργασία δεδομένων που αφορούν καταδίκες από ένα ιδιώτη δικηγόρο.
Επεξεργασία δεδομένων τα οποία προέρχονται από δύο ή περισσότερες πράξεις επεξεργασίας	Επεξεργασία δεδομένων τα οποία προέρχονται από δύο ή περισσότερες εργασίες επεξεργασίας δεδομένων που εκτελούνται για διαφορετικούς σκοπούς ή / και από διαφορετικούς υπεύθυνους επεξεργασίας κατά τρόπο που να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων.	Άντληση δεδομένων από των συνδυασμό δύο ή περισσοτέρων βάσεων δεδομένων του ίδιου υπεύθυνου επεξεργασίας Ή Συνδυασμός βάσεων δεδομένων διαφορετικών υπεύθυνων επεξεργασίας με σκοπό την περαιτέρω ταυτοποίηση ενός υποκειμένου των δεδομένων.
Επεξεργασία η οποία εμποδίζει ένα άτομο να ασκήσει ένα	Αυτό περιλαμβάνει επεξεργασία που εκτελείται σε δημόσια προσβάσιμο χώρο, την οποία οι πολίτες δεν μπορούν να αποφύγουν	Επεξεργασία δεδομένων μέσω κλειστού κυκλώματος παρακολούθησης σε δημόσιο χώρο (π.χ. κάμερες που ελέγχουν

Κριτήριο	Επεξήγηση	Παραδείγματα
δικαίωμα ή να χρησιμοποιήσει μια υπηρεσία ή μια σύμβαση	ή πράξεις επεξεργασίας που στοχεύουν στο να επιτρέπουν, να τροποποιούν ή να αρνούνται την πρόσβαση των υποκειμένων των δεδομένων σε μια υπηρεσία ή την ανάληψη μιας σύμβασης.	την κυκλοφορία, κάμερες στους χώρους των Μέσων Μαζικής Μεταφοράς)

Πίνακας 1 - Κριτήρια ΟΑ29

3.1.1 Λήψη απόφασης για την διενέργεια της Εκτίμησης Αντικτύπου

Στις περισσότερες περιπτώσεις, ένας υπεύθυνος επεξεργασίας δεδομένων μπορεί να θεωρήσει ότι μια επεξεργασία που πληροί δύο από τα παραπάνω κριτήρια θα απαιτούσε τη διεξαγωγή μιας Εκτίμησης Αντικτύπου.

Σε γενικές γραμμές, θεωρείται ότι όσο περισσότερα κριτήρια πληρούνται από την επεξεργασία, τόσο πιο πιθανό είναι να παρουσιαστεί υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και συνεπώς η διενέργεια της Εκτίμησης Αντικτύπου να αποτελεί νομική απαίτηση για τον υπεύθυνο επεξεργασίας.

Ωστόσο, σε ορισμένες περιπτώσεις, ένας υπεύθυνος επεξεργασίας δεδομένων μπορεί να θεωρήσει ότι μια επεξεργασία που πληροί μόνο ένα από αυτά τα κριτήρια ενέχει υψηλούς κινδύνους και συνεπώς να προβεί σε διενέργεια της Εκτίμησης Αντικτύπου.

Αντίστροφα, μια πράξη επεξεργασίας ενδέχεται να πληροί δύο ή περισσότερα από τα παραπάνω κριτήρια αλλά να θεωρείται από τον υπεύθυνο επεξεργασίας ότι δεν είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας θα πρέπει να αιτιολογήσει και να τεκμηριώσει αναλυτικά τους λόγους για τους οποίους δεν πραγματοποίησε την Εκτίμηση Αντικτύπου και να συμπεριλάβει / καταγράψει τις απόψεις του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, αλλά και των υπόλοιπων εμπλεκομένων στην διαδικασία επεξεργασίας.

Στο σημείο αυτό, είναι απαραίτητο να τονίσουμε ότι σε περιπτώσεις κατά τις οποίες δεν είναι ξεκάθαρο εάν η επεξεργασία ενδέχεται να επιφέρει υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και συνεπώς δεν είναι ξεκάθαρο εάν θα πρέπει ή όχι να πραγματοποιηθεί η Εκτίμηση Αντικτύπου συνιστάται η πραγματοποίηση της καθώς αποτελεί εν γένει χρήσιμο εργαλείο συμμόρφωσης με την ισχύουσα νομοθεσία περί προστασίας των δεδομένων προσωπικού χαρακτήρα.

Για παράδειγμα, στο πλαίσιο της αρχής της λογοδοσίας, κάθε υπεύθυνος επεξεργασίας δεδομένων θα πρέπει όπως ορίζει ο Κανονισμός στο Άρθρο 30 να "*τηρεί αρχείο των δραστηριοτήτων επεξεργασίας υπό την ευθύνη του*", το οποίο θα περιέχει μεταξύ άλλων, τους σκοπούς της επεξεργασίας, την περιγραφή των κατηγοριών δεδομένων που τυγχάνουν επεξεργασίας, τους αποδέκτες των δεδομένων και "*όπου είναι δυνατόν, μια γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που αναφέρονται στο άρθρο 32 παράγραφος 1*" και πρέπει να εκτιμήσει κατά πόσο είναι πιθανό να υπάρχει υψηλός κίνδυνος, ακόμη και αν τελικά αποφασίσει να μην πραγματοποιήσει Εκτίμηση Αντικτύπου.

Παράδειγμα Επεξεργασίας	Κριτήρια που ικανοποιούνται	Υπάρχει απαίτηση για την διεξαγωγή Εκτίμησης Αντικτύπου?
Ένα νοσοκομείο που επεξεργάζεται γενετικά δεδομένα και δεδομένα υγείας των ασθενών του	Επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα Επεξεργασία δεδομένων τα υποκείμενα των οποίων λογίζονται ως ευάλωτα	Ναι
Μια εταιρεία που παρακολουθεί τις δραστηριότητες των εργαζομένων της, συμπεριλαμβανομένης της παρακολούθησης του σταθμού εργασίας των εργαζομένων, της δραστηριότητας στο Διαδίκτυο κλπ.	Επεξεργασία δεδομένων τα υποκείμενα των οποίων λογίζονται ως ευάλωτα Επεξεργασία που οδηγεί σε Συστηματική Παρακολούθηση	Ναι
Η επεξεργασία δεδομένων προσωπικού χαρακτήρα ασθενών ή πελατών από μεμονωμένο ιατρό, άλλο ιατρικό προσωπικό ή δικηγόρο" (αιτιολογική σκέψη 91).	Επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα Επεξεργασία δεδομένων τα υποκείμενα των οποίων λογίζονται ως ευάλωτα	Όχι
Μια ιστοσελίδα ηλεκτρονικού εμπορίου που προβάλλει διαφημίσεις για συγκεκριμένα προϊόντα με βάση τη συμπεριφορά των προηγούμενων αγορών σε ορισμένα τμήματα της ιστοσελίδας της.	Επεξεργασία που οδηγεί σε κατάρτιση προφίλ με στόχο την αξιολόγηση ή την βαθμολόγηση	Όχι
Ένα ηλεκτρονικό περιοδικό που χρησιμοποιεί μια λίστα αλληλογραφίας για να στείλει ένα γενικό ημερήσιο digest στους συνδρομητές του	Κανένα	Όχι

Πίνακας 2 - Παραδείγματα Επεξεργασίας

3.2 Στάδιο διενέργειας της διενέργειας της Εκτίμησης Αντικτύπου

Η Εκτίμηση Αντικτύπου όπως ορίζει ο Κανονισμός θα πρέπει να διεξάγεται "*πριν από τη επεξεργασία δεδομένων προσωπικού χαρακτήρα*" (άρθρα 35 παράγραφος 1 και 35 παράγραφος 10, αιτιολογικές σκέψεις 90 και 93).

Η απαίτηση αυτή συμβαδίζει με τις απαιτήσεις για την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού οι οποίες αποτελούν επίσης θεμελιώδεις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων.

Η προσέγγιση αυτή εξασφαλίζει ότι θα ληφθούν τα ανάλογα και κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να επιτυγχάνεται η συμμόρφωση με τον Κανονισμό ενώ παράλληλα δεν θα παρεμποδίζεται η επίτευξη των λειτουργικών στόχων του συστήματος.

Αντίθετα, η διενέργεια μιας Εκτίμησης Αντικτύπου μετά τη δημιουργία ενός συστήματος, έργου ή εφαρμογής και την εφαρμογή των μέτρων ασφαλείας ενδέχεται να θέσει υπό αμφισβήτηση τις επιλογές που έχουν γίνει γεγονός που ενδέχεται να επηρεάσει σημαντικά το κόστος για την πραγματοποίηση των απαραίτητων αλλαγών στο σύστημα

Συχνά μια Εκτίμηση Αντικτύπου είναι χρήσιμο να διενεργείται παραπάνω από μία φορά στον κύκλο ζωής του έργου. Επίσης, είναι απαραίτητο ναι είναι δυναμική και ενημερωμένη σύμφωνα με τις αλλαγές οι οποίες πραγματοποιούνται στα έργα.

Για το λόγο αυτό θα πρέπει να επανεξετάζεται σε διάφορες χρονικές στιγμές σε όλο το διάστημα του σχεδιασμού και της υλοποίησης ενός έργου.

3.3 Υπεύθυνος για την διενέργεια της Εκτίμησης Αντικτύπου

Την γενική ευθύνη για τον σχεδιασμό και την υλοποίηση μιας Εκτίμησης Αντικτύπου φέρει ο υπεύθυνος επεξεργασίας.

Η διενέργεια της διαδικασίας δύναται να πραγματοποιηθεί με την αρωγή και σε συνεργασία με τον υπεύθυνο προστασίας δεδομένων του οργανισμού, σε περίπτωση κατά την οποία έχει οριστεί, και τον εκτελούντα την επεξεργασία.

Επίσης, θα πρέπει να ληφθεί υπόψη η γνώμη οντοτήτων οι οποίες επηρεάζονται άμεσα από την διαδικασία επεξεργασίας όπως τα υποκείμενα των δεδομένων αλλά και υπάλληλοι στο εσωτερικό του οργανισμού οι οποίοι εμπλέκονται στην επεξεργασία στα πλαίσια του σταδίου της διαβούλευσης το οποίο θα παρουσιάσουμε αναλυτικά στο επόμενο κεφάλαιο.

Ακόμη, θα πρέπει να τονίσουμε ότι η διενέργεια της Εκτίμησης Αντικτύπου μπορεί να πραγματοποιηθεί από κάποια Τρίτη οντότητα για λογαριασμό του υπεύθυνου επεξεργασίας , αλλά ο υπεύθυνος επεξεργασίας παραμένει τελικά υπεύθυνος για την πραγματοποίηση της.

3.4 Οντότητες οι οποίες δύναται να συμμετέχουν στην διαδικασία διενέργειας Εκτίμησης Αντικτύπου

Όπως τονίσαμε παραπάνω η ευθύνη για την διενέργεια της μελέτης Εκτίμησης Αντικτύπου βαραίνει τον υπεύθυνο επεξεργασίας ο οποίος καθορίζει τους σκοπούς και τα μέσα της εν λόγω πράξης επεξεργασίας.

Στην διενέργεια όμως της μελέτης ενδέχεται να έχουν σημαντικό ρόλο και άλλες οντότητες από το εσωτερικό ή το εξωτερικό του οργανισμού.

Ενδεικτικά οι εμπλεκόμενοι στην διενέργεια μιας μελέτης Εκτίμησης Αντικτύπου αποτυπώνονται στον ακόλουθο πίνακα:

Ρόλος	Υπεύθυνος Διεξαγωγής	Παρέχει Συμβουλές	Ενημερώνεται
Υπεύθυνος Επεξεργασίας	X		
Υπεύθυνος Προστασίας Δεδομένων		X	
Εκτελών την Επεξεργασία		X	
Υποκείμενα των Δεδομένων		X	X

Πίνακας 3 - Εμπλεκόμενοι στην Ε.Α

3.4.1 Ο Υπεύθυνος Προστασίας Δεδομένων.

Όπως ρητά ορίζει ο Κανονισμός ο υπεύθυνος επεξεργασίας πρέπει ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων.

Οι συμβουλές που θα δοθούν καθώς και οι αποφάσεις που λαμβάνει ο Υπεύθυνος Επεξεργασίας σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων πρέπει να καταγράφονται στην μελέτη Εκτίμησης Αντικτύπου.

Ο Υπεύθυνος Προστασίας Δεδομένων οφείλει να παρακολουθεί την διαδικασία της διενέργειας Εκτίμησης Αντικτύπου καθ΄ όλη τη διάρκεια ανάπτυξη της.

3.4.2 Ο εκτελών την επεξεργασία

Σε περίπτωση κατά την οποία η επεξεργασία διεξάγεται εν όλω ή εν μέρει από έναν εκτελούντα την επεξεργασία , ο εκτελών οφείλει να συνδράμει τον υπεύθυνο επεξεργασίας κατά την εκτέλεση της Εκτίμησης Αντικτύπου και να παράσχει όλες τις απαραίτητες πληροφορίες που είναι απαραίτητες και θα του ζητηθούν από τον υπεύθυνο επεξεργασίας.

3.4.3 Τα υποκείμενα των δεδομένων

Όπως ορίζει επίσης ο Κανονισμός ο υπεύθυνος επεξεργασίας θα πρέπει επίσης να "*αναζητήσει τις απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους όπου*

ενδείκνυται". Οι απόψεις αυτές θα μπορούσαν να αναζητηθούν με ποικίλα μέσα, ανάλογα με το πλαίσιο της πράξης επεξεργασίας.

Θα πρέπει να τονίσουμε επίσης, ότι σε περίπτωση κατά την οποία η τελική απόφαση του υπεύθυνου επεξεργασίας δεδομένων δε λάβει υπόψη τις απόψεις των υποκειμένων των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να τεκμηριώσει και να καταγράψει στην Εκτίμηση Αντικτύπου τους λόγους που τον οδήγησαν να λάβει την απόφαση αυτή.

Ο υπεύθυνος της επεξεργασίας οφείλει επίσης να τεκμηριώσει την απόφαση του να μην αναζητήσει τις απόψεις των υποκειμένων των δεδομένων, αν κρίνει ότι αυτό δεν είναι κατάλληλο, παραδείγματος χάριν εάν κάτι τέτοιο θα έθετε σε κίνδυνο την εμπιστευτικότητα των επιχειρηματικών σχεδίων των επιχειρήσεων ή θα ήταν δυσανάλογο ή ανέφικτο

3.5 Πεδίο εφαρμογής μιας Εκτίμησης Αντικτύπου

Η Εκτίμηση Αντικτύπου ενδέχεται να αφορά μια ενιαία πράξη επεξεργασίας ή ένα σύνολο παρόμοιων πράξεων επεξεργασίας.

Η Εκτίμηση Αντικτύπου σε ένα γενικό πλαίσιο αφορά μια ενιαία διαδικασία επεξεργασίας δεδομένων. Εντούτοις, όπως ορίζει ο Κανονισμός στο άρθρο 35 παράγραφος 1 "*μια ενιαία αξιολόγηση μπορεί να αφορά ένα σύνολο παρόμοιων πράξεων επεξεργασίας που παρουσιάζουν παρόμοιους υψηλούς κινδύνους".*

Υπάρχουν περιπτώσεις κατά τις οποίες ενδέχεται να είναι λογικό και οικονομικό το αντικείμενο μιας Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα να υπερβαίνει ένα μεμονωμένο σχέδιο. Αυτό μπορεί να σημαίνει ότι χρησιμοποιείται παρόμοια τεχνολογία για τη συλλογή των ίδιων δεδομένων για τους ίδιους σκοπούς όπως.

- εάν δημόσιες αρχές ή φορείς σκοπεύουν να εγκαθιδρύσουν μια κοινή εφαρμογή ή πλατφόρμα επεξεργασίας ή
- εάν περισσότεροι υπεύθυνοι επεξεργασίας σχεδιάζουν να θεσπίσουν μια κοινή εφαρμογή ή ένα περιβάλλον επεξεργασίας σε ένα βιομηχανικό τομέα ή κλάδο ή για μια ευρέως χρησιμοποιούμενη οριζόντια δραστηριότητα.

Για παράδειγμα, μια ομάδα δημοτικών αρχών, οι οποίες συγκροτούν ένα παρόμοιο σύστημα κλειστού κυκλώματος τηλεόρασης (CCTV) , θα μπορούσαν να εκτελούν μια ενιαία μελέτη Εκτίμησης Αντικτύπου η οποία να καλύπτει την επεξεργασία από αυτούς τους ξεχωριστούς υπεύθυνους επεξεργασίας ή ένας σιδηροδρομικός φορέας (ένας μόνος υπεύθυνος επεξεργασίας) θα μπορούσε να καλύψει την παρακολούθηση βίντεο σε όλους τους σιδηροδρομικούς σταθμούς με μία μελέτη Εκτίμησης Αντικτύπου.

Αυτό πρακτικά σημαίνει ότι μια Εκτίμηση Αντικτύπου σχετικά με την προστασία των δεδομένων δύναται να χρησιμοποιηθεί για την αξιολόγηση πολλαπλών πράξεων επεξεργασίας οι οποίες είναι παρόμοιες υπό την έννοια των κινδύνων, τη φύση, το πλαίσιο και το περιεχόμενο.

Όταν οι πράξεις επεξεργασίας αφορούν από κοινού υπεύθυνους επεξεργασίας, τότε θα πρέπει να καθοριστούν με ακρίβεια οι αντίστοιχες υποχρεώσεις τους. Η Εκτίμηση Αντικτύπου θα πρέπει να ορίζει ποιος είναι υπεύθυνος για την υλοποίηση των τεχνικών και οργανωτικών μέτρων που αποσκοπούν στην αντιμετώπιση των κινδύνων και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων.

Μια μελέτη Εκτίμησης Αντικτύπου μπορεί επίσης να είναι χρήσιμη για την αξιολόγηση των επιπτώσεων στην προστασία δεδομένων ενός προϊόντος τεχνολογίας, για παράδειγμα ενός υλικού ή λογισμικού, όπου αυτό είναι πιθανό να χρησιμοποιηθεί από διαφορετικούς υπεύθυνους επεξεργασίας δεδομένων για τη διεξαγωγή διαφορετικών διαδικασιών επεξεργασίας.

Φυσικά, ο υπεύθυνος επεξεργασίας δεδομένων που χρησιμοποιεί το προϊόν παραμένει υποχρεωμένος να εκτελεί τη δική του Εκτίμηση Αντικτύπου σε σχέση με την συγκεκριμένη εφαρμογή, αλλά αυτό μπορεί να ενημερωθεί από μια μελέτη που εκπονήθηκε από τον προμηθευτή του προϊόντος, εάν χρειάζεται. Ένα παράδειγμα θα μπορούσε να είναι η σχέση μεταξύ κατασκευαστών έξυπνων μετρητών και εταιρειών κοινής ωφέλειας.

3.6 Διαδικασία Διαβούλευσης

Η διαδικασία της διαβούλευσης αποτελεί ένα σημαντικό κομμάτι στην διαδικασία διενέργειας μιας Εκτίμησης Αντικτύπου καθώς παρέχει τη δυνατότητα στους εμπλεκόμενους στην επεξεργασία δεδομένων προσωπικού χαρακτήρα να επισημάνουν κινδύνους αλλά και λύσεις υπό το δικό τους πρίσμα και οπτική ανάλογα με τον τομέα ενδιαφέροντος ή εμπειρογνωμοσύνης του καθενός.

Μπορεί να λάβει χώρα σε οποιαδήποτε σημείο της διεργασίας μελέτης Εκτίμησης Αντικτύπου και διακρίνεται σε τρία επιμέρους μέρη:

- Την εσωτερική διαβούλευση
- Την εξωτερική διαβούλευση
- Την διαβούλευση με την Αρμόδια Εποπτική Αρχή

Η διαδικασία της διαβούλευσης δεν θα πρέπει να θεωρηθεί ως ξεχωριστό βήμα κατά την διενέργεια μια Εκτίμησης Αντικτύπου. Είναι ιδιαιτέρως σημαντικό να ενσωματωθεί σε όλα τα στάδια της διαδικασίας. Το γεγονός αυτό παρέχει την δυνατότητα στους υπεύθυνους για την διενέργεια της να αναζητούν και να αποκτούν τη συμβουλή και την γνώμη των κατάλληλων ανθρώπων την κατάλληλη στιγμή.

3.6.1 Εσωτερική Διαβούλευση

Η αποτελεσματική διαβούλευση με άτομα στο εσωτερικό του οργανισμού θα πρέπει να αποτελεί αναπόσπαστο κομμάτι κάθε Εκτίμησης Αντικτύπου. Κατά την διαδικασία της εσωτερικής διαβούλευσης ο υπεύθυνος επεξεργασίας θα πρέπει να αναζητήσει τις απόψεις και τις συμβουλές των εμπλεκόμενων στην διαδικασία επεξεργασίας στο εσωτερικό του οργανισμού προκειμένου να διασφαλιστεί ότι θα ληφθούν υπόψη όλες οι οπτικές.

Οι κίνδυνοι που ενέχει μια διαδικασία επεξεργασίας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων είναι πιθανότερο είτε να μην αναγνωρισθούν είτε να μην αντιμετωπιστούν αποτελεσματικά σε περιπτώσεις κατά τις οποίες η διαδικασία διενέργειας της Εκτίμησης Αντικτύπου δεν περιλαμβάνει συζητήσεις με τους εμπλεκόμενους στην δημιουργία ενός συστήματος ,προϊόντος ή υπηρεσίας.

Η διαδικασία της εσωτερικής διαβούλευσης μπορεί να περιλαμβάνει είτε άτυπες συζητήσεις (πχ μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου στο εσωτερικό του οργανισμού) είτε πιο επίσημες συνεδριάσεις και έγκριση από το διοικητικό συμβούλιο.

Θα πρέπει να τονίσουμε ότι όπως είναι λογικό οι περισσότεροι εσωτερικοί φορείς οι οποίοι συμμετέχουν στην διαδικασία επεξεργασίας έχουν άποψη σχετικά με τις λειτουργικές απαιτήσεις, ο στόχος όμως της εσωτερικής διαβούλευσης στα πλαίσια της Εκτίμησης Αντικτύπου είναι να επικεντρωθεί η προσοχή και το ενδιαφέρον στα θέματα που άπτονται της προστασίας των δεδομένων προσωπικού χαρακτήρα.

3.6.1.1.Συμμετέχοντες στην διαδικασία της εσωτερικής διαβούλευσης

Ο εντοπισμός του πλήρους φάσματος εσωτερικών οντοτήτων των οποίων η γνώμη θα πρέπει να αναζητηθεί θα είναι ευκολότερος εάν έχει πραγματοποιηθεί ο καθορισμός του πλαισίου της διαδικασίας επεξεργασίας κατά το πρώτο στάδιο της Εκτίμησης Αντικτύπου.

Ενδέχεται επίσης, να χρειαστεί να πραγματοποιηθεί κάποια αρχική εσωτερική διαβούλευση προκειμένου να καθοριστεί το πλαίσιο αυτό.

Σε ένα γενικό πλαίσιο οι συμμετέχοντες στην διαδικασία της εσωτερικής διαβούλευσης είναι οι κάτωθι:

- **Ομάδα διαχείρισης έργου:** Η ομάδα που είναι υπεύθυνη για τη γενική υλοποίηση ενός έργου θα διαδραματίσει κεντρικό ρόλο στη διενέργεια της Εκτίμησης Αντικτύπου καθώς είναι σε θέσει να αναλύσει με ενδελεχή τρόπο τις απαιτήσεις και τον τρόπο λειτουργίας του έργου.
- **Υπεύθυνος Προστασίας Δεδομένων:** Όπως ορίζει ο Κανονισμός στο Άρθρο 35 παράγραφο 2 εάν ένας οργανισμός διαθέτει έναν υπεύθυνο προστασίας δεδομένων αυτός θα πρέπει να έχει στενή σχέση με την μελέτη Εκτίμησης Αντικτύπου καθώς θα πρέπει να παρέχει τις συμβουλές του σε όλα τα στάδια ανάπτυξης της μελέτης. Ο Υπεύθυνος Προστασίας Δεδομένων εφόσον έχει οριστεί θα πρέπει να είναι σε θέση να παρέχει εξειδικευμένες γνώσεις σχετικά με θέματα ιδιωτικότητας και προστασίας δεδομένων προσωπικού χαρακτήρα σε όλη την διάρκεια της ανάπτυξης μιας Εκτίμησης Αντικτύπου.
- **Τμήμα Πληροφορικής:** Μηχανικοί υπολογιστών, προγραμματιστές και αναλυτές συστημάτων οι οποίοι σχεδιάζουν και υλοποιούν ένα προϊόν, ένα σύστημα ή μια παρεχόμενη υπηρεσία πρέπει να έχουν μια σαφή κατανόηση για τα θέματα της προστασίας δεδομένων προσωπικού χαρακτήρα. Θα πρέπει να είναι σε θέση να συμβουλεύουν σχετικά με τους κινδύνους και τις λύσεις ασφάλειας. Ο ρόλος του τμήματος της πληροφορικής δεν περιορίζεται στην ασφάλεια, αλλά μπορεί επίσης

να περιλαμβάνει συζητήσεις σχετικά με τη χρησιμότητα και την λειτουργικότητα οποιουδήποτε λογισμικού.

- **Τμήμα Επικοινωνίας και Δημοσίων Σχέσεων:** Η συμμετοχή συνεργατών από το τμήμα επικοινωνίας και δημοσίων σχέσεων είναι σημαντική καθώς μια μελέτη Εκτίμησης Αντικτύπου μπορεί να γίνει χρήσιμο κομμάτι της επικοινωνιακής στρατηγικής ενός οργανισμού.
- **Νομικό Τμήμα:** Η Εκτίμηση Αντικτύπου αποτελεί μια νομική απαίτηση που εισάγει ο Κανονισμός και θα πρέπει να ικανοποιούν οι οργανισμοί. Συνεπώς, η ενεργή συμμετοχή και η αναζήτηση των απόψεων των συνεργατών από νομικό τμήμα στο εσωτερικό του οργανισμού θα πρέπει να αποτελεί αναπόσπαστο κομμάτι της διαδικασίας διενέργειας μιας Εκτίμησης Αντικτύπου προκειμένου να διασφαλίζεται η εναρμόνιση με τις απαιτήσεις αυτές
- **Ανώτερα Διοικητικά Στελέχη:** Ένας βασικός παράγοντας επιτυχίας για την Εκτίμηση Αντικτύπου είναι η υποστήριξη της ανώτερης διοίκησης. Αν τα ανώτερα διοικητικά στελέχη δεν παρέχουν την απαραίτητη υποστήριξη, ο φόρτος εργασίας και ο χρόνος θα μπορούσαν να αυξηθούν και τα αποτελέσματα της Εκτίμησης Αντικτύπου να τεθούν υπό αμφισβήτηση.
  Ο τελευταίος λόγος για την έγκριση και την επικύρωση της Εκτίμησης Αντικτύπου ανήκει στην Διοίκηση για το λόγο αυτό κρίνεται απαραίτητη η συμμετοχή ορισμένων στελεχών στην διαδικασία ανάπτυξης της Εκτίμησης Αντικτύπου.

3.6.2 Εξωτερική Διαβούλευση

Η διαδικασία της εξωτερικής διαβούλευσης αποτελεί απαίτηση που εισάγει ο Κανονισμός στα πλαίσια της διενέργειας μιας μελέτης Εκτίμησης Αντικτύπου.

Συγκεκριμένα όπως αναφέρεται στο Άρθρο 35 παράγραφος 9 του Κανονισμού: "*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*."

Η εξωτερική διαβούλευση σημαίνει την αναζήτηση των απόψεων των ατόμων τα οποία θα επηρεαστούν από το έργο αλλά και από άλλες εξωτερικές οντότητες με ευρύτερη εμπειρία στο χώρο της προστασίας δεδομένων προσωπικού χαρακτήρα που δεν ανήκουν στο δυναμικό του οργανισμού.

Αφορά κυρίως τα υποκείμενα των δεδομένων αλλά μπορεί επίσης να αναφέρεται σε άτομα μέσα σε έναν οργανισμό (για παράδειγμα το προσωπικό στο τμήμα ανθρώπινου δυναμικού το οποίο θα επηρεαστεί από ένα νέο ηλεκτρονικό σύστημα)

Η εξωτερική διαβούλευση αποτελεί ένα σημαντικό μέρος της Εκτίμησης Αντικτύπου. καθώς η σημασία της στην διενέργεια της Εκτίμησης Αντικτύπου είναι διττή:

- Πρώτον, παρέχεται η δυνατότητα στον υπεύθυνο επεξεργασίας να κατανοήσει τις ανησυχίες των ατόμων των οποίων τα δεδομένα προσωπικού χαρακτήρα τυγχάνουν επεξεργασίας.

- Δεύτερον, η διαβούλευση θα βελτιώσει τη διαφάνεια όσον αφορά την διαδικασία επεξεργασίας καθιστώντας τα υποκείμενα των δεδομένων αλλά και εν γένει τους πολίτες ενήμερους για τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα προσωπικού χαρακτήρα τα οποία υφίστανται επεξεργασία στο πλαίσιο των δραστηριοτήτων του οργανισμού.

Η διαβούλευση θα πρέπει να σχεδιάζεται και να πραγματοποιείται έτσι ώστε η γνώμη των ατόμων να μπορεί να ληφθεί υπόψη κατά την ανάπτυξη και την υλοποίηση της πράξης επεξεργασίας. Ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σαφής σχετικά με τις πτυχές της διαδικασίας επεξεργασίας που είναι ανοικτές σε τροποποιήσεις αλλά και για εκείνες που είναι λιγότερο καθώς ένας οργανισμός ενδέχεται να μην επιθυμεί να αποκαλύψει όλα τα σχέδιά του στον έξω κόσμο. Το γεγονός αυτό θα μπορούσε να οφείλεται είτε σε λόγους ασφάλειας είτε σε λόγους εμπορικής ευαισθησίας και προστασίας των εμπορικών συμφερόντων του οργανισμού.

Η δημόσια διαβούλευση ωστόσο μπορεί να είναι ένας αποτελεσματικός τρόπος επικοινωνίας με τα φυσικά πρόσωπα για το πώς οι οργανισμοί χρησιμοποιούν τα προσωπικά τους δεδομένα.

Η εξωτερική διαβούλευση παρέχει επίσης την ευκαιρία στους υπεύθυνους επεξεργασίας να επωφεληθούν από ευρύτερες απόψεις και από την εμπειρία που ενδεχομένως να μην υπάρχουν εντός του ίδιου του οργανισμού με την αναζήτηση των απόψεων αλλά και των ειδικών γνώσεων εμπειρογνωμόνων και επιστημόνων στον τομέα της προστασίας των δεδομένων προσωπικού χαρακτήρα.

Μια αποτελεσματική εξωτερική διαβούλευση θα πρέπει να είναι:

- **Έγκαιρη**: Θα πρέπει να διεξάγεται στο σωστό στάδιο έτσι ώστε να υπάρχει αρκετός χρόνος για απαντήσεις και διορθώσεις.
- **Σαφής και αναλογική** : Θα πρέπει να είναι εστιασμένη στο συγκεκριμένο πλαίσιο επεξεργασίας.
- **Αντιπροσωπευτική** : Θα πρέπει να εξασφαλιστεί ότι έχει αναζητηθεί η γνώμη του συνόλου των υποκειμένων των δεδομένων και εν γένει των ατόμων που επηρεάζονται από την συγκεκριμένη επεξεργασία.

3.6.3 Διαβούλευση με την Αρμόδια Εποπτική Αρχή

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα η οποία αποτελεί την Αρμόδια Εποπτική Αρχή για θέματα που άπτονται της προστασίας των προσωπικών δεδομένων στη χώρα μας διαδραματίζει έναν σημαντικό ρόλο στη διαδικασία διενέργειας αλλά και αναθεώρησης μιας μελέτης Εκτίμησης Αντικτύπου.

Όπως εξηγείται παραπάνω μια μελέτη Εκτίμησης Αντικτύπου απαιτείται όταν μια διαδικασία επεξεργασίας "*είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*". Για παράδειγμα, η επεξεργασία δεδομένων υγείας σε

μεγάλη κλίμακα θεωρείται ότι ενδέχεται να οδηγήσει σε υψηλό κίνδυνο και συνεπώς απαιτεί τη διενέργεια Εκτίμησης Αντικτύπου.

Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για την εκτίμηση των κινδύνων που ενέχει η συγκεκριμένη πράξη επεξεργασίας και για τον προσδιορισμό των προβλεπόμενων τεχνικών και οργανωτικών μέτρων για την αντιμετώπιση των εν λόγω κινδύνων.

Όπως έχουμε αναφέρει ξανά στα πλαίσια της παρούσας εργασίας στόχος της Εκτίμησης Αντικτύπου αλλά και γενικά κάθε διαδικασίας αξιολόγησης και διαχείρισης κινδύνων δεν είναι η πλήρης εξάλειψη των κινδύνων. Αντικειμενικός στόχος είναι ο προσδιορισμός των κινδύνων και ο μετριασμός τους σε αποδεκτά επίπεδα.

Σε περίπτωση κατά την οποία θεωρείται ότι οι κίνδυνοι μειώθηκαν επαρκώς από τον υπεύθυνο επεξεργασίας δεδομένων , η επεξεργασία μπορεί να πραγματοποιηθεί χωρίς διαβούλευση με την εποπτική αρχή.

Αντίθετα, σε περιπτώσεις όπου οι εντοπισμένοι κίνδυνοι δεν μπορούν να αντιμετωπιστούν επαρκώς από τον υπεύθυνο επεξεργασίας δεδομένων (δηλαδή οι υπολειπόμενοι κίνδυνοι παραμένουν υψηλοί), ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να συμβουλευτεί την Αρμόδια Εποπτική Αρχή.

Ένα παράδειγμα υψηλού υπολειπόμενου κινδύνου περιλαμβάνει περιπτώσεις όπου τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίζουν σημαντικές ή ακόμη και μη αναστρέψιμες συνέπειες, τις οποίες δεν μπορούν να υπερνικήσουν (π.χ.: παράνομη πρόσβαση σε δεδομένα που οδηγούν σε απειλή για τη ζωή των υποκειμένων των δεδομένων).

Συνεπώς, σε περίπτωση κατά την οποία η επεξεργασία θα προκαλούσε υψηλό κίνδυνο για τα υποκείμενα των δεδομένων ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας όπως ορίζει ο Κανονισμός στο Άρθρο 35 παράγραφο 1 ο υπεύθυνος επεξεργασίας θα πρέπει να ζητεί την γνώμη της Αρμόδιας Εποπτικής Αρχής πριν από την επεξεργασία.

Κατά την ανάλυση και τον έλεγχο μιας Εκτίμησης Αντικτύπου, η Αρμόδια Εποπτικής Αρχή πρέπει να είναι σε θέση να επαληθεύσει όλους τους εντοπισθέντες κινδύνους και να αξιολογήσει εάν τα αντίστοιχα τεχνικά και οργανωτικά μέτρα είναι κατάλληλα και επαρκή για τον μετριασμό ή ελαχιστοποίηση των προσδιορισμένων κινδύνων.

Για το λόγο αυτό τα αποτελέσματα της Εκτίμησης Αντικτύπου θα πρέπει να παρουσιάζονται και να καταγράφονται με τέτοιο τρόπο έτσι ώστε η Αρμόδια Εποπτικής Αρχή να είναι σε θέση να ελέγχει και να αποφαίνεται κατά πόσο οι διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα από πλευράς του οργανισμού αναπτύσσονται με σεβασμό προς τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων και εναρμονίζονται με τις απαιτήσεις του Κανονισμού.

Κύρια αρμοδιότητα της Εποπτικής Αρχής είναι να παρέχει γραπτώς συμβουλές στον υπεύθυνο επεξεργασίας και, όπου απαιτείται, στον εκτελούντα την επεξεργασία εντός προθεσμίας μέχρι οκτώ εβδομάδων από την παραλαβή του αιτήματος διαβούλευσης προκειμένου να ακολουθήσει συγκεκριμένες ενέργειες για τον περιορισμό των κινδύνων σε αποδεκτά επίπεδα.

Κατά την διαδικασία διαβούλευσης με την εποπτική αρχή ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στην εποπτική αρχή τις ακόλουθες πληροφορίες:

- τους σκοπούς και τα μέσα της σχεδιαζόμενης επεξεργασίας
- τα μέτρα και τις εγγυήσεις για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σύμφωνα με Κανονισμό
- την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων
- 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
- κατά περίπτωση, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων
- κάθε άλλη πληροφορία που ζητεί η εποπτική αρχή

Επιπλέον, ο υπεύθυνος επεξεργασίας θα πρέπει να συμβουλεύεται την εποπτική αρχή κάθε φορά που το δίκαιο των κρατών μελών απαιτεί από τους υπεύθυνους επεξεργασίας να διαβουλεύονται με την εποπτική αρχή ή / και να λαμβάνουν προηγούμενη έγκριση από αυτήν σε σχέση με την εκτέλεση καθήκοντος που ασκείται από τον εν λόγω υπεύθυνο προς το δημόσιο συμφέρον, περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία

3.7 Διαδικασία διενέργειας μιας μελέτης Εκτίμησης Αντικτύπου.

Ο Κανονισμός παρέχει ελάχιστες οδηγίες σχετικά με τη διαδικασία διενέργειας μιας Εκτίμησης Αντικτύπου, προβλέποντας μόνο ότι πρέπει να εκτιμηθεί η πιθανότητα εμφάνισης και η σοβαρότητα των επιπτώσεων ενός κινδύνου, λαμβάνοντας υπόψη τη φύση, το πεδίο, το πλαίσιο και τους σκοπούς της επεξεργασίας.

Επίσης, παρέχονται κάποιες κατευθύνσεις, συγκεκριμένα βήματα και απαιτήσεις για την εκτέλεση μιας Εκτίμησης Αντικτύπου. Πιο συγκεκριμένα ο ορίζει στο Άρθρο 35 παράγραφος 7 τα ελάχιστα περιεχόμενα μιας Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα ως εξής :

"*Η εκτίμηση θα πρέπει να περιέχει τουλάχιστον:*

- *Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας*
- *Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς*

- *Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων*
- *Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων*"

Γίνεται επομένως αντιληπτό ότι παρέχεται ένα ευρύ, γενικό πλαίσιο για το σχεδιασμό και τη διεξαγωγή μιας Εκτίμησης Αντικτύπου και δεν καθορίζεται η ακριβής διαδικασία για τη διενέργειά της πέρα από τα ελάχιστα χαρακτηριστικά που περιεγράφηκαν παραπάνω.

Το γεγονός αυτό δίνει την δυνατότητα στους υπεύθυνους επεξεργασίας να μπορούν να σχεδιάσουν και να υλοποιήσουν μια μελέτη Εκτίμησης Αντικτύπου με ελευθερία, ευελιξία και η οποία να είναι εναρμονισμένη με τη φύση, το πλαίσιο και το είδος των πράξεων επεξεργασίας.

Έτσι, ο υπεύθυνος επεξεργασίας είναι σε θέση να καθορίζει την ακριβή δομή και μορφή της Εκτίμησης Αντικτύπου ανάλογα με τις συγκεκριμένες συνθήκες και ανάγκες κάθε οργανισμού.

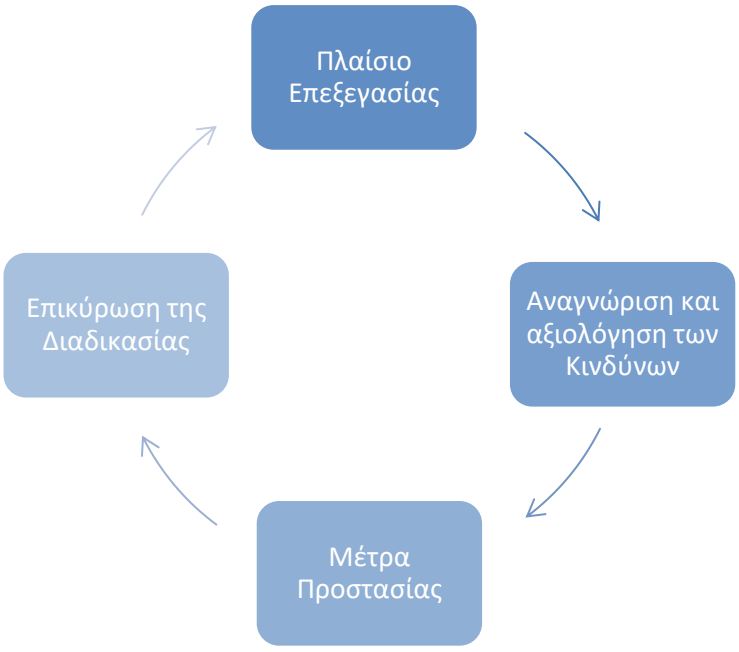
Παρά το γεγονός ότι δεν υπάρχει κανένας συγκεκριμένος τρόπος προσέγγισης, τα παρακάτω γενικά βήματα μπορούν να καθοδηγήσουν τους οργανισμούς στη διαδικασία διενέργειας μιας μελέτης Εκτίμησης Αντικτύπου:

- **Βήμα 1 :** Προσδιορισμός για το αν η διενέργεια της Εκτίμησης Αντικτύπου αποτελεί νομική υποχρέωση-Αρχική Αξιολόγηση.
- **Βήμα 2 :** Καθορισμός των χαρακτηριστικών του έργου και του πλαισίου επεξεργασίας ώστε να καταστεί δυνατή η εκτίμηση των κινδύνων
- **Βήμα 3 :** Προσδιορισμός των πιθανών κινδύνων που ενέχει η επεξεργασία για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
- **Βήμα 4 :** Προσδιορισμός των κατάλληλων τεχνικών και οργανωτικών μέτρων για την εξάλειψη ή τον περιορισμό των κινδύνων σε αποδεκτά επίπεδα.
- **Βήμα 5 :** Ενσωμάτωση των αποτελεσμάτων στην διαδικασία επεξεργασίας
- **Βήμα 6 :** Επανέλεγχος των διαδικασιών επεξεργασίας

Στην παρούσα εργασία πραγματοποιείται μια προσπάθεια μοντελοποίησης της διαδικασίας διενέργειας μιας Εκτίμησης Αντικτύπου και καταγραφής των στοιχείων τα οποία θα πρέπει να περιέχει προκειμένου να ικανοποιεί τις απαιτήσεις του Κανονισμού.

Η διαδικασία ανάπτυξης μιας Εκτίμησης Αντικτύπου αποτελείται από τέσσερα (4) βασικά στάδια :

1. **Καθορισμός του πλαισίου επεξεργασίας**: Καθορισμός και περιγραφή των πράξεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα, των δεδομένων που τυγχάνουν επεξεργασίας και των συμμετεχόντων στην επεξεργασία.
2. **Αναγνώριση και αξιολόγηση των Κινδύνων**: Καθορισμός και αξιολόγηση των κινδύνων που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα και που θα μπορούσαν να επηρεάσουν τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, προκειμένου να προσδιοριστεί εάν οι κίνδυνοι αντιμετωπίστηκαν επαρκώς.
3. **Καθορισμός και υλοποίηση των μέτρων προστασίας**: Καθορισμός και καταγραφή των υφιστάμενων ή προγραμματισμένων τεχνικών και οργανωτικών μέτρων προκειμένου να διασφαλίζεται η συμμόρφωση με τις νομικές απαιτήσεις αλλά και το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων για δεδομένα προσωπικού χαρακτήρα
4. **Επικύρωση της διαδικασίας**: Έλεγχος και λήψη απόφασης για το εάν τα αποτελέσματα της μελέτης θα εφαρμοστούν ή για το εάν η διαδικασία χρήζει αναθεώρησης και περαιτέρω διαβούλευσης.



Στο σημείο αυτό θα πρέπει να τονίσουμε ότι η ανάπτυξη μιας Εκτίμησης Αντικτύπου βασίζεται σε 2 βασικούς πυλώνες:

- Τη συμμόρφωση με τις θεμελιώδεις αρχές και τα δικαιώματα των υποκειμένων των δεδομένων που ορίζονται από το νόμο και τα οποία πρέπει να τηρούνται απαραιτήτως. Η συμμόρφωση με τις απαιτήσεις αυτές είναι μη διαπραγματεύσιμη καθώς θα πρέπει

να επιτυγχάνεται, ανεξάρτητα από τη φύση, τη σοβαρότητα και την πιθανότητα εμφάνισης των κινδύνων.

- Τη διαδικασία Διαχείρισης των Κινδύνων, με τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων, οι οποίοι σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα λαμβάνοντας 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.

3.8 Αναγνώριση των απαιτήσεων και των υποχρεώσεων του υπεύθυνου επεξεργασίας στα πλαίσια του Κανονισμού

Οι βασικές απαιτήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα, οι οποίες ορίζονται στον Κανονισμό και οι οποίες θα πρέπει να πληρούνται προκειμένου να επεξεργάζονται με νόμιμο τρόπο τα δεδομένα προσωπικού χαρακτήρα προστασίας από πλευράς υπεύθυνου και εκτελούντος την επεξεργασία είναι οι ακόλουθες:

- Η ικανοποίηση των βασικών αρχών επεξεργασίας δεδομένων προσωπικού χαρακτήρα όπως αυτές ορίζονται στον Κανονισμό.
- Η ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων, τα οποία περιλαμβάνουν διαδικασίες για την ενημέρωση του υποκειμένου των δεδομένων, τη διόρθωση και τη διαγραφή δεδομένων προσωπικού χαρακτήρα
- Η διαφάνεια των διαδικασιών ως προϋπόθεση για τη διασφάλιση των νομικών απαιτήσεων οι οποίες θα πρέπει να είναι τεκμηριωμένες και επαληθεύσιμες τόσο για τον ίδιο τον οργανισμό, όσο και για τα υποκείμενα των δεδομένων αλλά και τις αρμόδιες εποπτικές Αρχές
- Η ασφάλεια των διαδικασιών και των μέσων που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα με την υλοποίηση των κατάλληλων τεχνικών και οργανωτικών μέτρων

3.8.1 Νομικές απαιτήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα

Αναλυτικά οι βασικές νομικές απαιτήσεις τις οποίες θα πρέπει να ικανοποιεί κάθε υπεύθυνος επεξεργασίας στα πλαίσια συμμόρφωσης με τον Κανονισμό είναι οι ακόλουθες:

- **Αρχή του περιορισμού Σκοπού**: Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν θα πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς.
- **Αρχή της ελαχιστοποίησης των δεδομένων**: Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία
- **Ακρίβεια των δεδομένων** : Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας
- **Περίοδος κράτησης των δεδομένων προσωπικού χαρακτήρα:** Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο Γενικός Κανονισμός για την Προστασία των Δεδομένων για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων
- **Νομιμότητα, αντικειμενικότητα και διαφάνεια** : Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων**.**
- **Ακεραιότητα και εμπιστευτικότητα:** Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων
- **Δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων:** Όταν δεδομένα προσωπικού χαρακτήρα που αφορούν υποκείμενο των δεδομένων συλλέγονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες:
- **Δικαίωμα εναντίωσης στην επεξεργασία:** Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, , περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού

χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

- **Δικαίωμα διόρθωσης:** Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.
- **Δικαίωμα διαγραφής - δικαίωμα στη λήθη :**Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

  - τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,
  - το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,
  - το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 2,
  - τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,
  - τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας,
  - τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών που αναφέρονται στο άρθρο 8 παράγραφος 1.
- **Δικαίωμα περιορισμού της επεξεργασίας:** Το υποκείμενο των δεδομένων έχει το δικαίωμα να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα:
  - Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα

- Η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους
- Ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων
- Το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

- **Δικαίωμα στη φορητότητα των δεδομένων:** Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, όταν:
  - η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) και
  - η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

3.8.2 Οι κλασικές απαιτήσεις ασφάλειας πληροφοριών

Από τα τέλη της δεκαετίας του 1980, οι απαιτήσεις ασφάλειας πληροφοριών έχουν παίξει σημαντικό ρόλο στο σχεδιασμό και την ανάπτυξη των πληροφοριακών συστημάτων των οποίων η ασφάλεια πρέπει να εξασφαλίζεται.

Ο στόχος της ασφάλειας πληροφοριών είναι η προστασία των τριών βασικών ιδιοτήτων της πληροφορίας: της εμπιστευτικότητας(confidentiality), της ακεραιότητας(integrity) και της διαθεσιμότητας(availability) οι οποίες ορίζονται ως εξής:

- **Εμπιστευτικότητα (confidentiality)** είναι η απαίτηση για προστασία της ιδιότητας εκείνης της πληροφορίας που την καθιστά διαθέσιμη μόνο σε εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες
- **Ακεραιότητα (integrity)** είναι η απαίτηση για προστασία της ιδιότητας εκείνης της πληροφορίας που την καθιστά τροποποιήσιμη μόνο από εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες
- **Διαθεσιμότητα (availability)** είναι η απαίτηση για προστασία της ιδιότητας εκείνης της πληροφορίας που την καθιστά διαθέσιμη μέσα στον προβλεπόμενο χρόνο, όταν ζητείται από εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες

3.8.3 Απαιτήσεις ασφάλειας που στοχεύουν στην προστασία των υποκειμένων των δεδομένων

Πέρα από τις κλασικές απαιτήσεις ασφάλειας πληροφοριών , έχουν προκύψει περαιτέρω απαιτήσεις οι οποίες αφορούν ειδικά την προστασία των δεδομένων προσωπικού χαρακτήρα, και οι οποίες εισάγονται σε υφιστάμενους κανονισμούς προστασίας δεδομένων όπως και στο νέο Κανονισμό.

Από την οπτική της ασφάλειας των δεδομένων προσωπικού χαρακτήρα , οι οργανισμοί πρέπει επίσης να προστατεύουν τις επιχειρησιακές διαδικασίες οι οποίες περιλαμβάνουν την επεξεργασία προσωπικών δεδομένων.

Οι ακόλουθες απαιτήσεις προστασίας της προστασίας δεδομένων, αντικατοπτρίζουν τους στόχους του οργανισμού σε επιχειρησιακό επίπεδο

- Συμβατότητα
- Διαφάνεια
- Παρεμβατικότητα
- Λογοδοσία

Συγκεκριμένα οι εν λόγω απαιτήσεις ορίζονται ως εξής:

- **Συμβατότητα** είναι η απαίτηση η οποία αναφέρεται στην υποχρέωση επεξεργασίας των δεδομένων από πλευράς υπεύθυνου επεξεργασίας αποκλειστικά και μόνο για τον σκοπό για τον οποίο έχουν συλλεγεί. Τα σύνολα δεδομένων μπορούν ωστόσο να υποστούν επεξεργασία για δευτερεύοντες σκοπούς και μπορούν να συνδυαστούν με άλλα, δυνητικά διαθέσιμα στο κοινό δεδομένα. Αυτή η περαιτέρω επεξεργασία είναι νόμιμη μόνο υπό αυστηρά καθορισμένες συνθήκες. Ο Κανονισμός επιτρέπει αυτή τη χρήση των δεδομένων μόνο για αρχειακούς σκοπούς που είναι προς το δημόσιο συμφέρον, επιστημονικούς ή ιστορικούς ερευνητικούς σκοπούς ή για στατιστικούς σκοπούς.
- **Διαφάνεια** είναι η απαίτηση η οποία αναφέρεται στην υποχρέωση του υπεύθυνου επεξεργασίας να παρέχει στο υποκείμενο των δεδομένων αλλά και στις αρμόδιες εποπτικές αρχές όλες τις απαραίτητες πληροφορίες έτσι ώστε να είναι σε θέση να κατανοούν , σε διαφορετικό βαθμό, ποια δεδομένα συλλέγονται και υποβάλλονται σε επεξεργασία για συγκεκριμένο σκοπό, ποια συστήματα και διαδικασίες χρησιμοποιούνται για το σκοπό αυτό, ποιες είναι οι ροές των δεδομένων και ποιος είναι νομικά υπεύθυνος για τα δεδομένα και τα συστήματα στις διάφορες φάσεις της επεξεργασίας των δεδομένων.
  Η διαφάνεια είναι απαραίτητη για την παρακολούθηση και τον έλεγχο των δεδομένων σε όλη τη διάρκεια του κύκλου ζωής τους από την συλλογή τους έως τη διαγραφή τους και αποτελεί προϋπόθεση για νόμιμη επεξεργασία δεδομένων. Η ενημερωμένη συγκατάθεση μπορεί να δοθεί από τα υποκείμενα των δεδομένων μόνο εάν πληρείται η απαίτηση της διαφάνειας του συνόλου της επεξεργασίας των δεδομένων.

- **Παρεμβατικότητα** είναι η απαίτηση η οποία αναφέρεται στην υποχρέωση του υπεύθυνου επεξεργασίας να εξασφαλίζει την ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων .
  Για το σκοπό αυτό, οι υπεύθυνοι επεξεργασίας θα πρέπει να είναι σε θέση να παρεμβαίνουν στην επεξεργασία των δεδομένων καθ' 'όλη τη διάρκεια του κύκλου ζωής του από τη συλλογή μέχρι τη διαγραφή των δεδομένων.
- **Λογοδοσία** είναι η απαίτηση η οποία αναφέρεται στην υποχρέωση του υπεύθυνου επεξεργασίας να είναι σε θέση να αποδεικνύει ανά πάσα στιγμή ότι έχει αναπτύξει τα συστήματά του με απόλυτο σεβασμό στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ιδιαιτέρως στο δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα.
  Για το σκοπό αυτό οι υπεύθυνοι επεξεργασίας θα πρέπει να καταγράφουν τους εντοπισμένους κινδύνους αλλά και τα αντίστοιχα μέτρα τα οποία έχουν λάβει για την αντιμετώπιση των κινδύνων αυτών.
  Δεν αρκεί ένας οργανισμός να λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα αλλά πρέπει να είναι και σε θέση να αποδείξει ότι το έχει πράξει.
  Είναι πολύ σημαντικό να τονίσουμε ότι οι απαιτήσεις της προστασίας των δεδομένων προσωπικού χαρακτήρα απαιτούν ευρύτερη κατανόηση σε σύγκριση με την προστασία της ασφάλειας των πληροφοριακών συστημάτων δεδομένου ότι η προστασία των δεδομένων λαμβάνει επίσης υπόψη και μια εκτεταμένη πτυχή προστασίας.
  Η πτυχή αυτή αφορά την προστασία από κινδύνους οι οποίοι απορρέουν από τις δραστηριότητες του ίδιου του οργανισμού για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα εντός και εκτός των επιχειρηματικών διαδικασιών του.
  Συνεπώς, αυτό το οποίο διαφέρει είναι το γεγονός ότι οι οργανισμοί δεν πρέπει να διαθέτουν μόνο διαδικασίες και μηχανισμούς προκειμένου να επαληθεύουν την αξιοπιστία ενός ατόμου αλλά καλούνται πλέον οι ίδιοι να αποδεικνύουν την αξιοπιστία τους στα φυσικά πρόσωπα αλλά και στους εποπτικούς φορείς μέσω διαφανών και τεκμηριωμένων μηχανισμών και διαδικασιών.
  Η διενέργεια μιας μελέτης Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί το κατάλληλο εργαλείο για την επίτευξη του σκοπού αυτού.

3.8.4 Αντιστοίχιση απαιτήσεων ασφάλειας και προστασίας δεδομένων με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR)

Απαίτηση	Άρθρα Κανονισμού
Εμπιστευτικότητα	Άρθρο 5 παράγραφος 1 στοιχείο στ' Άρθρο 25 (Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού) Άρθρο 28 παράγραφος 3 στοιχείο β Άρθρο 32(Ασφάλεια Επεξεργασίας)
Ακεραιότητα	Άρθρο 5 παράγραφος 1 στοιχεία δ' και στ' Άρθρο 25 (Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού) Άρθρο 32 (Ασφάλεια Επεξεργασίας)
Διαθεσιμότητα	Άρθρο 5 παράγραφος 1 στοιχείο ε Άρθρο 13 (Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων) Άρθρο 14 (Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων) Άρθρο 15 (Δικαίωμα Πρόσβασης) Άρθρο 20 (Δικαίωμα Φορητότητας) Άρθρο 25 (Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού) Άρθρο 32 (Ασφάλεια Επεξεργασίας)
Συμβατότητα	Άρθρο 5 παράγραφος 1 στοιχεία β' και ε' Άρθρο 6 (Νομιμότητα της επεξεργασίας) Άρθρο 17 Άρθρο 20 Άρθρο 22 Άρθρο 25

Διαφάνεια	Άρθρο 5 παράγραφος 1 στοιχείο α' Άρθρο 12 Άρθρο 13 Άρθρο 14 Άρθρο 15 Άρθρο 19 Άρθρο 25 Άρθρο 30 Άρθρο 33 Άρθρο 35 Άρθρο 40 Άρθρο 42
Παρεμβατικότητα	Άρθρο 5 παράγραφος 1 στοιχεία β' και στ' Άρθρο 13 παράγραφος 2 στοιχείο γ' Άρθρο 14 παράγραφος 2 στοιχείο δ' Άρθρο 15 παράγραφος 1 στοιχείο ε' Άρθρο 16 Άρθρο 17 Άρθρο 18 Άρθρο 20 Άρθρο 21 Άρθρο 25 Άρθρο 32
Ελαχιστοποίηση Δεδομένων	Άρθρο 5 παράγραφος 1 στοιχεία γ και ε Άρθρο 25 Άρθρο 32
Λογοδοσία	Άρθρο 5 παράγραφος 2 Άρθρο 24 Άρθρο 30 Άρθρο 35

Άρθρο 36

Πίνακας 4 - Αντιστοίχιση Απαιτήσεων

Κεφάλαιο 4: Μεθοδολογία διενέργειας της μελέτης Εκτίμησης Αντικτύπου

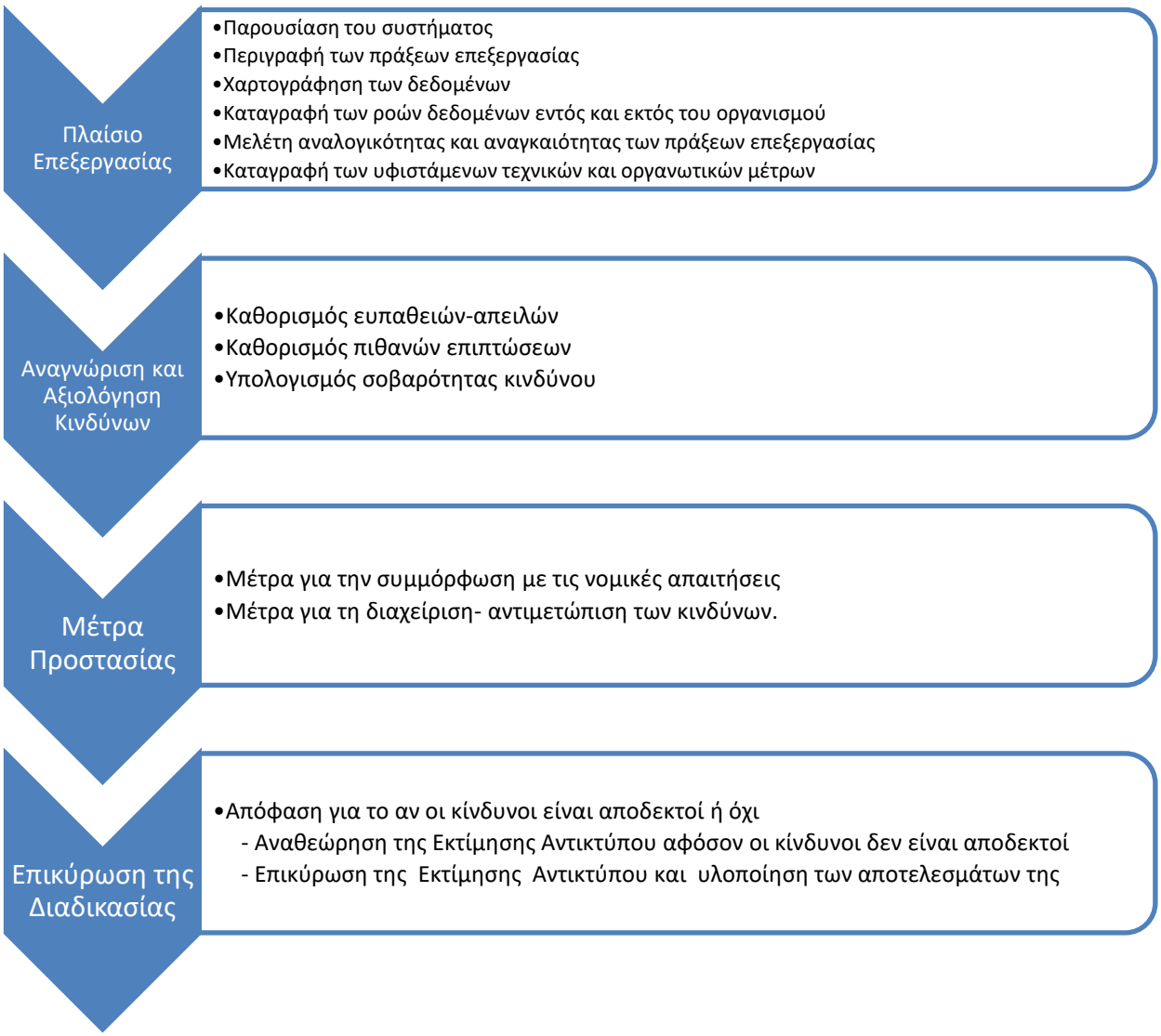
Στο κεφάλαιο αυτό πραγματοποιείται μια προσπάθεια μοντελοποίησης της διαδικασίας διενέργειας μιας μελέτης Εκτίμησης Αντικτύπου αλλά και των βημάτων τα οποία θα πρέπει να ακολουθήσουν οι οργανισμοί οι οποίοι φέρουν την υποχρέωση υλοποίηση της.

Η Εκτίμηση Αντικτύπου θα πρέπει να λογίζεται ως μια συνεχής διεργασία η οποία έχει ως στόχο τη διαρκή βελτίωση του επιπέδου συμμόρφωσης του οργανισμού με τις απαιτήσεις του Κανονισμού αλλά και εν γένει με τις απαιτήσεις ασφάλειας πληροφοριών.

Επομένως, μερικές φορές απαιτούνται αρκετές επαναλήψεις προκειμένου να επιτευχθεί η δημιουργία ενός συστήματος με αποδεκτό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα.

Κρίνεται επίσης απαραίτητη η παρακολούθηση της λειτουργίας του συστήματος για τον εντοπισμό των αλλαγών με την πάροδο του χρόνου (στο πλαίσιο, τα μέτρα προστασίας, τους κινδύνους κ.λπ.), για παράδειγμα, κάθε χρόνο, και η αναθεώρηση της Εκτίμησης Αντικτύπου εφόσον κάποια σημαντική αλλαγή λάβει χώρα

Το παρακάτω διάγραμμα παρουσιάζει τη λεπτομερή προσέγγιση για τη διενέργεια της μελέτης Εκτίμησης Αντικτύπου:



4.1 Στάδιο1: Πλαίσιο επεξεργασίας.

Στο πλαίσιο της διαδικασίας διενέργειας της Εκτίμησης Αντικτύπου οι οργανισμοί θα πρέπει να περιγράψουν τον τρόπο με τον οποίο τα δεδομένα συλλέγονται, αποθηκεύονται, χρησιμοποιούνται και διαγράφονται. Θα πρέπει να καταγράφεται ποια δεδομένα χρησιμοποιούνται, με ποιο τρόπο και ποιοι έχουν πρόσβαση σε αυτά. Αυτό το βήμα αποτελεί βασικό μέρος οποιασδήποτε διαδικασίας Εκτίμησης Αντικτύπου.

Η διεξοδική αξιολόγηση των κινδύνων για την προστασία της ιδιωτικής ζωής είναι δυνατή μόνο εάν ο οργανισμός κατανοεί πλήρως τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα. Μια ελλιπής κατανόηση του τρόπου με τον οποίο χρησιμοποιούνται τα δεδομένα μπορεί να ενέχει υψηλούς κίνδυνους για την ιδιωτική ζωή. Για παράδειγμα ενδέχεται να χρησιμοποιηθούν δεδομένα για μη νόμιμους σκοπούς ή δεδομένα τα οποία δεν είναι απαραίτητα για έναν συγκεκριμένο σκοπό επεξεργασίας.

Στο στάδιο αυτό στόχος είναι η απόκτηση σαφούς εικόνας της διαδικασίας επεξεργασίας που ενέχει υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Αποτελείται από δύο βήματα καθώς αρχικά θα πρέπει να καταγραφεί το γενικότερο πλαίσιο της διαδικασίας επεξεργασίας το οποίο περιλαμβάνει τη φύση, το πεδίο εφαρμογής, τους σκοπούς και τα προσδοκώμενα οφέλη της επεξεργασίας αλλά και τους συμμετέχοντες σε αυτήν ενώ στη συνέχεια θα πρέπει να καταγραφούν αναλυτικά όλες οι λεπτομέρειες της επεξεργασίας οι οποίες σχετίζονται άμεσα με τα δεδομένα προσωπικού χαρακτήρα όπως η αναλυτική καταγραφή του συνόλου των δεδομένων προσωπικού χαρακτήρα τα οποία συλλέγονται και οι ροές των εν λόγω δεδομένων από και προς το εσωτερικό του οργανισμού

Κάθε Εκτίμηση Αντικτύπου θα πρέπει να περιλαμβάνει επίσης τα οφέλη της επεξεργασίας όσον αφορά όλα τα ενδιαφερόμενα μέρη, όπως ένα υποκείμενο των δεδομένων ή μια ομάδα υποκειμένων ,του οργανισμού και της κοινωνίας εν γένει.

Επίσης, θα πρέπει να περιέχεται μια σαφής δήλωση ή περιγραφή του πλαισίου και του σκοπού της επεξεργασίας. Επίσης η εξέταση των οφελών πρέπει να πραγματοποιείται στο αρχικό στάδιο, δεδομένης της στενής σχέσης μεταξύ του «σκοπού» και των «οφελών» μιας συγκεκριμένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Πράγματι, ο Κανονισμός απαιτεί ρητά την εξέταση των "σκοπών επεξεργασίας" σε σχέση με τους κινδύνους που ενέχει η επεξεργασία αυτή. Έτσι, στο πλαίσιο των απαιτήσεων του Κανονισμού, το άρθρο 35 παράγραφος 7 υποδηλώνει ότι σε οποιαδήποτε Εκτίμηση Αντικτύπου θα πρέπει να λαμβάνεται υπόψη η αναλογικότητα των κινδύνων σε σχέση με τους σκοπούς, τα συμφέροντα ή τα οφέλη που επιδιώκονται. Αυτό δείχνει ότι η τελική αξιολόγηση του κινδύνου σχετίζεται με την τελική εκτίμηση του σκοπού, ή του οφέλους.

Ο λόγος για τον οποίο τα οφέλη και οι σκοποί της επεξεργασίας πρέπει να λαμβάνονται υπόψη κατά το αρχικό στάδιο της Εκτίμησης Αντικτύπου αλλά και της διαδικασίας επεξεργασίας γενικότερα είναι προκειμένου να αποφευχθεί η μη επιθυμητή ή περιττή μείωση των οφελών της επεξεργασίας, ιδίως όταν τα οφέλη είναι σαφή και προσδιορισμένα για όλους τους ενδιαφερόμενους.

Ένα ενδεικτικό παράδειγμα τέτοιας απώλειας των οφελών είναι η μείωση της λειτουργικότητας του συστήματος ή η λιγότερο αποτελεσματική εμπειρία του πελάτη κατά την χρήση του συστήματος.(όταν για παράδειγμα δεν επιτρέπεται η παροχή της δυνατότητας αποθήκευσης δεδομένων καρτών πληρωμής για μελλοντικές αγορές.)

Επίσης, ένα ιδιαιτέρως σημαντικό γεγονός είναι ότι κατά την αξιολόγηση των κινδύνων στο πλαίσιο του Κανονισμού πρέπει ο υπεύθυνος επεξεργασίας να διασφαλίσει ότι, διατηρώντας τα οφέλη, δεν θα επηρεαστούν δυσανάλογα αρνητικά τα υποκείμενα των δεδομένων όπως και τα θεμελιώδη δικαιώματά αλλά και οι ελευθερίες τους.

4.1.1 Γενική Περιγραφή της διεργασίας επεξεργασίας

Το στάδιο αυτό θα πρέπει να περιέχει αρχικά ορισμένες γενικές πληροφορίες για την μελέτη Εκτίμησης Αντικτύπου όπως στοιχεία για τον υπεύθυνο επεξεργασίας, τον Υπεύθυνο Προστασίας Δεδομένων , των συμμετεχόντων σε αυτή, την ημερομηνία διεξαγωγής και την έκδοση της Εκτίμησης Αντικτύπου αλλά και τα στοιχεία του ατόμου που έδωσε την τελική έγκριση για την επικύρωση των περιεχομένων της.

Ακολούθως, το στάδιο αυτό θα πρέπει να περιέχει την περιγραφή των πράξεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα, των σκοπών για τους οποίους συλλέχθηκαν αρχικά τα δεδομένα , της νομικής βάσης, τους συμμετέχοντες σε αυτή όπως και πληροφορίες σχετικά με τρίτες οντότητες στις οποίες διαβιβάζονται τα δεδομένα.

Ο Υπεύθυνος επεξεργασίας θα πρέπει επίσης να είναι σε θέση να απαντήσει στην ερώτηση*:*

Ποια θα είναι τα οφέλη από τη συγκεκριμένη διεργασία για τον οργανισμό, τα υποκείμενα των δεδομένων και για την κοινωνία γενικά?

Συνοπτικά στο στάδιο αυτό θα πρέπει να καταγράφονται τα ακόλουθα στοιχεία:

- Περιγραφή της λειτουργίας της διεργασίας επεξεργασίας.
- Καθορισμός και καταγραφή των σκοπών της διαδικασίας επεξεργασίας
- Καταγραφή των συμμετεχόντων στην διεργασία επεξεργασίας.
- Αναγνώριση και καταγραφή του υπεύθυνου επεξεργασίας.
- Αναγνώριση και καταγραφή του εκτελούντα την επεξεργασία.
- Αναγνώριση και καταγραφή του Υπεύθυνου Επεξεργασίας Δεδομένων.

Στους παρακάτω πίνακες καταγράφονται οι πληροφορίες που πρέπει να περιέχει η Εκτίμηση Αντικτύπου στο στάδιο αυτό.

Γενικά Στοιχεία Πράξης Επεξεργασίας	
Υπεύθυνος Επεξεργασίας	
Εκτελών την Επεξεργασία	
Όνομα πράξης Επεξεργασίας ή Έργου/Συστήματος/Εφαρμογής για το οποίο πραγματοποιήθηκε η Εκτίμηση Αντικτύπου	
Συμμετέχοντες στην διαδικασία εκπόνησης της μελέτης Εκτίμησης Αντικτύπου	
Υπεύθυνος Προστασίας Δεδομένων	
Υπεύθυνος Επικύρωσης	
Ημερομηνία διεξαγωγής	
Έκδοση (Αρχική ή Αναθεωρημένη)	

Περιγραφή Πράξης Επεξεργασίας	
Όνομα διαδικασίας Επεξεργασίας ή Έργου/Συστήματος/Εφαρμογής για το οποίο πραγματοποιήθηκε η Εκτίμηση Αντικτύπου	
Περιγραφή της διαδικασίας επεξεργασίας	
Δεδομένα που συλλέγονται	
Σκοπός της Επεξεργασίας	
Νομική Βάση Επεξεργασίας	
Συμμετέχοντες στην Επεξεργασία	

Τρίτα Μέρη στα οποία διαβιβάζονται τα δεδομένα
Εκτελών την Επεξεργασία

4.1.2 Χαρτογράφηση των δεδομένων προσωπικού χαρακτήρα

Αφού έχει προηγηθεί η γενική περιγραφή της φύσης και του πεδίου της πράξης επεξεργασίας, ο υπεύθυνος επεξεργασίας θα πρέπει να περιγράψει και να χαρτογραφήσει τις ροές προσωπικών δεδομένων τα οποία συλλέγονται στα πλαίσια της συγκεκριμένης πράξη επεξεργασίας.

Η ανάλυση αυτή θα πρέπει να είναι επαρκώς λεπτομερής ώστε να παρέχει μια αίσθηση για το ποια δεδομένα θα συλλέγονται, θα χρησιμοποιούνται ,θα γνωστοποιούνται και θα διαβιβάζονται, πώς θα κρατούνται και θα προστατεύονται και ποιος θα έχει πρόσβαση σε αυτά.

Στο στάδιο αυτό η Εκτίμηση Αντικτύπου θα πρέπει να περιέχει την περιγραφή των διεργασιών οι οποίες απαιτούν την επεξεργασία δεδομένων αλλά και των υποστηρικτικών αγαθών τα οποία σχετίζονται με τα προσωπικά δεδομένα σε όλη τη διάρκεια του κύκλου ζωής τους από τη συλλογή μέχρι και τη διαγραφή τους.

Θα πρέπει επίσης να εξηγεί ποια δεδομένα χρησιμοποιούνται, για ποιο σκοπό και σύμφωνα με ποια νομική βάση πραγματοποιείται η επεξεργασία.

Αυτό το βήμα αποτελεί βασικό μέρος οποιασδήποτε Εκτίμησης Αντικτύπου καθώς η διεξοδική αξιολόγηση των κινδύνων για την προστασία της ιδιωτικής ζωής είναι δυνατή μόνο εάν οργανισμός κατανοεί πλήρως τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα προσωπικού χαρακτήρα σε ένα έργο. Μια ελλιπής κατανόηση μπορεί να προκαλέσει έναν σημαντικό κίνδυνο για δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

Αναλυτικά **για κάθε διεργασία** στο σύστημα η οποία απαιτεί την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να καταγράφονται τα εξής στοιχεία:

- Τα δεδομένα προσωπικού χαρακτήρα τα οποία είναι απαραίτητα για την επίτευξη των σκοπών της διεργασίας
- Το είδος των δεδομένων αυτών δηλαδή αν τα δεδομένα αυτά είναι απλά ή ευαίσθητα
- Τον σκοπό της επεξεργασίας για κάθε δεδομένο ξεχωριστά ή για μια κατηγορία δεδομένων
- Τη νομική βάση στην οποία βασίζεται η επεξεργασία
- Τη μέθοδο συλλογής των δεδομένων

- Τους αποδέκτες των δεδομένων προσωπικού χαρακτήρα σε περίπτωση κατά την οποία τα δεδομένα διαβιβάζονται σε τρίτα μέρη και το σκοπό για τον οποίο είναι απαραίτητη η πράξη αυτή
- Τα άτομα τα οποία έχουν εξουσιοδοτημένη πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και τεκμηριωμένη αιτιολόγηση γιατί συμβαίνει αυτό
- Την περίοδο διατήρησης των δεδομένων για κάθε τύπο ή κατηγορία δεδομένων ξεχωριστά και τεκμηριωμένη αιτιολόγηση
- Την καταγραφή των υποστηρικτικών αγαθών τα οποία σχετίζονται με τα δεδομένα προσωπικού χαρακτήρα και είναι απαραίτητα για την επίτευξη των σκοπών της επεξεργασίας.
- Τον προσδιορισμό και την καταγραφή των υποκειμένων των δεδομένων

Περιγραφή ροών Δεδομένων Προσωπικού Χαρακτήρα
Όνομα διαδικασίας Επεξεργασίας ή Έργου/Συστήματος/Εφαρμογής για το οποίο πραγματοποιήθηκε η Εκτίμηση Αντικτύπου
Δεδομένα Προσωπικού Χαρακτήρα που είναι απαραίτητα.
Είδος Δεδομένων Προσωπικού Χαρακτήρα (Απλά η Ευαίσθητα)
Σκοπός της Επεξεργασίας
Νομική Βάση της Επεξεργασίας
Μέθοδος συλλογής δεδομένων
Χρονική Περίοδος Κράτησης των Δεδομένων
Άτομα με εξουσιοδοτημένη πρόσβαση στα δεδομένα και αιτιολόγηση
Τρίτα Μέρη στα οποία διαβιβάζονται τα δεδομένα
Μέθοδος μετάδοσης των δεδομένων
Υποστηρικτικά αγαθά
Υφιστάμενα τεχνικά και οργανωτικά μέτρα

4.1.3 Εκτίμηση αναλογικότητας και αναγκαιότητας

Στο στάδιο αυτό ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί σε μια εκτίμηση της αναλογικότητας και της αναγκαιότητας της υπό εξέτασης διαδικασίας επεξεργασίας.

Αυτό σημαίνει ότι θα πρέπει να προβεί σε:

- Καταγραφή των λόγων σύμφωνα με τους οποίους οι σκοποί της επεξεργασίας που καθορίζονται, είναι σαφείς και νόμιμοι
- Καθορισμό της νομική βάσης της επεξεργασίας
- Τεκμηρίωση γιατί κάθε ένα από τα δεδομένα που συλλέγονται είναι απαραίτητο για την επίτευξη των σκοπών της επεξεργασίας
- Τεκμηρίωση για το εάν οι διάρκειες αποθήκευσης για κάθε δεδομένο δικαιολογούνται από τις νομικές απαιτήσεις ή / και τις ανάγκες επεξεργασίας.
- Αξιολόγηση για το κατά πόσο τα δεδομένα τα οποία συλλέγονται είναι απαραίτητα για την επίτευξη των σκοπών επεξεργασίας.
- Τα οφέλη της επεξεργασίας όσον αφορά τα ενδιαφερόμενα μέρη, όπως ένα υποκείμενο των δεδομένων ή μια ομάδα υποκειμένων ,του οργανισμού και της κοινωνίας εν γένει.

Μια ολοκληρωμένη Εκτίμηση Αντικτύπου θα πρέπει να περιέχει τις ακόλουθες πληροφορίες σχετικά με τον κύκλο ζωής των δεδομένων κατά τη διαδικασία της επεξεργασίας.

- **Συλλογή Δεδομένων**
  - Τα προσωπικά δεδομένα των οποίων η συλλογή είναι απαραίτητη για την επίτευξη των σκοπών της επεξεργασίας συμπεριλαμβανομένων τυχόν ευαίσθητων δεδομένων.
  - Τον συγκεκριμένο σκοπό για τον οποίο κρίνεται απαραίτητη η συλλογή των δεδομένων αυτών
  - Τη νομική βάση της συλλογής των δεδομένων
  - Με ποιο τρόπο σχετίζεται η συλλογή με τις λειτουργίες ή τις δραστηριότητες του οργανισμού
  - Με ποιο πραγματοποιείται η συλλογή (π.χ. έντυπα, ηλεκτρονικά έντυπα, ηλεκτρονικές συναλλαγές, CCTV κ.λπ.)
  - Οποιεσδήποτε δυνητικά ευαίσθητες ή παρεμβατικές μεθόδους συλλογής (για παράδειγμα, φωτογραφίες, δακτυλικά αποτυπώματα, δοκιμές φαρμάκων, συλλογή γενετικών δεδομένων)
- **Χρήση Δεδομένων**
  - Όλες τις προγραμματισμένες χρήσεις των δεδομένων, συμπεριλαμβανομένων των σπάνιων χρήσεων
  - Τον τρόπο με τον οποίο όλες αυτές οι χρήσεις σχετίζονται με το σκοπό της συλλογής
  - Τυχόν δευτερεύουσες χρήσεις των δεδομένων.
  - Εάν απαιτείται συγκατάθεση για τη δευτερεύουσα χρήση
  - Εάν η δευτερεύουσα χρήση σχετίζεται ή σχετίζεται άμεσα με το σκοπό της συλλογής
  - Εάν ένα άτομο μπορεί να αρνηθεί τη συγκατάθεσή του για δευτερεύουσες χρήσεις και να εξακολουθήσει να συμμετέχει στο έργο
  - Τυχόν συνέπειες για τα άτομα που αρνούνται τη συγκατάθεση
- **Αποκάλυψη δεδομένων**
  - Ποια άτομα θα έχουν πρόσβαση στα δεδομένα

- Με ποιο τρόπο θα έχουν πρόσβαση στα δεδομένα
- Για ποιο λόγο θα τους δοθεί η πρόσβαση στα δεδομένα
- Κατά πόσον τα δεδομένα πρέπει να δημοσιεύονται ή να γνωστοποιούνται σε μητρώο, περιλαμβανομένου δημόσιου μητρώου
- Εάν το υποκείμενο θα ενημερωθεί για την αποκάλυψη των δεδομένων του σε τρίτες οντότητες
- Εάν η αποκάλυψη επιτρέπεται ή απαιτείται από το νόμο, και εάν ναι, σύμφωνα με ποια νομική βάση
- Εάν τα δεδομένα θα αποκαλυφθούν σε τρίτες οντότητες εκτός Ευρωπαϊκής Ένωσης και αν ναι σε ποιες χώρες

- **Διατήρηση και διαγραφή των δεδομένων**
  - Την περίοδο διατήρησης των δεδομένων
  - Την διαδικασία διαγραφής των δεδομένων μετά το πέρας της περιόδου κράτησης
  - Την πολιτική διατήρησης δεδομένων και το χρονοδιάγραμμα καταστροφ

4.1.4 Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα

Είδος δεδομένων προσωπικού χαρακτήρα	Κατηγορίες δεδομένων προσωπικού χαρακτήρα

Απλά δεδομένα προσωπικού χαρακτήρα: κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο	• Στοιχεία αναγνώρισης όπως:
	  ○ Όνομα και Επώνυμο
	  ○ Ηλικία
	  ○ Διεύθυνση κατοικίας
	  ○ Επάγγελμα
	  ○ Οικογενειακή κατάσταση
	• Φυσικά χαρακτηριστικά
	• Στοιχεία που αφορούν την Εκπαίδευση
	  ○ Επαγγελματική ζωή
	  ○ Βιογραφικό σημείωμα
	  ○ Εκπαίδευση και επαγγελματική κατάρτιση
	  ○ Βραβεία
	• Οικονομική κατάσταση
	  ○ Εισόδημα
	  ○ Περιουσιακά στοιχεία
	  ○ Οικονομική συμπεριφορά
	  ○ Φορολογική Κατάσταση
	• Προσωπική ζωή
	  ○ Ενδιαφέροντα
	  ○ Δραστηριότητες
	  ○ Συνήθειες
	• Δεδομένα σύνδεσης
	  ○ Διεύθυνση Διαδικτυακού Πρωτοκόλλου(IP διεύθυνση)
	  ○ Cookies

Είδος δεδομένων προσωπικού χαρακτήρα	Κατηγορίες δεδομένων προσωπικού χαρακτήρα
Ευαίσθητα **δεδομένα προσωπικού χαρακτήρα**	Δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν : ○ Φυλετική ή εθνοτική καταγωγή ○ Πολιτικά φρονήματα ○ Θρησκευτικές ή φιλοσοφικές πεποιθήσεις ○ Συμμετοχή σε συνδικαλιστική οργάνωση ○ Ποινικές καταδίκες και αδικήματα ○ Τη σεξουαλική ζωή φυσικού προσώπου ○ Τον γενετήσιο προσανατολισμό Γενετικά δεδομένα: Τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου Βιομετρικά Δεδομένα: Δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα Δεδομένα που αφορούν την υγεία: Δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του

Πίνακας 5 - Κατηγορίες Δεδομένων

4.1.5 Υποστηρικτικά Αγαθά

Τα υποστηρικτικά αγαθά αποτελούν συστατικά ενός πληροφοριακού συστήματος τα οποία έχουν άμεση σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε όλη τη διάρκεια του κύκλου ζωής τους από τη συλλογή μέχρι την διαγραφή.

Είδος των υποστηρικτικών Αγαθών	Παραδείγματα
Υλικό	• Τερματικά • Εξυπηρετητές • Μονάδες εξωτερικής αποθήκευσης • Σκληροί Δίσκοι • Εκτυπωτές
Λογισμικό	• Λειτουργικό Σύστημα • Βάσεις Δεδομένων • Εταιρικές Εφαρμογές
Δίκτυα	• Καλώδιο ηλεκτρικού ρεύματος και δεδομένων • Οπτικές ίνες • Μηχανήματα δικτύου • ασύρματα δίκτυα • οπτικές ίνες • συσκευές δρομολόγησης και μεταγωγής
Ανθρώπινο Δυναμικό	• Χρήστες • Διαχειριστές • Διοικητικά Στελέχη • Τρίτες Οντότητες
Μέσα έγγραφης αποτύπωσης	• Έγγραφα χαρτιού • Εκτυπώσεις • Φωτοαντίγραφα, • Χειρόγραφα έγγραφα

Μέσα μετάδοσης αρχείων	• Ηλεκτρονικό Ταχυδρομείο • Ροές Εργασίας

Πίνακας 6 - Υποστηρικτικά Αγαθά

4.2 Στάδιο 2: Αναγνώριση και Αξιολόγηση Κινδύνων

Σε αυτό το στάδιο, οι οργανισμοί θα πρέπει να προσδιορίσουν και να αξιολογήσουν τους πιθανούς κινδύνους που ενέχει η διαδικασία της επεξεργασίας όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα.

Θεμελιώδης αρχή της Εκτίμησης Αντικτύπου η οποία την διαφοροποιεί από τη βασική προσέγγιση αξιολόγησης κινδύνων στον τομέα της ασφάλειας πληροφοριών είναι ότι αποτελεί μια μορφή διαχείρισης κινδύνου για τα υποκείμενα των δεδομένων.

Κατά τη διεξαγωγή της ένας οργανισμός θα πρέπει να εξετάσει συστηματικά τον τρόπο με τον οποίο μια πράξη επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα επηρεάσει τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Υπάρχουν διάφοροι τρόποι με τους οποίους ένα έργο μπορεί να επηρεάσει την ιδιωτική ζωή ή να θέσει σε κίνδυνο τα δεδομένα προσωπικού χαρακτήρα. Οι κίνδυνοι για τα υποκείμενα των δεδομένων συνήθως συνεπάγονται και συσχετισμένους κινδύνους για τον οργανισμό. Για παράδειγμα, ένα έργο το οποίο ενέχει υψηλό κίνδυνο για τις ελευθερίες και τα δικαιώματα των υποκειμένων των δεδομένων αυξάνει επίσης τον κίνδυνο για τον ίδιο τον οργανισμό στο πλαίσιο της επιβολής προστίμων ή της απώλειας φήμης.

Σε αυτό το βήμα, οι προσδιορισμένοι κίνδυνοι και οι συναφείς απειλές αξιολογούνται συναρτήσει της σοβαρότητα των επιπτώσεων και της πιθανότητα εμφάνισης ενός κινδύνου. Προκειμένου να αξιολογηθούν οι επιπτώσεις και η πιθανότητα, δύναται να χρησιμοποιηθούν αρκετά ευρέως διαθέσιμα μοντέλα.

Το ενδεικτικό μοντέλο αξιολόγησης που προτείνεται και αναλύεται στο πλαίσιο της παρούσας εργασίας βασίζεται κυρίως στη μεθοδολογία που προτείνει η Γαλλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (CNIL).

Ωστόσο, είναι αποδεκτή η χρήση εναλλακτικών μεθοδολογιών εφόσον οι κίνδυνοι για την προστασία της ιδιωτικής ζωής που μπορούν να επηρεάσουν το υποκείμενο των δεδομένων προσδιορίζονται και ποσοτικοποιούνται κατάλληλα

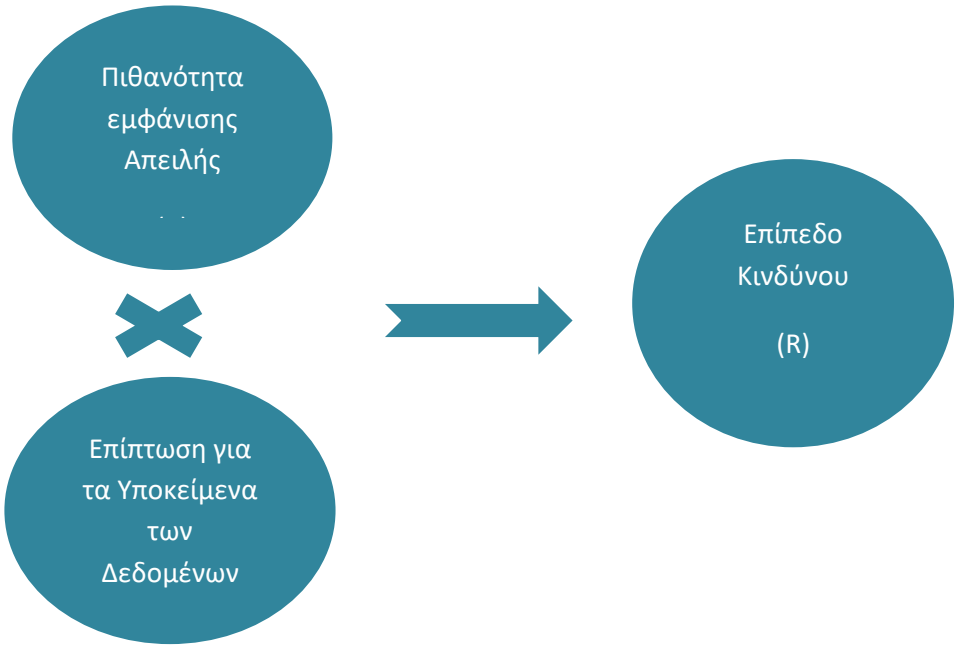
4.2.1 Αναγνώριση Κινδύνων

Στο στάδιο αυτό οι οργανισμοί θα πρέπει να καταγράφουν όλους τους πιθανούς κινδύνους που ελλοχεύουν από την διενέργεια μιας πράξης επεξεργασίας σχετικά με τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων των οποίων τα δεδομένα τυγχάνουν επεξεργασίας.

Η έννοια του κινδύνου

Κίνδυνος είναι ένα υποθετικό σενάριο το οποίο περιγράφει πως **οι πηγές των κινδύνων στο πλαίσιο απειλών** (πχ ένας εργαζόμενος στο εσωτερικό του οργανισμού) δύναται να εκμεταλλεύονται ευπάθειες **των υποστηρικτικών για τα δεδομένα προσωπικού χαρακτήρα αγαθών** (πχ σύστημα διαχείρισης αρχείων το οποίο επιτρέπει την τροποποίηση των δεδομένων) επιτρέποντας να λάβουν χώρα **μη επιθυμητά γεγονότα** .

(πχ μη εξουσιοδοτημένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα) προκαλώντας **επιπτώσεις** για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.(πχ αίσθημα εισβολής στην ιδιωτική ζωή).



Στο πλαίσιο της Εκτίμησης Αντικτύπου ο κίνδυνος ορίζεται ως το γινόμενο της πιθανότητας να συμβεί ένα **γεγονός** επί την επίπτωση που θα προκύψει για τα υποκείμενα των δεδομένων λόγω του περιστατικού.

Στο πεδίο της προστασίας δεδομένων προσωπικού χαρακτήρα ως **γεγονός** ορίζεται ένα περιστατικό ή μια κατάσταση του συστήματος, του δικτύου, ή μιας υπηρεσίας που υποδεικνύει την παραβίαση των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων λαμβάνοντας υπόψη τη φύση, το πεδίο, το πλαίσιο και το σκοπό της επεξεργασίας.

Η **πιθανότητα** να συμβεί ένα περιστατικό παραβίασης των δεδομένων είναι συνάρτηση της πιθανότητας να εμφανιστεί μια απειλή και της πιθανότητας αυτή η απειλή να εκμεταλλευτεί τις σχετικές ευπάθειες του συστήματος.

Η **επίπτωση** της εμφάνισης ενός περιστατικού παραβίασης των δεδομένων είναι συνάρτηση των ενδεχόμενων επιπτώσεων που θα έχει το περιστατικό στο υποκείμενο των δεδομένων ως αποτέλεσμα της ζημίας που θα υποστούν τα δικαιώματα και οι ελευθερίες του.

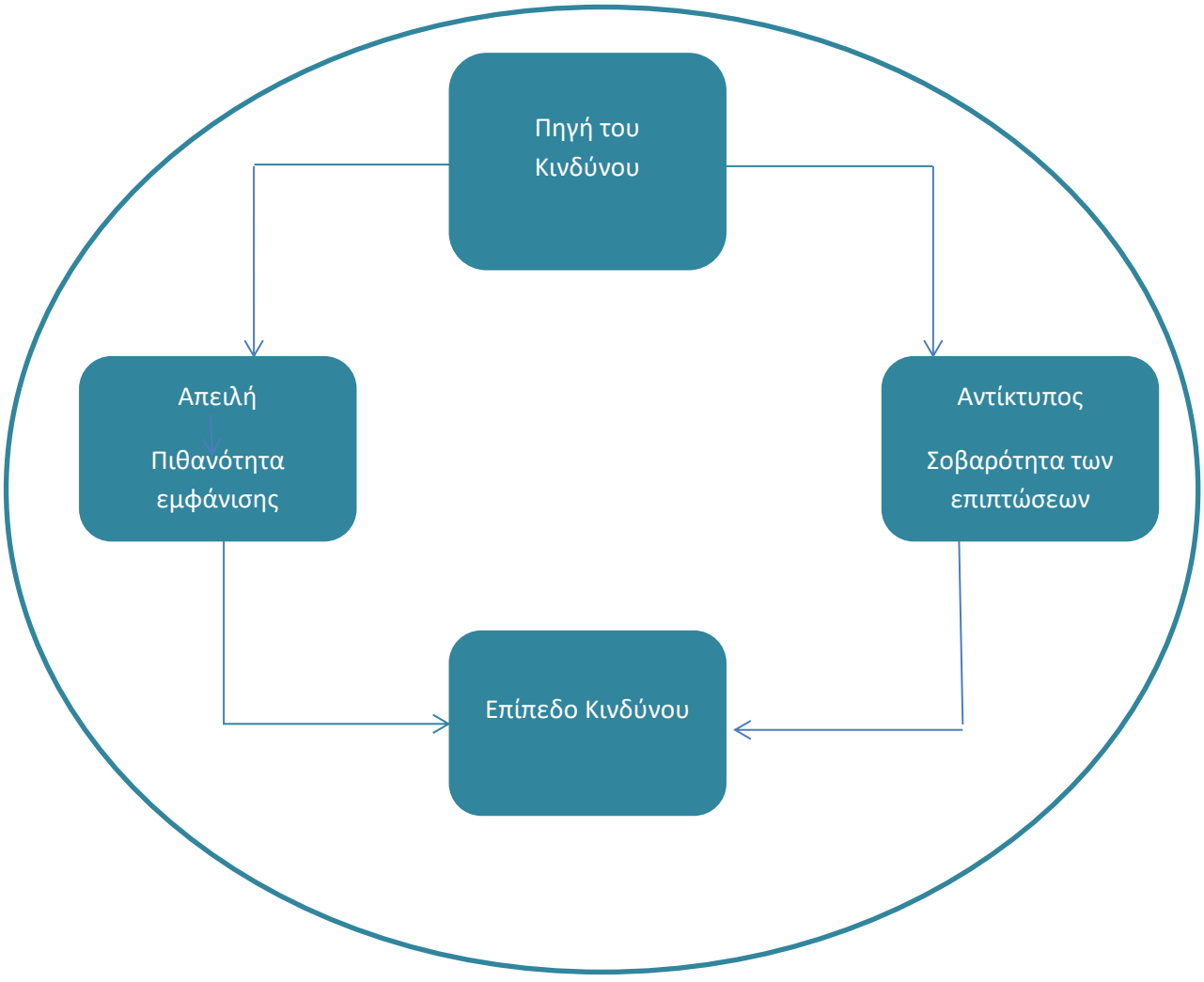
Έτσι, οι οργανισμοί πρέπει να έχουν διαδικασίες που τους επιτρέπουν να σταθμίζουν με αξιοπιστία και συνέπεια τους κινδύνους προκειμένου να συμμορφωθούν με τις απαιτήσεις του Κανονισμού.

Στο στάδιο αυτό της Εκτίμησης Αντικτύπου ο υπεύθυνος επεξεργασίας θα πρέπει να αναγνωρίσει και να καταγράψει το σύνολο των κινδύνων που ενέχει η σχεδιαζόμενη επεξεργασία δεδομένων προσωπικού χαρακτήρα τόσο για τον ίδιο τον οργανισμό όσο και για τα υποκείμενα των δεδομένων.

Για κάθε έναν από τους αναγνωρισμένους κινδύνους ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί στις ακόλουθες ενέργειες προκειμένου να αξιολογήσει το επίπεδο σοβαρότητας κάθε κινδύνου και εν συνεχεία να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αντιμετώπιση των κινδύνων αυτών.

- Προσδιορισμός των πηγών των κινδύνων
- Προσδιορισμός των απειλών
- Προσδιορισμός των επιπτώσεων
- Υπολογισμός επιπέδου κινδύνου

Ο στόχος του υπεύθυνου επεξεργασίας είναι μετά το πέρας του σταδίου αυτού να έχει αποκτήσει μια σαφή και τεκμηριωμένη εικόνα των αιτιών και των συνεπειών των ενδεχόμενων κινδύνων



Οι βασικοί κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που ενέχει η επεξεργασία των δεδομένων προσωπικού χαρακτήρα παρουσιάζονται στον ακόλουθο πίνακα

Κίνδυνος	Περιγραφή
Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα προσωπικού χαρακτήρα – Απώλεια Εμπιστευτικότητας	Αποκάλυψη των δεδομένων σε οντότητες με μη εξουσιοδοτημένη πρόσβαση σε αυτά χωρίς να πραγματοποιείται περαιτέρω επεξεργασία. Κοινοποίηση των δεδομένων πέρα από τον έλεγχο και χωρίς τη συγκατάθεση ή ακόμα και τη γνώση του υποκειμένου σε άτομα χωρίς δικαίωμα πρόσβασης σε αυτά Μη επιθυμητή διάδοση φωτογραφίας στο Διαδίκτυο Χρήση των δεδομένων για σκοπούς μη συμβατούς με τους σχεδιαζόμενους αρχικούς σκοπούς και σε ένα μη νόμιμο πλαίσιο για διαφημιστικούς σκοπούς για επιθέσεις κλοπής ταυτότητας (identity theft) Συσχέτιση των δεδομένων με άλλα δεδομένα του υποκειμένου με σκοπό την περαιτέρω ταυτοποίηση του.
Μη εξουσιοδοτημένη τροποποίηση δεδομένων προσωπικού χαρακτήρα - Απώλεια Ακεραιότητας	Τα δεδομένα τροποποιούνται σε έγκυρα ή μη έγκυρα δεδομένα. Η χρήση των δεδομένων αυτών δεν πραγματοποιείται με τον ενδεδειγμένο τρόπο γεγονός το οποίο μπορεί να προκαλέσει σφάλματα, δυσλειτουργίες ή άρνηση πρόσβασης σε μια παρεχόμενη και προσδοκώμενη υπηρεσία. Τροποποίηση των δεδομένων σε άλλα έγκυρα δεδομένα γεγονός που προκαλεί τη διακοπή ή δυσλειτουργία των πράξεων επεξεργασίας. Συσχέτιση μεταξύ της ταυτότητας των υποκειμένων με βιομετρικά δεδομένα άλλων ατόμων
Απώλεια διαθεσιμότητας των δεδομένων	Απώλεια δεδομένων τα οποία είναι απαραίτητα για την ενδεδειγμένη και προσδοκώμενη τέλεση των πράξεων επεξεργασίας Ορισμένες αλλεργίες δεν αναφέρονται πλέον σε ιατρικό φάκελο ενός ασθενή, Ορισμένες πληροφορίες που αφορούν φορολογικά στοιχεία δεν είναι πλέον διαθέσιμες και έτσι δεν μπορεί να υπολογιστεί το ποσό πληρωμής.
Αποτυχία συμμόρφωσης με τις νομικές απαιτήσεις του Κανονισμού	Η ικανοποίηση των νομικών απαιτήσεων τις οποίες θεσπίζει ο Κανονισμός είναι μη διαπραγματεύσιμη.

Πίνακας 7 - Παραδείγματα Κινδύνων

Στο στάδιο αυτό ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί στην αναλυτική καταγραφή των κινδύνων που ενέχει η συγκεκριμένη διαδικασία επεξεργασίας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων

Κίνδυνος	Περιγραφή	Πηγή Εμφάνισης

Στη συνέχεια ο υπεύθυνος επεξεργασίας πρέπει να αναγνωρίσει και να καταγράψει τις πηγές οι οποίες ενδέχεται να προκαλέσουν την εμφάνιση ενός κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Προκειμένου να το πράξει αυτό θα πρέπει να είναι σε θέση να απαντήσει στην ερώτηση : "*Ποιος ή τι θα μπορούσε να επηρεάσει το συγκεκριμένο πλαίσιο επεξεργασίας δεδομένων προσωπικού χαρακτήρα υπό εξέταση και να οδηγήσει στην εμφάνιση ενός κινδύνου*"

Κατηγορίες Πηγών Κινδύνων	Παραδείγματα	Τύπος Ενέργειας	Αιτία Ή Κίνητρο
Ανθρώπινος Παράγοντας στο Εσωτερικό του Οργανισμού	Εργαζόμενοι Διαχειριστές Συστημάτων Εκπαιδευόμενοι Διοικητικά Στελέχη	Σκόπιμη	Σκόπιμη Ενέργεια Οικονομικό Κίνητρο Εκδίκηση Προσωπικό όφελος Κοινωνικοί Παράγοντες
		Μη σκόπιμη	Μη Σκόπιμη Ενέργεια Απροσεξία Λάθος χρήσης Έλλειψη κινήτρου Μη ενδεδειγμένη Εκπαίδευση Μη σωστή κατανόηση συστήματος

Κατηγορίες Πηγών Κινδύνων	Παραδείγματα	Τύπος Ενέργειας	Αιτία Ή Κίνητρο
Ανθρώπινος Παράγοντας στο Εξωτερικό του Οργανισμού	Αποδέκτες των προσωπικών δεδομένων Εξουσιοδοτημένοι συνεργάτες	Σκόπιμη	
	Πάροχοι Υπηρεσιών Επισκέπτες Τέως Υπάλληλοι Πελάτες Προσωπικό Συντήρησης Ανταγωνιστές Επισκέπτες Κυβερνοεγληματίες Τρομοκράτες	Μη σκόπιμη	
Μη ανθρώπινος Παράγοντας	Κακόβουλο λογισμικό Διαβρωτικά ή εκρηκτικά υλικά Φυσικές καταστροφές Υποδομές Υλικό Μηχανήματα		

Πίνακας 8 - Πηγές Κινδύνων

4.2.2 Προσδιορισμός των απειλών

Ως **απειλή** ορίζεται η δυνητική αιτία πρόκλησης ενός περιστατικού παραβίασης των δεδομένων προσωπικού χαρακτήρα που μπορεί να προκαλέσει αρνητικές επιπτώσεις για τα υποκείμενα των δεδομένων.

Ως **ευπάθεια** ορίζεται η αδυναμία ενός υποστηρικτικού για τα δεδομένα προσωπικού χαρακτήρα αγαθού ή ομάδας αγαθών που δύναται να την εκμεταλλευτούν μια ή περισσότερες απειλές.

Φυσικές Απειλές	Απειλές Τεχνικής Φύσης	Ανθρώπινες Απειλές
Φωτιά Πλημμύρα Σεισμός Φυσικά Φαινόμενα	Διακοπή Ηλεκτροδότησης Αστοχία λογισμικού συστήματος και εφαρμογών Αστοχία Δικτύου Βλάβη εξυπηρετητή Βλάβη συσκευής Δικτύου	**Σκόπιμες** ○ Πλαστοπροσωπία από εσωτερικούς ή εξωτερικούς χρήστες ή από παρόχους υπηρεσιών ○ Μη εξουσιοδοτημένη χρήση εφαρμογής ○ Μη εξουσιοδοτημένη αποκάλυψη ή τροποποίηση δεδομένων ○ Φιλτράρισμα επικοινωνιών ○ Παρεμβολές στις επικοινωνίες ○ Κλοπή Υλικού ή λογισμικού ○ Εισαγωγή κακόβουλου λογισμικού ○ Ηθελημένη πρόκληση βλάβης-βανδαλισμός **Μη σκόπιμες ή τυχαίες** ○ Εσφαλμένη διαγραφή ή αποκάλυψη δεδομένων ○ Λανθασμένη δρομολόγηση πακέτων ○ Σφάλμα συντήρησης υλικού ή λογισμικού ○ Εισαγωγή κακόβουλου λογισμικού

Πίνακας 9 - Κατηγορίες και παραδείγματα απειλών

Μια απειλή μπορεί να πραγματοποιηθεί μόνο εφόσον ένα αγαθό έχει ευπάθειες σε αυτήν.

Ο παρακάτω πίνακας παραθέτει τις κατηγορίες των ευπαθειών και ορισμένα χαρακτηριστικά παραδείγματα αυτών.

Κατηγορίες Ευπαθειών	Παραδείγματα
Ευπάθειες Υλικού	Έλλειψη σωστών πρακτικών απόσυρσης υλικού Τήρηση υλικού σε μη εγκεκριμένες περιβαντολλογικές συνθήκες (θερμοκρασία, σκόνη)
Ευπάθειες Λογισμικού	Παράλειψη αποσύνδεσης χρηστών Έλλειψη τεκμηρίωσης των εφαρμογών
Ευπάθειες Δικτύου	Μη κρυπτογραφημένη μετάδοση εμπιστευτικών δεδομένων Χρήση μη προστατευόμενων δημόσιων δικτύων
Ευπάθειες Προσωπικού	Έλλειψη δράσεων ενημέρωσης και εκπαίδευσης για θέματα προστασίας Δεδομένων προσωπικού χαρακτήρα Άγνοια της Νομοθεσίας Έλλειψη διαδικασιών ασφάλειας
Ευπάθειες Διαχειριστικής Φύσης	Έλλειψη πολιτικών ασφαλείας και προστασίας δεδομένων Έλλειψη τεκμηριωμένων διαδικασιών αναφοράς και διαχείρισης περιστατικών παραβίασης των δεδομένων προσωπικού χαρακτήρα Έλλειψη τεκμηριωμένων διαδικασιών ελέγχου πρόσβασης
Ευπάθειες Εγκαταστάσεων	Τοποθεσία σε περιοχές συχνών φαινομένων όπως πλημμύρας ή σε σεισμογενείς περιοχές Τοποθεσία σε περιοχές όπου το δίκτυο ηλεκτροδότησης είναι ασταθές

Πίνακας 10 - Κατηγορίες και Παραδείγματα Ευπαθειών

Στο βήμα αυτό ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί στις ακόλουθες ενέργειες στο πλαίσιο της διεξαγωγής μιας Εκτίμησης Αντικτύπου :

- Αναγνώριση και καταγραφή των πιθανών απειλών για κάθε συγκεκριμένη πράξη επεξεργασίας
- Για κάθε αναγνωρισμένη απειλή:
  - Συσχέτιση της απειλής με τη πηγή που μπορεί να την προκαλέσει
  - Συσχέτιση της απειλής με τα υποστηρικτικά αγαθά που σχετίζονται με την

εν λόγω απειλή

- Συσχέτιση της απειλής με την ευπάθεια των υποστηρικτικών αγαθών που σχετίζονται με την εν λόγω απειλή

- Καταγραφή των υλοποιημένων ή σχεδιαζόμενων μέτρων προστασίας που σχετίζονται με την απειλή αυτή
- Υπολογισμός της πιθανότητας εμφάνισης της απειλής, ανάλογα με το επίπεδο των ευπαθειών των υποστηρικτικών αγαθών, το είδος των πηγών κινδύνων και τα μέτρα προστασίας που έχουν υλοποιηθεί.

Κίνδυνος	Απειλή	Πηγή κινδύνου	Υποστηρικτικό Αγαθό	Ευπάθεια που εκμεταλλεύεται	Μέτρο Προστασίας (εάν υπάρχει)	Επίπεδο Πιθανότητας Εμφάνισης Απειλής
						• Χαμηλό • Μεσαίο • Σημαντικό • Υψηλό

4.2.3 Υπολογισμός Πιθανότητας Εμφάνισης μιας Απειλής

Η πιθανότητα εμφάνισης μιας απειλής εκφράζει το πόσο εφικτό είναι να λάβει χώρα μια απειλή και υπολογίζεται συναρτήσει του επιπέδου ευπάθειας που παρουσιάζει ένα υποστηρικτικό για τα δεδομένα αγαθό και τα υφιστάμενα ή σχεδιαζόμενα τεχνικά και οργανωτικά μέτρα ασφαλείας για την αντιμετώπιση της.

Η παρακάτω κλίμακα δύναται να χρησιμοποιηθεί για τον καθορισμό του επιπέδου – πιθανότητα εμφάνισης μια συγκεκριμένης απειλής.

Επίπεδο Πιθανότητας	Επεξήγηση	Παράδειγμα
Χαμηλό Επίπεδο – 1--	Δεν φαίνεται δυνατό το ενδεχόμενο μια συγκεκριμένη απειλή να εκμεταλλευτεί μια ή περισσότερες ευπάθειες .	• Κλοπή εγγράφων τα οποία είναι αποθηκευμένα σε ένα δωμάτιο που προστατεύεται από μηχανισμό πρόσβασης που βασίζεται στην χρήση βιομετρικού χαρακτηριστικού σε συνδυασμό με κωδικό πρόσβασης. • Παραβίαση του συστήματος από ένα άτομο που ενεργεί χωρίς κακόβουλη πρόθεση και έχει περιορισμένα δικαιώματα πρόσβασης
Μεσαίο Επίπεδο –2--	Φαίνεται δύσκολο το ενδεχόμενο μια συγκεκριμένη απειλή να εκμεταλλευτεί μια ή περισσότερες ευπάθειες .	• Κλοπή εγγράφων τα οποία είναι αποθηκευμένα σε ένα δωμάτιο που προστατεύεται από μηχανισμό πρόσβασης που βασίζεται σε κωδικό. • Παραβίαση του συστήματος από ένα άτομο που ενεργεί με κακόβουλη πρόθεση και έχει περιορισμένα δικαιώματα πρόσβασης
Σημαντικό Επίπεδο –3--	Φαίνεται πιθανό το ενδεχόμενο μια συγκεκριμένη απειλή να εκμεταλλευτεί μια ή περισσότερες ευπάθειες. .	• Κλοπή εγγράφων που είναι αποθηκευμένα σε ένα δωμάτιο στο οποίο δεν επιτρέπεται η πρόσβαση αν δεν έχει προηγηθεί η ταυτοποίηση από τον υπάλληλο υποδοχής • Παραβίαση του συστήματος από ένα άτομο που ενεργεί χωρίς κακόβουλη πρόθεση αλλά δικαιώματα διαχειριστή

Επίπεδο Πιθανότητας	Επεξήγηση	Παράδειγμα
Υψηλό Επίπεδο –4--	Φαίνεται εξαιρετικά πιθανό το ενδεχόμενο μια συγκεκριμένη απειλή να εκμεταλλευτεί μια η περισσότερες ευπάθειες	• Κλοπή εγγράφων που είναι αποθηκευμένα σε ένα δωμάτιο στο οποίο έχει πρόσβαση ο οποιοσδήποτε. • Παραβίαση του συστήματος από ένα άτομο που ενεργεί με κακόβουλη πρόθεση και έχει δικαιώματα διαχειριστή

Πίνακας 11 - Επίπεδο Πιθανότητας

4.2.4 Υπολογισμός της σοβαρότητας των επιπτώσεων μιας απειλής

Ως **Επίπτωση(impact)** ορίζεται μια δυσμενής κατάσταση είτε υλικής, είτε ψυχικής φύσης στην οποία ενδέχεται να περιέλθει το υποκείμενο των δεδομένων λόγω της εκδήλωσης ενός περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα τα οποία τυγχάνουν επεξεργασίας από έναν οργανισμό.

Η **σοβαρότητα** αντιπροσωπεύει το μέγεθος ενός κινδύνου. Εκτιμάται κατ' αρχήν ως προς την έκταση των πιθανών επιπτώσεων στα υποκείμενα των δεδομένων λαμβάνοντας υπόψη τους υφιστάμενους, προγραμματισμένους ή συμπληρωματικούς μηχανισμούς ασφαλείας. Επίσης, θα πρέπει κατά τον υπολογισμό του επιπέδου της επίπτωσης να λαμβάνεται υπόψη το είδος των δεδομένων για τα οποία έχει αναγνωριστεί κάποιος κίνδυνος

Στο στάδιο αυτό ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί:

- Στην καταγραφή των επιπτώσεων για κάθε αναγνωρισμένη απειλή.
- Στον υπολογισμό του επιπέδου της σοβαρότητας κάθε επίπτωσης.

Κίνδυνος	Είδος δεδομένων	Επίπτωση	Επίπεδο Σοβαρότητας Επίπτωσης

Οντότητα η οποία θα επηρεαστεί	Είδος Επίπτωσης
Υπεύθυνος επεξεργασίας / Εκτελών την επεξεργασία	• Απώλεια φήμης • Απώλεια εμπορικής αξίας • Άμεση οικονομική ζημία (πχ επιβολή προστίμου)
Υποκείμενο των δεδομένων	• Ηθική βλάβη • Οικονομική ζημία • Καταπάτηση προσωπικών δικαιωμάτων και ελευθεριών • Επιπτώσεις στην υγεία • Προσβολή • Ενόχληση • Διάκριση • Άρνηση παροχής υπηρεσίας • Κατάχρηση ή υποκλοπή ταυτότητας

Πίνακας 12 - Παραδείγματα Επιπτώσεων

Στον παρακάτω πίνακα παρουσιάζονται τα επίπεδα των επιπτώσεων που ενδέχεται να επιφέρει η εκδήλωση ενός κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων

Επίπεδο Σοβαρότητας Επίπτωσης	Επεξήγηση	Παράδειγμα
Χαμηλό – 1--	Το υποκείμενο των δεδομένων είτε δεν θα επηρεαστεί είτε ενδέχεται να συναντήσει ορισμένες συνέπειες, τις οποίες δύναται να ξεπεράσει χωρίς ιδιαίτερο πρόβλημα	• Λήψη ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (π.χ.spams) • Επαναχρησιμοποίηση δεδομένων που δημοσιεύθηκαν σε ιστοσελίδες για σκοπούς στοχευμένης διαφήμισης (δεδομένα σε μέσα κοινωνικής δικτύωσης) • Αίσθημα εισβολής στην ιδιωτική ζωή χωρίς πραγματική ή αντικειμενική συνέπεια (π.χ. εμπορική χρήση δεδομένων) • Απώλεια χρόνου κατά την διαδικασία επιβολής ενός αιτήματος .
Μεσαίο –2--	Το υποκείμενο των δεδομένων ενδέχεται να επηρεαστεί σε σημαντικό βαθμό. Προκειμένου να είναι σε θέση να ξεπεράσει τις συνέπειες πρέπει να αντιμετωπίσει ορισμένες δυσκολίες.	• Στοχευμένη ηλεκτρονική διαφήμιση που αφορά δεδομένα τα οποία το υποκείμενο ήθελε να παραμείνουν εμπιστευτικά (π.χ. διαφήμιση για προϊόντα εγκυμοσύνης, φάρμακα για θεραπεία συγκεκριμένων ασθενειών) • Μη αναμενόμενη οικονομική ζημία ➢ Λανθασμένη επιβολή προστίμων ➢ Επιπλέον χρεώσεις από λανθασμένη επεξεργασία δεδομένων

Επίπεδο Σοβαρότητας Επίπτωσης	Επεξήγηση	Παράδειγμα
		• Αποκλεισμός της πρόσβασης σε ήδη υπάρχον λογαριασμό για συγκεκριμένη ηλεκτρονική υπηρεσία. • Εκφοβισμός μέσω των κοινωνικών δικτύων • Συναισθηματική διαταραχή λόγω διάδοσης προσωπικών δεδομένων και αμαύρωσης της εικόνας του υποκειμένου
Σημαντικό –3--	Το υποκείμενο των δεδομένων ενδέχεται να επηρεαστεί σε πολύ σημαντικό βαθμό. Προκειμένου να είναι σε θέσει να ξεπεράσει τις συνέπειες πρέπει να αντιμετωπίσει σημαντικές δυσκολίες.	• Πρόκληση σοβαρής συνέπειας στην υγεία η οποία συνεπάγεται μακροπρόθεσμη βλάβη στο υποκείμενο των δεδομένων ➢ επιδείνωση της κατάστασης υγείας λόγω ακατάλληλης ιατρικής φροντίδας. • Οικονομική ζημία ως αποτέλεσμα απάτης ➢ Μέσω της χρήσης κοινωνικής μηχανικής και παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου (social engineering and phishing e-mails)

Επίπεδο Σοβαρότητας Επίπτωσης	Επεξήγηση	Παράδειγμα
		• Απώλεια δικαιώματος χρήσης μιας υπηρεσίας ή μιας προσφοράς ή απόρριψη αίτησης λόγω εσφαλμένων δεδομένων ή απώλεια δεδομένων ➢ Απόρριψη αίτησης για δάνειο ➢ Απόρριψη αιτήματος υποτροφίας ➢ Μη καταβολή επιδόματος ➢ Απαγόρευση συμμετοχής σε εξετάσεις • Απώλεια εργασίας • Αίσθημα παραβίασης των θεμελιωδών δικαιωμάτων ➢ Διάκριση ➢ Ελευθερία έκφρασης • Εκβιασμός • Cyberbullying και παρενόχληση
Υψηλό –4--	Το υποκείμενο των δεδομένων ενδέχεται να αντιμετωπίσει σημαντικές, ή ακόμα και μη αναστρέψιμες, συνέπειες, τις οποίες μπορεί να μην είναι σε θέση να ξεπεράσει.	• Πρόκληση μακροπρόθεσμης ή μόνιμης βλάβης στην υγεία • Θάνατος • Απώλεια πρόσβασης σε συστήματα κρίσιμων υποδομών ➢ Υγεία ➢ Μεταφορές ➢ Ενέργεια

Επίπεδο Σοβαρότητας Επίπτωσης	Επεξήγηση	Παράδειγμα

Πίνακας 12 - Επίπεδο Επιπτώσεων

4.2.5 Υπολογισμός Σοβαρότητας Κινδύνου

Στο στάδιο αυτό ο υπεύθυνος επεξεργασίας θα πρέπει να:

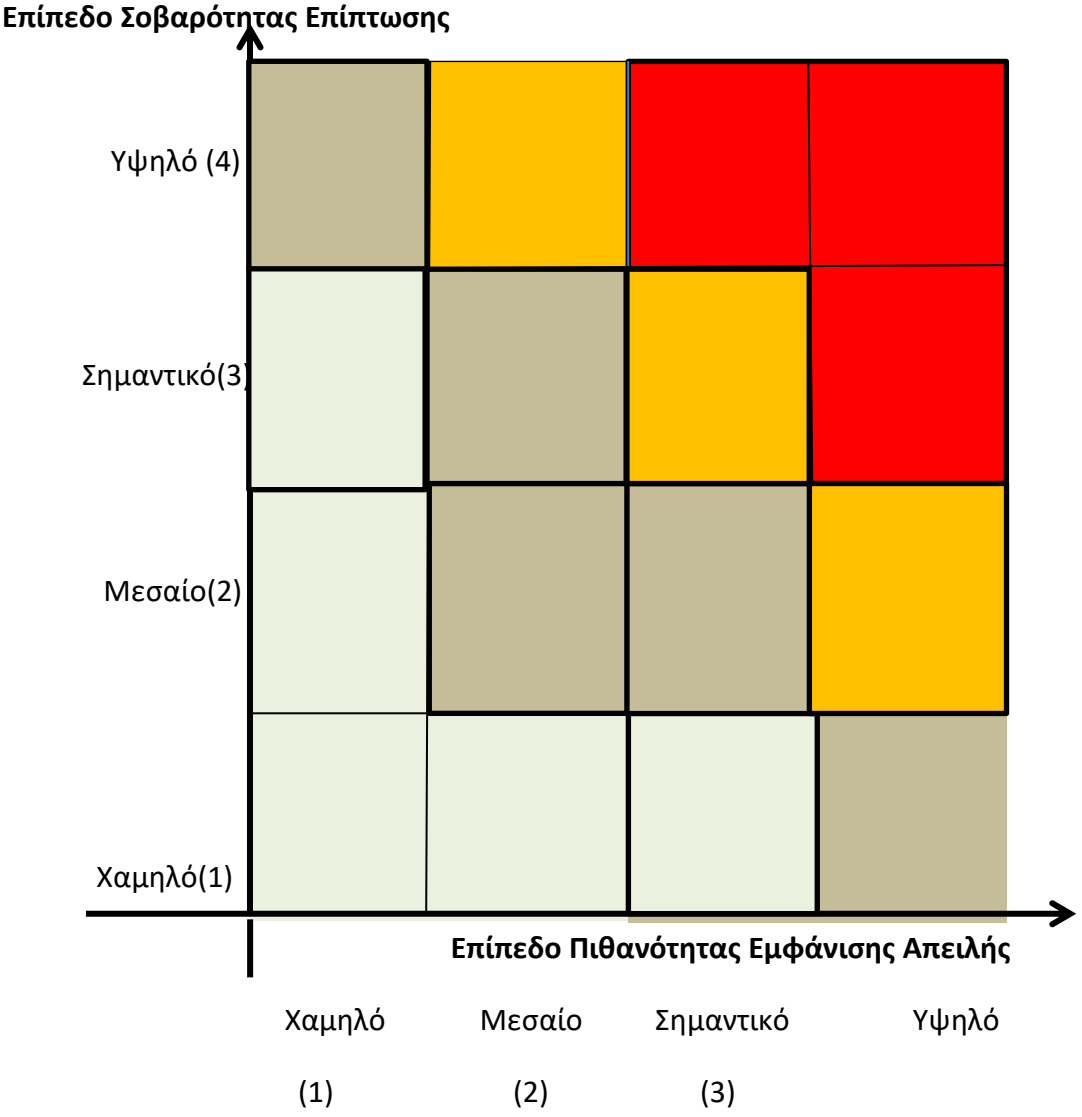
- προβεί στον καθορισμό του επιπέδου σοβαρότητας του κινδύνου για κάθε αναγνωρισμένο κίνδυνο. Η διαδικασία αυτή πραγματοποιείται συνυπολογίζοντας την πιθανότητα εμφάνισης και του επιπέδου σοβαρότητας των επιπτώσεων ενός κινδύνου.
- δημιουργήσει έναν πλήρη κατάλογο των κινδύνων που ενέχει η πράξη επεξεργασίας που σχεδιάζει και να κατατάξει τους κίνδυνους ανάλογα με το επίπεδο σοβαρότητας του κάθε κινδύνου.

Στο βήμα αυτό της Εκτίμησης Αντικτύπου ο υπεύθυνος επεξεργασίας αφού πρώτα έχει καθορίσει το επίπεδο της πιθανότητας εμφάνισης αλλά και το επίπεδο σοβαρότητας των επιπτώσεων όπως είδαμε στα προηγούμενα βήματα θα πρέπει να υπολογίσει το αντίστοιχο επίπεδο σοβαρότητας του κινδύνου.

Στο πλαίσιο της παρούσας εργασίας ακολουθείται το μοντέλο το οποίο προτείνει η Γαλλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (CNIL) όπως έγινε για τον καθορισμό των επιπέδων εμφάνισης μιας απειλής και της σοβαρότητας των επιπτώσεων εμφάνισης της συγκεκριμένης απειλής .

Έτσι λοιπόν, όπως παρουσιάζεται στον ακόλουθο πίνακα, ορίζονται 4 επίπεδα σοβαρότητας του κινδύνου

Κίνδυνος	Επίπεδο Πιθανότητας Εμφάνισης	Επίπεδο Σοβαρότητας Επίπτωσης	Επίπεδο Κινδύνου	Αποδοχή του Κινδύνου


Επίπεδο Σοβαρότητας Επίπτωσης
Υψηλό (4)
Σημαντικό(3)
Μεσαίο(2)
Χαμηλό(1)
Επίπεδο Πιθανότητας Εμφάνισης Απειλής
Χαμηλό
Μεσαίο
Σημαντικό
Υψηλό
(1)
(2)
(3)

- **Καθορισμός των επιπέδων σοβαρότητας του κινδύνου.**

Επίπεδο Κινδύνου	Περιγραφή	Μέθοδος Διαχείρισης Κινδύνου
Χαμηλό 1-3	Κίνδυνοι με χαμηλό ή μεσαίο επίπεδο πιθανότητας εμφάνισης και χαμηλό ή μεσαίο επίπεδο σοβαρότητας επιπτώσεων	Είναι δυνατή η αποδοχή των κινδύνων αυτών.
Μεσαίο 4-7	Κίνδυνοι με σημαντικό ή υψηλό επίπεδο πιθανότητας εμφάνισης και χαμηλό ή μέτριο επίπεδο σοβαρότητας επιπτώσεων	Οι κίνδυνοι αυτοί θα πρέπει να περιοριστούν σε αποδεκτό επίπεδο με την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων τα οποία να περιορίζουν ιδίως την πιθανότητα εμφάνισης ενός κινδύνου.
Σημαντικό 8- 10	Κίνδυνοι με σημαντικό ή υψηλό επίπεδο σοβαρότητας επιπτώσεων και χαμηλό ή μεσαίο επίπεδο πιθανότητας εμφάνισης.	Οι κίνδυνοι αυτοί θα πρέπει να αποφευχθούν ή να περιοριστούν σε αποδεκτό επίπεδο με την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων τα οποία να περιορίζουν ιδίως την σοβαρότητα των επιπτώσεων.
Υψηλό >10	Κίνδυνοι με σημαντικό ή υψηλό επίπεδο πιθανότητας εμφάνισης και σημαντικό ή υψηλό επίπεδο σοβαρότητας επιπτώσεων	Οι κίνδυνοι αυτοί θα πρέπει να αποφευχθούν ή να περιοριστούν σε αποδεκτό επίπεδο με την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων τα οποία να περιορίζουν εξίσου την πιθανότητα εμφάνισης αλλά και τη σοβαρότητα των επιπτώσεων. Θα πρέπει να ληφθούν: • Μέτρα Πρόληψης: μέτρα τα οποία να αποτρέπουν την εμφάνιση ενός κινδύνου και υλοποιούνται πριν την εμφάνιση ενός κινδύνου.

Επίπεδο Κινδύνου	Περιγραφή	Μέθοδος Διαχείρισης Κινδύνου
		• Μέτρα Αντιμετώπισης:Μέτρα τα οποία να καθορίζουν τις πράξεις κατά την διάρκεια εκδήλωσης ενός περιστατικού • Μέτρα Ανάκαμψης:Μέτρα τα οποία καθορίζουν τις πράξεις μετά την εκδήλωση και αντιμετώπιση ενός περιστατικού και τα οποία τα περιορίζουν τη σοβαρότητα των επιπτώσεων

Πίνακας 13 - Επίπεδα Κινδύνου

4.3 Στάδιο 3: Μέτρα προστασίας

Στο στάδιο αυτό αφού έχουν έχει προηγηθεί η αναγνώριση και η αξιολόγηση των κινδύνων που ενέχει η επεξεργασία για τα υποκείμενα των δεδομένων ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί σε όλες τις απαραίτητες ενέργειες για την αντιμετώπιση των κινδύνων αυτών.

Ο Γενικός Κανονισμός απαιτεί από τους οργανισμούς εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζουν αλλά και να είναι σε θέση να αποδείξουν ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται σύμφωνα με τις απαιτήσεις τις οποίες θέτει ο Κανονισμός αλλά και με απόλυτο σεβασμό στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Στόχος του υπεύθυνου επεξεργασίας κατά την διενέργεια αυτού του σταδίου είναι ο προσδιορισμός, η αναλυτική καταγραφή και η εφαρμογή των τεχνικών και οργανωτικών μέτρων προκειμένου να εξασφαλιστεί η συμμόρφωση του οργανισμού με τις νομικές απαιτήσεις τις οποίες θέτει ο Κανονισμός και η αντιμετώπιση κάθε πιθανού κινδύνου για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Είναι σημαντικό να τονίσουμε ότι στόχος μιας Εκτίμησης Αντικτύπου και γενικότερα της διαδικασίας Διαχείρισης Κινδύνου δεν είναι να εξαλείψει εντελώς τους κινδύνους κάτι το οποίο στο χώρο της ασφάλειας πληροφοριών είναι πρακτικά ανέφικτο.

Ο σκοπός της διαδικασίας είναι να μειώσει τον κίνδυνο σε ένα αποδεκτό επίπεδο, διατηρώντας παράλληλα την ευχρηστία και την λειτουργικότητα του συστήματος.

Όταν ένας οργανισμός αποφασίζει για τα τεχνικά και οργανωτικά μέτρα τα οποία θα πρέπει να λάβει θα πρέπει να εξετάσει κατά πόσον τα μέτρα αυτά για την προστασία των δεδομένων είναι αναλογικά με τους στόχους του οργανισμού.

Τα μέτρα αυτά συνεπώς θα πρέπει να είναι αναλογικά, επαρκή και κατάλληλα σύμφωνα με το πλαίσιο επεξεργασίας το οποίο έχει προσδιοριστεί και καταγραφεί στο αρχικό στάδιο της Εκτίμησης Αντικτύπου.

Τα μέτρα προστασίας μπορεί είτε να δημιουργηθούν από το μηδέν από τον υπεύθυνο επεξεργασίας είτε να υιοθετηθούν καλές πρακτικές και οδηγίες οι οποίες εκδίδονται από αναγνωρισμένους φορείς ή διεθνή πρότυπα αφού πρώτα προσαρμοστούν στις απαιτήσεις κάθε υπεύθυνου επεξεργασίας και εναρμονιστούν με το πλαίσιο της επεξεργασίας.

Επιπλέον, τυχόν συμβάντα τα οποία έχουν ήδη λάβει χώρα , καθώς και τυχόν δυσκολίες στην εφαρμογή ορισμένων μέτρων προστασίας δύναται να χρησιμοποιηθούν για τη βελτίωση της διαδικασίας επιλογής συγκεκριμένων μέτρων προστασίας.

Στο σημείο αυτό θα πρέπει να τονιστεί ότι το συγκεκριμένο στάδιο της Εκτίμησης Αντικτύπου ενδέχεται να αναθεωρηθεί και να επαναληφθεί ορισμένες φορές έως ότου εφαρμοστούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας τα οποία να εξασφαλίζουν τη συμμόρφωση του οργανισμού με τις απαιτήσεις του Κανονισμού.

Σε περίπτωση κατά την οποία στο στάδιο αξιολόγησης της Εκτίμησης Αντικτύπου τεκμηριωθεί ότι ένα μέτρο προστασίας δεν είναι αποτελεσματικό καθώς δεν εξαλείφει έναν συγκεκριμένο κίνδυνο ή δεν τον περιορίζει σε αποδεκτά επίπεδα τότε ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόσει εναλλακτικά μέτρα προστασίας προκειμένου να εξασφαλίσει ένα αποδεκτό επίπεδο ασφάλειας για τον οργανισμό.

Στο στάδιο αυτό η Εκτίμηση Αντικτύπου αποτελείται από 2 επιμέρους ενότητες:

- Την λήψη μέτρων για την ικανοποίηση των νομικών απαιτήσεων τις οποίες θέτει ο Κανονισμός
- Τη λήψη μέτρων για την αντιμετώπιση και διαχείριση των κινδύνων που εντοπίστηκαν στο προηγούμενο στάδιο

και θα πρέπει να περιέχει:

- Μια αναλυτική λίστα με τα μέτρα προστασίας τα οποία έχει επιλέξει ο υπεύθυνος επεξεργασίας να υλοποιήσει.
- Αναλυτική περιγραφή των μέτρων τα οποία επιλέχθηκαν
- Αντιστοίχιση των μέτρων αυτών με τις απαιτήσεις του Κανονισμού τις οποίες καλούνται να ικανοποιήσουν
- Αντιστοίχιση των μέτρων με τους κινδύνους που καλούνται να αντιμετωπίσουν
- Τεκμηρίωση της επιλογής των συγκεκριμένων μέτρων προστασίας.
- Το αποτέλεσμα που είχε η εφαρμογή του συγκεκριμένου μέτρου προστασίας στην αντιμετώπιση του κινδύνου

Στο σημείο αυτό ο υπεύθυνος επεξεργασίας θα πρέπει λαμβάνοντας 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, να εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται η συμμόρφωση με τις παραπάνω απαιτήσεις αλλά και το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων.

Υπάρχουν ποικίλοι τρόποι για τον μετριασμό των κινδύνων, μερικοί από τους οποίους αναφέρονται στον Γενικό Κανονισμό.

Για παράδειγμα, ο Κανονισμός αναφέρεται σε διάφορα μέτρα μετριασμού του κινδύνου, συμπεριλαμβανομένης της κρυπτογράφησης, της ψευδωνυμοποίησης , της ανωνυμοποίησης των δεδομένων προσωπικού χαρακτήρα.

Τα μέτρα ασφαλείας μπορούν να εντάσσονται στις παρακάτω τρεις κύριες κατηγορίες όπως φαίνεται στον παρακάτω πίνακα:

Κατηγορία	Μέτρα Ασφάλειας
Οργανωτικά μέτρα	• Κατάρτιση Πολιτικής Ασφαλείας • Καθορισμός ρόλων και αρμοδιοτήτων στο εσωτερικό του οργανισμού • Κατάρτιση Σχεδίου Αντιμετώπισης Περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα • Κατάρτιση Σχεδίου Ανάκαμψης από Καταστροφή • Ανάπτυξη Συμβάσεων με Τρίτα μέρη με τα οποία υπάρχουν σχέσεις συνεργασίας • Ανάπτυξη διαδικασιών εκπαίδευσης προσωπικού σχετικά με θέματα προστασίας δεδομένων προσωπικού χαρακτήρα αλλά και ασφάλειας πληροφοριακών συστημάτων εν γένει. • Ανάπτυξη διαδικασιών εσωτερικού ελέγχου των διεργασιών που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα
Τεχνικά μέτρα	• Ανωνυμοποίηση των δεδομένων • Κρυπτογράφηση των δεδομένων • Ψευδωνυμοποίηση των δεδομένων • Ανιχνευσιμότητα των δεδομένων • Δημιουργία αντιγράφων ασφαλείας • Λογικός έλεγχος πρόσβασης • Έλεγχος ακεραιότητας των δεδομένων • Τήρηση Αρχείων καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας • Χρήση έμπιστων και ασφαλών πρωτοκόλλων επικοινωνίας
Μέτρα φυσικής Ασφάλειας	• Έλεγχος φυσικής πρόσβασης • Προστασία από φυσικές καταστροφές • Ασφάλεια γραφείων, χώρων και εγκαταστάσεων

Πίνακας 14 - Ενδεικτικά Μέτρα Ασφάλειας

4.3.1 Ικανοποίηση των νομικών απαιτήσεων

Στην ενότητα αυτή ο υπεύθυνος επεξεργασίας θα πρέπει να καθορίσει και να καταγράψει τα μέτρα και τις διαδικασίες που έχει υλοποιήσει ή σχεδιάζει να υλοποιήσει για την ικανοποίηση των νομικών απαιτήσεων που ορίζει ρητά ο Κανονισμός.

Η συμμόρφωση με τις απαιτήσεις αυτές είναι αδιαπραγμάτευτη και συνεπώς ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί σε όλες τις απαραίτητες ενέργειες για την ικανοποίησή τους. Αναλυτικά οι απαιτήσεις αυτές καταγράφονται στον παρακάτω πίνακα

Νομική Απαίτηση	Μέτρο - Διαδικασία	Περιγραφή Μέτρου-Διαδικασίας
Περιορισμός του Σκοπού της Επεξεργασίας		
Ελαχιστοποίηση των δεδομένων		
Ακρίβεια των δεδομένων		
Περίοδος κράτησης των δεδομένων		
Νομιμότητα, αντικειμενικότητα και διαφάνεια		
Εμπιστευτικότητα των δεδομένων		
Ακεραιότητα		
Διαθεσιμότητα		
Λογοδοσία		
Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού		
Αρχεία των δραστηριοτήτων επεξεργασίας		
Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα		
Ορισμός του υπευθύνου προστασίας		
Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς		

Νομική Απαίτηση	Μέτρο - Διαδικασία	Περιγραφή Μέτρου-Διαδικασίας
οργανισμούς		
Δικαίωμα ενημέρωσης		
Δικαίωμα εναντίωσης		
Δικαίωμα πρόσβασης		
Δικαίωμα διόρθωσης		
Δικαίωμα διαγραφής		
Δικαίωμα φορητότητας		
Δικαίωμα περιορισμού της επεξεργασίας		

Πίνακας 15 - Αντιστοίχιση μέτρων

4.3.2 Διαχείριση Κινδύνου

Αφού έχουν προσδιοριστεί και αξιολογηθεί οι πιθανοί κίνδυνοι ο υπεύθυνος επεξεργασίας θα πρέπει να καθορίσει τον τρόπο διαχείρισης των κινδύνων αυτών. Πρέπει επίσης, να περιγράψει τον τρόπο με τον οποίο επιτεύχθηκε η συμμόρφωση με τις απαιτήσεις του Κανονισμού, όπως ορίζονται, ή να παρουσιάσει μια αιτιολόγηση εάν δεν έχει κατορθώσει να εφαρμόσει τα κατάλληλα μέτρα για τον σκοπό αυτό.

Όταν έχει εντοπιστεί ένας κίνδυνος στόχος του οργανισμού είναι η μείωση του επιπέδου του σε αποδεκτά πλαίσια με τη εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων ασφάλειας.

Τα μέτρα ασφαλείας μπορούν να μειώσουν το επίπεδο του κινδύνου είτε μειώνοντας τη πιθανότητα η απειλή να εκμεταλλευτεί επιτυχώς μια ευπάθεια, είτε μειώνοντας την επίπτωση για τα υποκείμενα των δεδομένων μιας επιτυχούς απειλής.

Οι πιθανές επιλογές που μπορούν να ληφθούν για τη διαχείριση αυτών των κινδύνων είναι οι ακόλουθες:

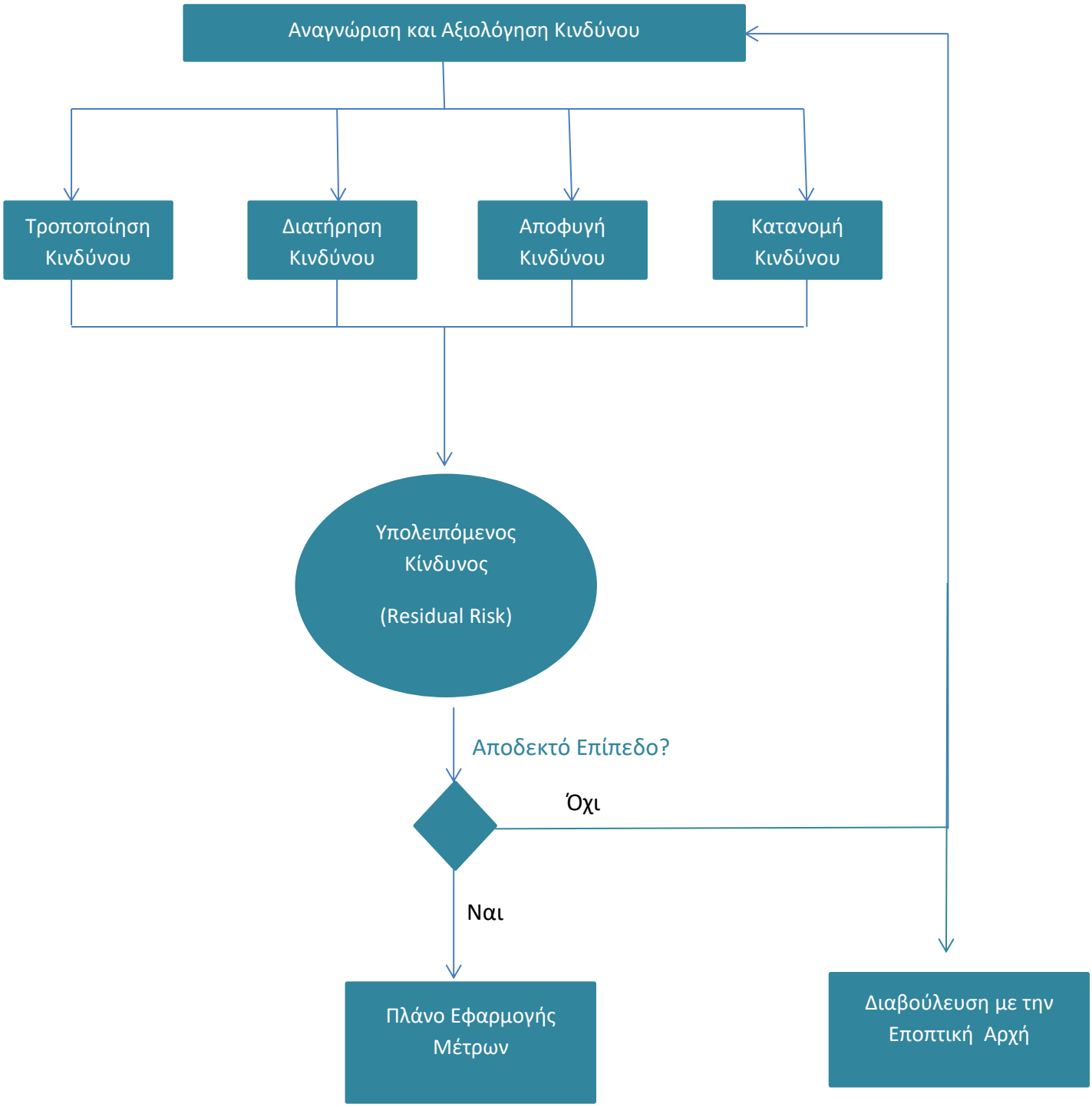
- **Τροποποίηση Κινδύνου**: Ο υπεύθυνος επεξεργασίας διαχειρίζεται τον κίνδυνο με τον προσδιορισμό και την εφαρμογή πρόσθετων ή εναλλακτικών τεχνικών και οργανωτικών μέτρων προς εκείνα που έχουν ήδη εφαρμοστεί ή σχεδιαστεί , μειώνοντας έτσι τον κίνδυνο σε αποδεκτά επίπεδα.
- **Διατήρηση Κινδύνου:** Ο υπεύθυνος επεξεργασίας αποδέχεται τον κίνδυνο ως έχει, εάν πληροί τα κριτήρια αποδοχής, χωρίς περαιτέρω ενέργειες.
- **Αποφυγή Κινδύνου:** Ο υπεύθυνος επεξεργασίας αποφασίζει να μην θέσει σε εφαρμογή την διαδικασία επεξεργασίας που ενέχει ένα συγκεκριμένο κίνδυνο.

- **Κατανομή κινδύνου**: Ο κίνδυνος μοιράζεται με ένα τρίτο μέρος, το οποίο μπορεί να διαχειριστεί αποτελεσματικότερα τον εντοπισμένο κίνδυνο και να μειώσει έτσι τον κίνδυνο σε αποδεκτά επίπεδα.

Κίνδυνος	Διαχείριση Κινδύνου			
	Τροποποίηση	Διατήρηση	Αποφυγή	Κατανομή

4.3.3 Σχέδιο Διαχείρισης Κινδύνου

Στο στάδιο αυτό ο υπεύθυνος επεξεργασίας για κάθε αναγνωρισμένο κίνδυνο θα πρέπει να επιλέξει και καταγράψει τον τρόπο με τον οποίο θα διαχειριστεί τον κίνδυνο επιλέγοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα. Το παρακάτω σχήμα περιγράφει την διαδικασία διαχείρισης των κινδύνων.


Αναγνώριση και Αξιολόγηση Κινδύνου
Τροποποίηση Κινδύνου
Διατήρηση Κινδύνου
Αποφυγή Κινδύνου
Κατανομή Κινδύνου
Υπολειπόμενος Κίνδυνος
(Residual Risk)
Αποδεκτό Επίπεδο?
Όχι
Ναι
Πλάνο Εφαρμογής Μέτρων
Διαβούλευση με την Εποπτική Αρχή

4.4 Στάδιο 4: Επικύρωση των αποτελεσμάτων

Το στάδιο αυτό της Εκτίμησης Αντικτύπου θα πρέπει να συνοψίζει τα γενικά αποτελέσματα και να περιγράφει τα συμπεράσματα της διαδικασίας, συμπεριλαμβανομένου του κατά πόσον τα μέτρα τα οποία έχουν υλοποιηθεί ή πρόκειται να υλοποιηθούν είναι επαρκή για την προστασία των δεδομένων προσωπικού χαρακτήρα τα οποία υφίστανται επεξεργασία.

Επίσης, πρέπει να ληφθεί η απόφαση για την τελική επιβεβαίωση των αποτελεσμάτων και την επικύρωση των διαδικασιών οι οποίες έλαβαν χώρα στα προηγούμενα στάδια.

Σε περίπτωση κατά την οποία κριθεί ότι τα μέτρα είναι επαρκή και περιορίζουν τους αναγνωρισμένους κινδύνους σε αποδεκτά επίπεδα τότε η Εκτίμηση Αντικτύπου ολοκληρώνεται.

Σε αντίθετη περίπτωση η Εκτίμηση θα πρέπει να αναθεωρηθεί και να υιοθετηθούν εναλλακτικά μέτρα για τον περιορισμό συγκεκριμένων κινδύνων.

4.4.1 Αξιολόγηση των αποτελεσμάτων

Στο στάδιο αυτό της Εκτίμησης Αντικτύπου ο υπεύθυνος επεξεργασίας θα πρέπει να προβεί σε μια αναλυτική αξιολόγηση των υφιστάμενων και των σχεδιαζόμενων τεχνικών και οργανωτικών μέτρων ασφαλείας όσον αφορά το κατά πόσο η εφαρμογή των συγκεκριμένων μέτρων έχει περιορίσει την εμφάνιση των κινδύνων σε αποδεκτά επίπεδα.

Η Εκτίμηση Αντικτύπου θα πρέπει να περιέχει:

- Έναν κατάλογο των αναγνωρισμένων κινδύνων που ενέχει η επεξεργασία
- Έναν κατάλογο με τα μέτρα τα οποία έχουν εφαρμοστεί ή πρόκειται να εφαρμοστούν για κάθε συγκεκριμένο κίνδυνο
- Μια αξιολόγηση για το αν τα μέτρα αυτά είναι επαρκή για τον περιορισμό των κινδύνων σε αποδεκτά επίπεδα

Κίνδυνος – Νομική Απαίτηση	Μέτρο Προστασίας	Αποτέλεσμα Διαχείρισης Κινδύνου	Επίπεδο Σοβαρότητας	Αξιολόγηση
		• Εξάλειψη Κινδύνου • Περιορισμός Κινδύνου • Αποφυγή Κινδύνου • Μεταβίβαση Κινδύνου	• Αποδεκτό • Μη αποδεκτό	• Επικύρωση • Αναθεώρηση

4.4.1.1 Η Εκτίμηση Αντικτύπου δεν γίνεται αποδεκτή

Σε περίπτωση κατά την οποία κρίνεται ότι ορισμένοι κίνδυνοι δεν έχουν αντιμετωπιστεί καταλλήλως και ο υπολειπόμενος κίνδυνος είναι υψηλός τότε ο υπεύθυνος επεξεργασίας οφείλει είτε να επανεξετάσει τα προηγούμενα βήματα της Εκτίμησης Αντικτύπου και συγκεκριμένα να αναζητήσει εναλλακτικά μέτρα για τον περιορισμό των κινδύνων αυτών σε αποδεκτά επίπεδα είτε να προχωρήσει σε Διαβούλευση με την Αρμόδια Εποπτική Αρχή.

Συνεπώς, ο υπεύθυνος επεξεργασίας θα πρέπει στο στάδιο αυτό να προβεί σε :

- Καταγραφή των κινδύνων για τους οποίους το επίπεδο ασφάλειας κρίνεται ως μη αποδεκτό
- Επανάληψη των προηγούμενων σταδίων της Εκτίμησης Αντικτύπου με στόχο την εύρεση μέτρων και πρακτικών για την αντιμετώπιση των κινδύνων αυτών
- Διαβούλευση με την αρμόδια Εποπτική Αρχή σε περιπτώσεις κατά τις οποίες ο υπεύθυνος της επεξεργασίας δεν είναι σε θέση να εντοπίσει και να υλοποιήσει επαρκή μέτρα για τη μείωση των κινδύνων σε αποδεκτό επίπεδο.

Στο στάδιο λοιπόν αυτό η Εκτίμηση Αντικτύπου θα πρέπει να περιλαμβάνει έναν λεπτομερή κατάλογο των κινδύνων για τους οποίους ο υπεύθυνος επεξεργασίας δεν έχει καταφέρει να υλοποιήσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τον περιορισμό τους σε αποδεκτά επίπεδα. Οι κίνδυνοι αυτοί θα αναφέρονται ως υπολειπόμενοι κίνδυνοι(residual risks).

Ακόμη, στο στάδιο αυτό ο υπεύθυνος επεξεργασίας εφόσον δεν είναι σε θέση να εντοπίσει εκείνα τα κατάλληλα μέτρα για τον περιορισμό των κινδύνων θα πρέπει να προβεί σε διαβούλευση με την αρμόδια εποπτική αρχή.

- **Κατάλογος Υπολειπόμενων Κινδύνων**

Υπολειπόμενος Κίνδυνος	Επίπεδο Κινδύνου	Μέτρα τα οποία έχουν ληφθεί	Δράση Αντιμετώπισης
			• Λήψη εναλλακτικών μέτρων • Διαβούλευση με την Εποπτική Αρχή

4.4.1.2 Η Εκτίμηση Αντικτύπου γίνεται αποδεκτή.

Σε περίπτωση κατά την οποία κρίνεται ότι οι κίνδυνοι οι οποίοι έχουν αναγνωρισθεί έχουν αντιμετωπιστεί επαρκώς με την εφαρμογή των κατάλληλων μέτρων τότε ο υπεύθυνος

επεξεργασίας προχωρά στην δημιουργία του πλάνου αλλά και τη σύνταξη της επίσημης έκθεσης της Εκτίμησης Αντικτύπου.

- Ανάπτυξη του πλάνου εφαρμογής των μέτρων ασφαλείας
- Σύνταξη της τελικής έκθεσης της Εκτίμησης Αντικτύπου

4.4.2 Πλάνο Εφαρμογής Μέτρων Προστασίας

Τα τεχνικά και οργανωτικά μέτρα τα οποία έχουν επιλεγεί από τον υπεύθυνο επεξεργασίας και καταγραφεί στην Εκτίμηση Αντικτύπου θα πρέπει να αξιολογούνται τακτικά ως προς τη αναλογικότητα και την αποτελεσματικότητα τους.

Ο υπεύθυνους επεξεργασίας θα πρέπει να διεξάγει μια ανάλυση κόστους-οφέλους για τα υλοποιημένα μέτρα αλλά και να προβεί σε διαβούλευση με τους εργαζόμενους οι οποίοι επηρεάζονται άμεσα από την εφαρμογή ενός μέτρου προκειμένου να αξιολογήσει την αποτελεσματικότητα αλλά και την λειτουργικότητα του.

Για το λόγο αυτό συνιστάται η ανάπτυξη ενός πλάνου εφαρμογής των μέτρων προστασίας. Το έγγραφο αυτό συνιστά έναν κατάλογο με όλα τα προβλεπόμενα μέτρα ασφάλειας τα οποία ο υπεύθυνος επεξεργασίας έχει επιλέξει να εφαρμόσει για τον περιορισμό των κινδύνων και τη συμμόρφωση με τις απαιτήσεις του Κανονισμού.

Περιλαμβάνει πληροφορίες για το κόστος , την εφαρμογή, την πρόοδο και τον έλεγχο αποτελεσματικότητας των μέτρων

- **Ο παρακάτω πίνακας μπορεί να χρησιμοποιηθεί για την ανάπτυξη του πλάνου αυτού και την παρακολούθηση της εφαρμογής του:**

Κίνδυνος – Μέτρο Νομική Απαίτηση	Υπεύθυνος Υλοποίησης	Δυσκολία Υλοποίησης	Κόστος Υλοποίησης	Χρονική Διάρκεια Ισχύος	Κατάσταση Υλοποίησης	Παρατηρήσεις Εργαζομένων που επηρεάζονται από την εφαρμογή του μέτρου

Οι κλίμακες που ακολουθούν δύναται να χρησιμοποιηθούν για τον προσδιορισμό των επιπέδων κάθε κατηγορίας ελέγχου των μέτρων:

Κριτήριο	Επίπεδο 1	Επίπεδο 2	Επίπεδο 3
Δυσκολία Υλοποίησης	Χαμηλό	Μέτριο	Υψηλό
Κόστος Υλοποίησης	Μηδενικό	Μέτριο	Υψηλό
Χρονική Διάρκεια Ισχύος	6 μήνες	1 χρόνος	3 χρόνια

Κατάσταση Υλοποίησης	Δεν έχει ξεκινήσει	Υπό υλοποίηση	Ολοκληρωμένο

Πίνακας 16 - Αξιολόγηση Μέτρων

4.4.3 Σύνταξη Έκθεσης Εκτίμησης Αντικτύπου

Η διεξαγωγή μιας Εκτίμησης Αντικτύπου όπως έχουμε τονίσει αφορά κυρίως τη διαδικασία ταυτοποίησης και περιορισμού των κινδύνων με τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων. Αυτά είναι τα στάδια που θα παράσχουν διαβεβαιώσεις ότι ένας οργανισμός χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα με σεβασμό για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Ωστόσο, είναι επίσης σημαντικό ο υπεύθυνος επεξεργασίας να διατηρεί ένα αρχείο με τη μεθοδολογία και τα αποτελέσματα της διαδικασίας. Αυτό θα διασφαλίσει ότι όντως εφαρμόζονται τα αναγκαία μέτρα και έχει στόχο την ικανοποίηση τις απαίτησης της λογοδοσίας αλλά και της διαφάνειας στα πλαίσια του Κανονισμού. Μπορεί επίσης να χρησιμοποιηθεί προκειμένου να παρέχει τις απαραίτητες διαβεβαιώσεις στο κοινό, την αρμόδια εποπτική αρχή αλλά και σε άλλους ενδιαφερόμενους ότι η διαδικασία επεξεργασίας έχει αναλυθεί διεξοδικά και έχει αναπτυχθεί με απόλυτο σεβασμό για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

Δεν υπάρχει κάποια νομική απαίτηση για την σύνταξη μιας έκθεσης Εκτίμησης Αντικτύπου, ωστόσο συνιστά καλή πρακτική όσον αφορά τους υπεύθυνους επεξεργασίας.

Η έκθεση της Εκτίμησης Αντικτύπου συνοψίζει όλα τα σημαντικά ευρήματα και αποτελέσματα της διαδικασίας διενέργειας μιας Εκτίμησης Αντικτύπου.

Η έκθεση πρέπει να περιλαμβάνει μια επισκόπηση των πράξεων επεξεργασίας, εξηγώντας γιατί έχουν αναληφθεί και πώς θα επηρεάσουν τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Μπορεί να περιλαμβάνει ή να αναφέρει τα αποτελέσματα παράγονται κατά τη διάρκεια της Εκτίμησης Αντικτύπου, για παράδειγμα την περιγραφή των ροών δεδομένων και το μητρώο των κινδύνων . Η έκθεση θα πρέπει να περιγράφει επίσης πώς εντοπίστηκαν κίνδυνοι και πώς θα αντιμετωπιστούν.

Βασικά στοιχεία τα οποία θα πρέπει να περιλαμβάνονται σε μια έκθεση Εκτίμησης Αντικτύπου είναι τα κάτωθι:

- Μεθοδολογία διενέργειας της Εκτίμησης Αντικτύπου
- Περιγραφή του Έργου
- Περιγραφή των ροών πληροφοριών
- Τα αποτελέσματα της ανάλυσης ,συμπεριλαμβανομένων των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που έχουν εντοπιστεί, καθώς και των μέτρων που έχουν επιλεγεί για την αντιμετώπιση των κινδύνων αυτών.
- Περιγραφή τυχόν κινδύνων οι οποίοι δεν κατέστη δυνατόν να μετριαστούν (υπολειπόμενοι κίνδυνοι- residual risks)

- Εάν είναι αναγκαίο, μπορούν να παρέχονται λεπτομερέστερες πληροφορίες όπως για παράδειγμα σχετικά με τις διαδικασίες διαβούλευσης και τα αποτελέσματα τους στα παραρτήματα.

ΕΚΘΕΣΗ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ

- **ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ:**
  - Στοιχεία υπεύθυνου επεξεργασίας
  - Στοιχεία υπεύθυνου προστασίας δεδομένων
  - Στοιχεία ατόμου που έδωσε την τελική έγκριση
  - Στοιχεία συμμετεχόντων στην διενέργεια της μελέτης
  - Ημερομηνία διεξαγωγής
- **ΕΙΣΑΓΩΓΗ** :
  - Περιγραφή των υπό εξέταση πράξεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα
  - Μεθοδολογία διενέργειας της Εκτίμησης Αντικτύπου
- **ΚΥΡΙΟ ΜΕΡΟΣ**
  - Περιγραφή του σκοπού της επεξεργασίας
  - Περιγραφή των ροών πληροφοριών
  - Κατάλογος εντοπισθέντων κινδύνων
  - Κατάλογος μέτρων προστασίας
  - Κατάλογος υπολειπόμενων κινδύνων
- **ΣΥΜΠΕΡΑΣΜΑΤΑ:**
  - Σκεπτικό για την επικύρωση της Εκτίμησης Αντικτύπου
- **ΠΑΡΑΡΤΗΜΑΤΑ**
  - Λεπτομερής περιγραφή του πεδίου εφαρμογής
  - Λεπτομερής παρουσίαση των μέτρων

Είναι σημαντικό να τονιστεί ότι η έκθεση της Εκτίμησης Αντικτύπου θα πρέπει να αποτελεί ένα έγγραφο γραμμένο σε όσο το δυνατό πιο απλή και κατανοητή μορφή έτσι ώστε να μπορεί εύκολα να ερμηνευθεί από όλους ενδιαφερόμενους φορείς του έργου.

Επίσης, το έγγραφο αυτό πρέπει να είναι διαθέσιμο στην αρμόδια εποπτική Αρχή. Αυτό σημαίνει ότι θα πρέπει ο υπεύθυνος επεξεργασίας να κοινοποιεί την Εκτίμηση Αντικτύπου στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα όποτε η Αρχή το ζητήσει.

Τέλος, ως καλή πρακτική στο πλαίσιο της διαφάνειας από πλευράς υπευθύνου επεξεργασίας αλλά και ενίσχυσης του κύρους του Οργανισμού συνίσταται η δημοσιοποίηση μέρους ή του συνόλου της αναφοράς της Εκτίμησης Αντικτύπου.

4.4.4 Δημοσίευση Αποτελεσμάτων Εκτίμησης Αντικτύπου

Η δημοσίευση της Εκτίμησης Αντικτύπου δεν αποτελεί νομική απαίτηση του Κανονισμού Ωστόσο, η δημοσίευση υλικού που σχετίζεται με την Εκτίμηση Αντικτύπου, συμπεριλαμβανομένης της έκθεσης ,σε περίπτωση που έχει παραχθεί, συνιστά καλή πρακτική για τους υπεύθυνους και τους εκτελούντες την επεξεργασία.

Επαφίεται στην απόφαση του υπεύθυνου επεξεργασίας αν θα το πράξει ή όχι. Ο σκοπός μιας τέτοιας πράξης θα ήταν να συμβάλει στην ενίσχυση της εμπιστοσύνης στις διαδικασίες επεξεργασίας του υπεύθυνου επεξεργασίας και να αποδείξει την υπευθυνότητα και τη διαφάνεια που διακατέχει τον οργανισμό.

Αυτό θα μπορούσε να συμβεί ιδιαίτερα όταν μια δημόσια αρχή εκτελεί μια Εκτίμηση Αντικτύπου.

Το κομμάτι της Εκτίμησης Αντικτύπου το οποίο δύναται να δημοσιοποιηθεί δεν χρειάζεται να περιέχει ολόκληρη την αξιολόγηση, ειδικά όταν αυτή θα μπορούσε να αποκαλύψει συγκεκριμένες πληροφορίες σχετικά με τους κινδύνους ασφαλείας για τον υπεύθυνο επεξεργασίας δεδομένων ή να αποκαλύψει εμπορικά μυστικά ή εμπορικά ευαίσθητες πληροφορίες του οργανισμού.

Υπό τις συνθήκες αυτές, η δημοσιευμένη έκδοση θα μπορούσε να συνίσταται απλώς σε μια περίληψη των κύριων ευρημάτων της Εκτίμησης Αντικτύπου, ή μάλιστα μόνο σε μια δήλωση ότι έχει πραγματοποιηθεί μια Εκτίμηση Αντικτύπου.

Περιεχόμενα Εκτίμησης Αντικτύπου	Ενδιαφερόμενα Μέρη	
	Εποπτική Αρχή	Ευρύ Κοινό
Στοιχεία υπεύθυνου επεξεργασίας	✓	✓
Στοιχεία υπεύθυνου προστασίας δεδομένων	✓	✓
Στοιχεία ατόμου που έδωσε την τελική έγκριση	✓	
Στοιχεία συμμετεχόντων στην διενέργεια της μελέτης	✓	✓
Ημερομηνία διεξαγωγής	✓	✓

Περιεχόμενα Εκτίμησης Αντικτύπου	Ενδιαφερόμενα Μέρη	
Περιγραφή των υπό εξέταση πράξεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα	✓	
Μεθοδολογία διενέργειας της Εκτίμησης Αντικτύπου	✓	✓
Περιγραφή του σκοπού της επεξεργασίας	✓	✓
Περιγραφή των ροών πληροφοριών	✓	✓
Κατάλογος εντοπισμένων κινδύνων	✓	✓
Κατάλογος μέτρων προστασίας	✓	✓
Κατάλογος υπολειπόμενων κινδύνων	✓	
Σκεπτικό για την επικύρωση της Εκτίμησης Αντικτύπου	✓	
Λεπτομερής περιγραφή του πεδίου εφαρμογής	✓	
Λεπτομερής παρουσίαση των μέτρων	✓	

Πίμακας 17 - Δημοσίευση Περιεχομένων

4.4.5 Αναθεώρηση της Εκτίμησης Αντικτύπου

Μια επιτυχημένη και αποδεκτή μελέτη Εκτίμησης Αντικτύπου δεν θα πρέπει να λογίζεται ως ένα στατικό έγγραφο αλλά ως μια συνεχώς εξελισσόμενη διαδικασία.

Αυτό οφείλεται στο γεγονός ότι τα περισσότερα έργα υφίστανται αλλαγές πριν τεθούν σε τελική εφαρμογή.

Καθώς το έργο εξελίσσεται, η Εκτίμηση Αντικτύπου πρέπει να επανεξετάζεται, να ενημερώνεται ή να αναθεωρείται εάν οι εξελίξεις στο σχεδιασμό ή στην υλοποίηση του έργου δημιουργούν νέες επιπτώσεις και κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που δεν είχαν εξεταστεί προηγουμένως.

Σε περίπτωση κατά την οποία οι αλλαγές είναι σημαντικές και έχουν ως αποτέλεσμα αντίστοιχα σημαντικές νέες επιπτώσεις που δεν εξετάστηκαν στην Εκτίμηση Αντικτύπου, ενδέχεται να χρειαστεί να διενεργηθεί νέα , ακολουθώντας τα βήματα που περιγράφονται παραπάνω.

Η διαδικασία αναθεώρησης της Εκτίμησης Αντικτύπου είναι απαραίτητη ιδίως :

- Όταν λάβει χώρα μια σημαντική αλλαγή στη πράξη επεξεργασίας μετά την έναρξη ισχύος του Κανονισμού. Για παράδειγμα, όταν χρησιμοποιείται μια νέα τεχνολογία ή όταν επεξεργάζονται τα δεδομένα για διαφορετικό σκοπό. Σε αυτές τις περιπτώσεις η επεξεργασία είναι ουσιαστικά μια νέα πράξη και θα μπορούσε να απαιτήσει την διενέργεια Εκτίμησης Αντικτύπου.

- Όταν υπάρχει μεταβολή του κινδύνου που παρουσιάζεται από την πράξη επεξεργασίας. Οι κίνδυνοι και το επίπεδο κινδύνου μπορούν να αλλάξουν ως αποτέλεσμα μιας αλλαγής σε ένα από τα συστατικά μέρη της επεξεργασίας (δεδομένα, υποστηρικτικά αγαθά, πηγές κινδύνου κ.λπ.) ή επειδή εξελίσσεται το πλαίσιο της επεξεργασίας (σκοπός, λειτουργικότητα κ.λπ. .)
- Τα συστήματα επεξεργασίας δεδομένων μπορούν να εξελιχθούν με την πάροδο του χρόνου και συνεπώς ενδέχεται να προκύψουν νέοι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.
- Το οργανωτικό ή κοινωνικό πλαίσιο της πράξης επεξεργασίας υποστεί αλλαγές. Για παράδειγμα: οι επιπτώσεις ορισμένων αυτοματοποιημένων αποφάσεων έχουν γίνει πιο σημαντικές, νέες κατηγορίες φυσικών προσώπων γίνονται ευάλωτες σε διακρίσεις ή τα δεδομένα προορίζονται να διαβιβαστούν σε παραλήπτες δεδομένων που βρίσκονται σε χώρα εκτός της Ένωσης.

Ως ορθή πρακτική, συνιστάται η τακτική αναθεώρηση κάθε Εκτίμησης Αντικτύπου ανά 3 τουλάχιστον έτη. Η αξιολόγηση αυτή συνιστάται επίσης για την επεξεργασία δεδομένων που πραγματοποιήθηκε πριν από τον Μάιο του 2018 και για το λόγο αυτό δεν υπόκειται σε υποχρέωση διενέργειας Εκτίμησης Αντικτύπου, ώστε να διασφαλιστεί ότι 3 χρόνια μετά την ημερομηνία αυτή ή νωρίτερα, ανάλογα με το πλαίσιο, οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων αντιμετωπίζονται αποτελεσματικά.

Συνεπώς , ο υπεύθυνος επεξεργασίας θα πρέπει να διαθέτει διαδικασίες συνεχούς ελέγχου και αναθεώρησης της μελέτης Εκτίμησης Αντικτύπου. Η αναθεώρηση της Εκτίμησης Αντικτύπου θα πρέπει να πραγματοποιείται μετά το πέρας ενός καθορισμένου χρονικού πεδίου όπως για παράδειγμα τα 3 έτη είτε εάν πραγματοποιηθεί κάποια σημαντική αλλαγή στο πλαίσιο επεξεργασίας είτε τέλος εάν αναγνωρισθούν νέοι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Κεφάλαιο 5: Συμπεράσματα

Η μελέτη Εκτίμησης Αντικτύπου αποτελεί ένα χρήσιμο εργαλείο για τους υπεύθυνους επεξεργασίας δεδομένων προκειμένου να υλοποιούν συστήματα επεξεργασίας δεδομένων τα οποία συμμορφώνονται με τις απαιτήσεις του νέου νομικού πλαισίου σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και το οποίο έχει καθολική εφαρμογή από τις 25 Μαΐου του 2018 σε όλη τη Ευρωπαϊκή Ένωση.

Παρά το γεγονός ότι η διενέργεια Εκτίμησης Αντικτύπου δεν είναι υποχρεωτική για όλες τις πράξεις επεξεργασίας αλλά μόνο για εκείνες οι οποίες δύναται να ενέχουν υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων οι υπεύθυνοι επεξεργασίας θα πρέπει να θεωρούν τη διεξαγωγή μιας Εκτίμησης Αντικτύπου ως μια χρήσιμη και θετική δραστηριότητα που βοηθά στη συμμόρφωση με το νόμο.

Ο Γενικός Κανονισμός καθορίζει τα βασικά κριτήρια διεξαγωγής και τα ελάχιστα περιεχόμενα μιας Εκτίμησης Αντικτύπου δεν θεσπίζει όμως κάποια συγκεκριμένη διαδικασία για την διεξαγωγή της. Συνεπώς, παρέχεται στους υπεύθυνους επεξεργασίας η δυνατότητα να διεξάγουν μια μελέτη Εκτίμησης Αντικτύπου με μια σχετική ελευθερία. Η Εκτίμηση Αντικτύπου είναι μια διεργασία επεκτάσιμη και η οποία μπορεί να λάβει διαφορετικές μορφές.

Η εκπόνηση μιας μελέτης Εκτίμησης Αντικτύπου αποτελεί βασικό στοιχείο της συμμόρφωσης με τον κανονισμό όπου σχεδιάζεται ή λαμβάνει χώρα επεξεργασία δεδομένων υψηλού κινδύνου. Αυτό σημαίνει ότι οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει αρχικά να χρησιμοποιούν τα κριτήρια που καθορίζονται στο παρόν έγγραφο για να καθορίσουν εάν πρέπει ή όχι να γίνει μια Εκτίμηση Αντικτύπου. Στη συνέχεια θα πρέπει να επιλέξουν μια μεθοδολογία για την διενέργεια της και να προβούν στην τεκμηρίωση των αποτελεσμάτων.

Όταν προγραμματίζεται η ανάπτυξη ενός έργου, ενός συστήματος ή μιας εφαρμογής που περιλαμβάνει μια πιθανή επεξεργασία υψηλού κινδύνου, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει:

- να επιλέξει μια μεθοδολογία που να ικανοποιεί τα κριτήρια που θεσπίζει ο Κανονισμός και να καθορίσει και να εφαρμόσει μια συστηματική διαδικασία διενέργειας της μελέτης Εκτίμησης Αντικτύπου.
- να εξασφαλίσει την συμμέτοχη στην διαδικασία των κατάλληλων ενδιαφερόμενων μερών και να καθορίσει με σαφήνεια τους ρόλους και τις αρμοδιότητες τους (υπεύθυνος επεξεργασίας, υπεύθυνος προστασίας δεδομένων, υποκείμενο των

δεδομένων ή εκπρόσωποί τους, επιχειρήσεις, τεχνικές υπηρεσίες, υπεύθυνος ασφάλειας πληροφοριών κ.λπ.)

- να διαβουλεύεται με την εποπτική αρχή όταν δεν είναι σε θέση να υλοποιήσει επαρκή μέτρα για την άμβλυνση των υψηλών κινδύνων ·
- να τεκμηριώνει λεπτομερώς τις αποφάσεις που έχουν ληφθεί.
- να επανεξετάζει περιοδικά την Εκτίμηση Αντικτύπου και την επεξεργασία που αξιολογεί, τουλάχιστον όταν υπάρχει κάποια σημαντική μεταβολή των κινδύνων
- να προσκομίσει την έκθεση της έκθεσης της Εκτίμησης Αντικτύπου στην αρμόδια εποπτική αρχή όταν το ζητήσει ·

Η εκπόνηση μιας επιτυχημένης Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί μια ιδιαιτέρως κρίσιμη και σημαντική διεργασία για κάθε οργανισμό που επεξεργάζεται προσωπικά δεδομένα.

Ακόμα και σε περιπτώσεις κατά τις οποίες η διενέργεια μελέτης Εκτίμησης Αντικτύπου δεν αποτελεί νομική απαίτηση στα πλαίσια του Κανονισμού η εκπόνηση της είναι απαραίτητη καθώς αποτελεί σημαντικό εργαλείο συμμόρφωσης με άλλες απαιτήσεις των οποίων η ικανοποίηση είναι αδιαπραγμάτευτη όπως η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού αλλά και οι αρχές της διαφάνειας και τη λογοδοσίας.

Κεφάλαιο 6: Βιβλιογραφία

- https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf
- https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf
- https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf
- https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/04/SDM-Methodology_V1_EN1.pdf
- https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- https://iapp.org/media/pdf/resource_center/BM-DPIA_under_GDPR.pdf
- https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf
- https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20Test%20Phase%20Guidelines%20and%20Requirements%20%282%29%20%282%29_0.pdf
- https://www.sans.org/reading-room/whitepapers/legal/generation-privacy-europe-impact-information-security-complying-gdp-37457
- https://andersonsantana.files.wordpress.com/2015/10/anpf2015.pdf
- http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
- https://ec.europa.eu/energy/en/content/dpia-template-smart-grid-and-smart-metering-systems
- https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf
- https://tizydorczyk.pl/images/doc/WP248_EN_rev01_2017_10_04.pdf
- http://ec-wu.at/spiekermann/publications/2012_EJIS_PIA_final_rev8.pdf

- https://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf