ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Τίτλος διπλωματική εργασίας:

«Εκτίμηση Αντικτύπου Απώλειας Ιδιωτικότητας»

Ονοματεπώνυμο Μεταπτυχιακού Φοιτητή:

Μαρία Τριανταφυλλοπούλου

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Γεώργιος Σταμούλης

Λαμία, Μάρτιος 2020

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Title: «Privacy Impact Assessment»

Name: Maria Triantafillopoulou

Master thesis

George Stamoulis

Lamia, March 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΚΑΤΕΥΘΥΝΣΗ :

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

Τίτλος διπλωματικής εργασίας:

«Εκτίμηση Αντικτύπου Απώλειας Ιδιωτικότητας»

Ονοματεπώνυμο Μεταπτυχιακού Φοιτητή:

Μαρία Τριανταφυλλοπούλου

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Γεώργιος Σταμούλης

Λαμία, Μάρτιος 2020

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Η ΔΗΛΟΥΣΑ

10/03/20

Μαρία Τριανταφυλλοπούλου

Τίτλος διπλωματική εργασίας:

«Εκτίμηση Αντικτύπου Απώλειας Ιδιωτικότητας»

Ονοματεπώνυμο Μεταπτυχιακού Φοιτητή:

Μαρία Τριανταφυλλοπούλου

Τριμελής Επιτροπή:

Γεώργιος Σταμούλης (Επιβλέπων)

Αντώνιος Δαδαλιάρης

Γεώργιος Δημητρίου

Επιστημονικός Σύμβουλος:

Θεόδωρος Ντούσκας

Περιεχόμενα

1.1 Προσωπικά Δεδομένα

Τα προσωπικά δεδομένα αποτελούν ένα ιδιαίτερο κεφάλαιο που απασχολεί τελευταία τόσο τον επιχειρηματικό κόσμο όσο και τον κόσμο του διαδικτύου. Ως προσωπικό δεδομένο λοιπόν, καλείται κάθε πληροφορία που αναφέρεται και προσδιορίζει μονοσήμαντα έναν άνθρωπο, όπως το ονοματεπώνυμο, η ηλικία, το επάγγελμα, τα φυσικά χαρακτηριστικά, η εκπαίδευση, η οικονομική κατάσταση, το πολιτικό φρόνημα, η θρησκευτική πεποίθηση, το ποινικό μητρώο, η ερωτική ζωή αλλά και πολλά άλλα (Αλεξανδροπούλου - Αιγυπτιάδου , 2016).

Τα δεδομένα αυτά δύνανται να καταγραφούν με πολλούς και διαφορετικούς τρόπους είτε από δημόσιους οργανισμούς, είτε από συλλόγους και ιδιωτικούς φορείς, είτε από ιστοσελίδες στις οποίες ο χρήστης διατηρεί ηλεκτρονικό λογαριασμό (Αλεξανδροπούλου - Αιγυπτιάδου , 2016). Μιας και πρόκειται για έναν ιδιαίτερα μεγάλο όγκο πληροφορίας, τα δεδομένα αυτά έχουν διαχωριστεί σε κατηγορίες ανάλογα πάντα με το είδος και τη σημαντικότητά τους. Ειδικότερα υπάρχουν (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2015) :

- ***Τα κοινά δεδομένα*** : Πρόκειται για μία κατηγορία όχι ιδιαίτερα ευαίσθητων προσωπικών δεδομένων η συλλογή και η επεξεργασία του ατόμου είναι αρκετή απλά μονά και με την προφορική συγκατάθεση του υποκειμένου. Τέτοιου είδους δεδομένα είναι το ονοματεπώνυμο, το επάγγελμα, η διεύθυνση κατοικίας, το μορφωτικό επίπεδο, η περιουσιακή κατάσταση, η οικογενειακή κατάσταση, οι καταναλωτικές συνήθειες, οι τραπεζικοί λογαριασμοί και το ύψος του μισθού.
- ***Τα ευαίσθητα δεδομένα*** : Ως ευαίσθητα, καλούνται τα δεδομένα εκείνα που εκπορεύονται από την αυστηρά προσωπική ζωή του υποκειμένου και δεν δύνανται να συλλεχθούν ή να επεξεργασθούν εάν δεν υπάρχει ανάλογη αδειοδότηση από την Αρχή Προστασίας Προσωπικών δεδομένων. Στην κατηγορία αυτή συμπεριλαμβάνονται οι θρησκευτικές πεποιθήσεις, οι σεξουαλικές προτιμήσεις, το ποινικό μητρώο, τα γενετικά δεδομένα, η υγεία, κτλ.
- ***Τα Δημόσια Δεδομένα*** : Στην κατηγορία αυτή εντάσσονται τα δεδομένα που σχετίζονται με το δημόσιο και άρα τα δεδομένα που παράγονται από δημόσιους και ιδιωτικούς φορείς.
- ***Τα Ανοικτά Δεδομένα*** : Πρόκειται για τα δεδομένα εκείνα που χρησιμοποιούνται, επαναχρησιμοποιούνται και διανέμονται ελεύθερα υπό τον όρο πάντα να γίνεται αναφορά στους δημιουργούς και να διατίθενται, με τη σειρά τους, υπό τους ίδιους όρους

Καθώς λοιπόν, όπως είναι αντιληπτό το εύρος, ο όγκος, το είδος αλλά και ο αριθμός των προσωπικών δεδομένων είναι μεγάλος στην πλειοψηφία των περιπτώσεων απαιτείται επεξεργασία αυτών. Ως επεξεργασία καλείται η κάθε εργασία που πραγματοποιείται πάνω στα δεδομένα προσωπικού χαρακτήρα και συχνά λαμβάνει τη μορφή της συλλογής, της καταχώρησης, της οργάνωσης, της αποθήκευσης, της χρήσης, της διασύνδεσης, της διαγραφής, της καταστροφής και πολλών άλλων(Bird&Bird, 2017). Η διαδικασία αυτή κρίνεται καίριας σημασίας καθώς πάνω σε αυτή βασίζεται σειρά υπηρεσιών που προσφέρεται στο άτομο από δημόσιους και ιδιωτικούς φορείς. Ο ίδιος ο νόμος, ορίζει ως επεξεργασία των δεδομένων προσωπικού χαρακτήρα, κάθε εργασία ή σειρά εργασιών που έχει εφαρμοστεί σε προσωπικά δεδομένα από το Δημόσιο ή από Νομικό Πρόσωπο Δημοσίου Δικαίου, ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς την βοήθεια αυτοματοποιημένων μεθόδων (Αυγουστιανάκης, 2001). Μάλιστα αυτός παραθέτει ένα ενδεικτικό κατάλογο των παραπάνω εργασιών που περιλαμβάνει (Αλεξανδροπούλου - Αιγυπτιάδου , 2016):

- ✓ **Τη συλλογή** και άρα την πρώτη φάση της επεξεργασίας η οποία αφορά την αναζήτηση, εύρεση και συγκέντρωση των δεδομένων (π.χ. συνέντευξη και συμπλήρωση των ερωτηματολογίων, βιντεοσκόπηση, φωτογράφιση ηχογράφηση)
- ✓ **Την καταχώριση**, δηλαδή την τοποθέτηση όγκου δεδομένων σε μία βάση ώστε να είναι δυνατή η επεξεργασία τους
- ✓ **Την οργάνωση**, δηλαδή την κατηγοριοποίηση δεδομένων με συγκεκριμένα κριτήρια, με χρήση ή χωρίς τη χρήση κάποιου εξειδικευμένου λογισμικού
- ✓ **Τη διατήρηση ή αποθήκευση** σε οποιοδήποτε μέσο αποθήκευσης
- ✓ **Την τροποποίηση** με διαδικασίες όπως η κρυπτογράφηση, η ανωνυμοποίηση, η ψευδωνυμοποίηση
- ✓ **Την εξαγωγή** σε έντυπη ή ηλεκτρονική μορφή
- ✓ **Τη χρήση** τους σε περιπτώσεις όπως τα δικαστήρια όπου γίνεται χρήση των δεδομένων προσωπικού χαρακτήρα
- ✓ **Τη διαβίβαση**, και άρα τη μετάδοση αυτών προς ένα τρίτο πρόσωπο
- ✓ **Την διάδοση η κάθε άλλης μορφής διάθεση**, δηλαδή τη μετάδοση προσωπικών δεδομένων σε κάθε κατεύθυνση και σε μεγαλύτερο αριθμό αποδεκτών (δημοσίευση στο διαδίκτυο, σε έντυπα ή στα μέσα μαζικής ενημέρωσης)
- ✓ **Την συσχέτιση ή το συνδυασμό**, που οδηγεί σε δημιουργία άμεσων σχέσεων, συγκρίσεων αλλά και αντιπαράθεσης δεδομένων σε δύο ή και περισσότερες βάσεις με στόχο πάντα την εξαγωγή συμπερασμάτων από τους υπευθύνους επεξεργασίας

- ✓ **Την διασύνδεση**, των δεδομένων ενός αρχείου με δεδομένα αλλού ή άλλων αρχείων, τα οποία τηρούνται από έναν υπεύθυνο επεξεργασίας ή τον ίδιο υπεύθυνο αλλά για διαφορετικό σκοπό
- ✓ **Τη δέσμευση** (κλείδωμα), δηλαδή τον αποκλεισμό κάθε επιπλέον επεξεργασίας π.χ. απόκρυψη δεδομένων
- ✓ **Την διαγραφή – καταστροφή**. Η έννοια της διαγραφής αφορά δεδομένα που δεν είναι ορατά η "αναγνώσιμα" από κάθε ανθρώπινη αίσθηση

Οι όροι Δεδομένα Προσωπικού Χαρακτήρα, συνοδεύονται συχνά από την έννοια του υποκειμένου η οποία σε κάθε περίπτωση αναφέρεται στο φυσικό πρόσωπο στο οποίο αφορούν τα δεδομένα και η ταυτότητα του οποίου δύναται να προσδιοριστεί άμεσα έμμεσα διαμέσου αναζήτησης σε βάσεις που εμπεριέχουν δεδομένα που χαρακτηρίζουν τη φυσική, βιολογική, κοινωνική, και πολιτική υπόστασή του (Αρμαμέντος & Σωτηρόπουλος, 2005). Είναι χαρακτηριστικό ότι με τον Ν.2472/1997, όπως και με την σχετική οδηγία 95/46 /ΕΚ, προστατεύονται μόνο τα (ζώντα) φυσικά πρόσωπα και όχι τα νομικά πρόσωπα π.χ. (σωματεία, εταιρείες). Ασφαλώς και υπάρχει εάν πλαίσιο προστασίας και για τα νομικά πρόσωπα, αυτό όμως υπόκειται σε γενικές διατάξεις περί αθέμιτου ανταγωνισμού κλπ (Αρμαμέντος & Σωτηρόπουλος, 2005).

Κράτη όπως η Αυστρία, το Λουξεμβούργο και η Ελβετία, έχουν συμπεριλάβει και τα νομικά πρόσωπα στο θεσμικό τους πλαίσιο περί προσωπικών δεδομένων ενώ η οδηγία 2002/58 της Ε.Ε, περιλαμβάνει ρυθμίσεις που αφορούν και στα νομικά πρόσωπα (Γιαννακούλα & Μηλαπίδου, 2017).

Για να γίνει επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα, θα πρέπει σε κάθε περίπτωση, να οριστεί ένας Υπεύθυνος Επεξεργασίας Προσωπικών Δεδομένων αρμοδιότητα του οποίου θα είναι τόσο ο σκοπός όσο και ο τρόπος της επεξεργασίας των δεδομένων από οποιαδήποτε μορφή οργανισμού. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο (Αρκουλή, 2010).

Έτσι λοιπόν, και σύμφωνα πάντα με βάση τα όσα ορίζονται από το νόμο, ο υπεύθυνος επεξεργασίας δεδομένων επεξεργάζεται τα δεδομένα όπως απαιτείται και σε κάθε περίπτωση και μετά το πέρας της επεξεργασίας τους είναι υπεύθυνος και για την καταστροφή αυτών (Αρκουλή, 2010).

1. 2 Γενική περιγραφή των απαιτήσεων ασφάλειας και προστασίας της Ιδιωτικότητας

Η έννοια της ιδιωτικότητας αποτέλεσε ένα κοινωνικό και ηθικό ζήτημα το οποίο έχει μελετηθεί από επιστήμονες και φιλοσόφους για πολλά έτη σε όλα τα μήκη και τα πλάτη του κόσμου. Σύμφωνα με τους δικαστές S. Warren και L. Brandeis στις ΗΠΑ η ιδιωτικότητα είναι «…το δικαίωμα των πολιτών σε μία ανενόχλητη ιδιωτική ζωή (the right to fan individual to be let alone)» (Γκριτζαλης, Λαμπρινουδάκης, Κάτσικας, & Μήτρου, 2010). Ήταν πολύ λίγα τα χρόνια μετά τη διατύπωση αυτή όταν η προστασίας της ιδιωτικότητας θεσμοθετήθηκε ως θεμελιώδες ανθρώπινο δικαίωμα στη Διακήρυξη των Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών, στη Διεθνή Σύμβαση για τα Πολιτικά Δικαιώματα, και στα Θεμελιώδη Δικαιώματα των πολιτών της Ευρωπαϊκής Ένωσης (Γκριτζαλης, Λαμπρινουδάκης, Κάτσικας, & Μήτρου, 2010).

Στην πορεία των χρόνων, η έννοια της ιδιωτικότητας συμπεριέλαβε και σειρά επιμέρους δικαιωμάτων όπως αυτό της ιδιωτικής ζωής, του αποκλειστικού ελέγχου της πρόσβασης στον ιδιωτικό χώρο, της εχεμύθειας, του απορρήτου και της ανωνυμίας. Παράλληλα με τα παραπάνω και τη μελέτη της ιδιωτικότητας από πολλά επιστημονικά πεδία, η ραγδαία αύξηση της πληροφορικής και των τηλεπικοινωνιών, οδήγησε στην ανάπτυξη υπηρεσιών τέτοιων που αποσκοπούν στην παροχή μιας διαφορετικής ποιότητας ζωής στο σύνολο των πολιτών, αλλά και στην αμεσότερη πρόσβαση στην πληροφορία διαμέσου του διαδικτύου. Στο χώρο αυτό, όμως, η αποκέντρωση της επεξεργασίας των δεδομένων και η διείσδυση της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας, αλλάζουν ριζικά το περιβάλλον χρήσης των προσωπικών πληροφοριών, οπότε εγείρονται σημαντικά ζητήματα σχετικά με την προστασία της ιδιωτικότητας στον ψηφιακό κόσμο (Ακριβοπούλου Χ. , 2011).

Εύλογα λοιπόν, όλες οι χώρες του κόσμου προέβησαν στη θέσπιση νόμων, ώστε τα προσωπικά δεδομένα να είναι πλήρως προστατευμένα και να ορίζονται δια νόμου διαδικασίες, όπως η συλλογή και η επεξεργασία των δεδομένων από δημόσιους και ιδιωτικούς φορείς (Αλεξανδροπούλου - Αιγυπτιάδου , 2016). Η θέσπιση νόμων από την κάθε χώρα, σημαίνει ταυτόχρονα και την ύπαρξης μίας δημόσιας αρχής, ρόλος της οποίας θα είναι η επιτήρηση της εφαρμογής των νόμων αυτών.

Οι απαιτήσεις ασφάλειας και ιδιωτικότητας των δεδομένων - πληροφοριών περιλαμβάνουν τα κάτωθι (Γκρίτζαλης & Γκρίτζαλης, 2004):

- ***Εμπιστευτικότητα (Confidentiality):*** αφορά στην προστασία από αποκάλυψη δεδομένων σε μη εξουσιοδοτημένες οντότητες

- ***Ακεραιότητα (Integrity):*** αφορά στην προστασία από μη εξουσιοδοτημένη εισαγωγή, τροποποίηση ή διαγραφή δεδομένων
- ***Διαθεσιμότητα (Availability):*** αφορά στην προστασία από μη-διάθεση των δεδομένων
- ***Αυθεντικότητα (Authenticity):*** αφορά στη διασφάλιση της ταυτότητας κάθε εμπλεκόμενης οντότητας
- ***Μη Αποποίηση (Non Repudiation):*** αφορά στην προστασία από άρνηση μιας οντότητας για πραγματοποίηση συγκεκριμένης δραστηριότητας. Για την μετατροπή της ιδιωτικότητας από μία γενική έννοια σε τεχνική απαίτηση έχουν ορισθεί οι επιμέρους απαιτήσεις ιδιωτικότητας :
    - *Αυθεντικοποίηση (Authentication):* η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας. Αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας ενός Π.Σ., ωστόσο έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας.
    - *Εξουσιοδότηση (Authorization):* η διαδικασία μέσω της οποίας μία οντότητα αποκτά δικαιώματα - πρόσβαση σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος.
    - *Αναγνώριση (Identification):* η διαδικασία μέσω της οποία ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.
- ***Προστασία Δεδομένων (Data Protection):*** η διαδικασία μέσω της οποίας διασφαλίζονται, σύμφωνα και με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, οι κάτωθι αρχές (Γκρίτζαλης & Γκρίτζαλης, 2004):
    - Αρχή της νομιμότητας και της δικαιοσύνης.
    - Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν.
    - Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων.
    - Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων.
    - Αρχή της ασφάλειας και της ακεραιότητας.
    - Εποπτεία και Επικύρωση.
- ***Ανωνυμία (Anonymity):*** η διαδικασία μέσω της οποίας διασφαλίζεται ότι μία οντότητα μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με μια άλλη οντότητα χωρίς να αποκαλύψει την ταυτότητά της

- ***Ψευδωνυμία (Pseydonymity):*** η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση (Identification) μιας οντότητας από μη εξουσιοδοτημένες τρίτες οντότητες
- ***Μη-συνδεσιμότητα (Unlinkability):*** η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, οδηγώντας έτσι στην αποκάλυψη της ταυτότητάς της.
- ***Μη-παρατηρησιμότητα (Unobservability):*** η διαδικασία μέσω της οποία προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν ίχνη της πρώτης.

Η αξία της ιδιωτικότητας έγκειται στην ικανότητα της να παρέχει στο πρόσωπο προστασία από κάθε εισβολή ή παρέμβαση στον ιδιωτικό του χώρο, καθώς και από κάθε είδους καταπιεστική, χειραγωγική, ελεγκτική ή πατερναλιστική συμπεριφορά, η οποία στοχεύει στον περιορισμό της ελευθερίας του προσώπου να αναπτύσσει απρόσκοπτα την προσωπικότητά του και της αυτονομίας του να διαμορφώνει και να απολαμβάνει τις σχέσεις του με τους οικείους του, καθώς και τις επιλογές εκείνες μέσα από τις οποίες τελικά αυτοπροσδιορίζεται (Ακριβοπούλου Χ. , 2012).

Η προστασία του δικαιώματος στην ιδιωτική ζωή, προστατεύει στον ίδιο τον άνθρωπο, την ταυτότητα και την αξιοπρέπεια αυτού. Οι βασικές αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων, όπως ορίστηκαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης, στις Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων (OECD, 1980) και που, περισσότερο ή λιγότερο, αντανακλώνται σε όλους τους σύγχρονους σχετικούς νόμους των δημοκρατικών κρατών παγκοσμίως, είναι οι παρακάτω (Ακριβοπούλου Χ. , 2012):

- *Αρχή περιορισμού της συλλογής (Collection Limitation Principle):* Θα πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων, η συλλογή τους θα πρέπει να πραγματοποιείται με χρήση θεμιτών και σύννομων μέσων και – όπου είναι δυνατό – με τη συναίνεση ή την ενημέρωση του χρήστη.
- *Αρχή ποιότητας των δεδομένων (Data Quality Principle):* Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν ενώ – στο βαθμό που είναι απαραίτητο για το σκοπό αυτό – θα πρέπει να είναι πλήρη, ακριβή και ενημερωμένα.
- *Αρχή προσδιορισμού του σκοπού (Purpose Specification Principle):* Ο σκοπός για τον οποίο συλλέγονται προσωπικά δεδομένα θα πρέπει να προσδιορίζεται το αργότερο

κατά τη χρονική στιγμή της συλλογής τους, ενώ η συνακόλουθη χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση του σκοπού αυτού ή κάποιου πλήρως συμβατού σκοπού.

- *Αρχή περιορισμού της χρήσης (Use Limitation Principle):* Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται σε τρίτες οντότητες ή να χρησιμοποιούνται για άλλο σκοπό εκτός από τον προσδιορισμένο, σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός εάν υπάρχει η σχετική συναίνεση του χρήστη ή η εξουσιοδότηση από το νόμο.
- *Αρχή προστασίας της ασφάλειας (Security Safeguards Principle):* Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση των κατάλληλων μηχανισμών απέναντι σε κινδύνους, όπως η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες.
- *Αρχή της διαφάνειας (Openness Principle):* Θα πρέπει να υπάρχει γενική διαφάνεια αναφορικά με τις πολιτικές και τις πρακτικές που σχετίζονται με τη συλλογή και επεξεργασία των προσωπικών δεδομένων, καθώς και με την ταυτότητα του φορέα που διενεργεί τη συλλογή και επεξεργασία.
- *Αρχή της συμμετοχής του ατόμου (Individual Participation Principle):* Το κάθε άτομο θα πρέπει να έχει το δικαίωμα (Ακριβοπούλου Χ. , 2012):
    - Να αποκτά είτε απ' ευθείας από τον υπεύθυνο της επεξεργασίας είτε μέσω κάποιου άλλου τρόπου, επιβεβαίωση αναφορικά με το αν ο υπεύθυνος της επεξεργασίας διαθέτει δεδομένα που σχετίζονται με το εν λόγω άτομο.
    - Να του ανακοινώνονται δεδομένα που σχετίζονται με αυτό, μέσα σε εύλογο χρονικό διάστημα, με εύλογο τρόπο, σε μορφή εύκολα κατανοητή και εφόσον η ανακοίνωση προϋποθέτει κόστος, αυτό να μην είναι υπερβολικό.
    - Να του παρέχονται οι λόγοι για τους οποίους απορρίπτονται αιτήσεις του που αναφέρονται στις δύο παραπάνω παραγράφους και να διατηρεί στην περίπτωση αυτή τη δυνατότητα της αμφισβήτησης, της απόρριψης και της περαιτέρω διεκδίκησης.
    - Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτό, και, σε περίπτωση επιτυχημένης αμφισβήτησης, να μπορεί να προχωρεί σε εξάλειψη, διόρθωση ή ολοκλήρωση των δεδομένων αυτών.
- *Αρχή της ευθύνης (Accountability Principle):* Κάθε υπεύθυνος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι υπόλογος, αναφορικά με την εφαρμογή των μέτρων εκείνων που προάγουν τις παραπάνω αρχές, που πρέπει να

διέπουν την προστασία των προσωπικών δεδομένων. Στις παραπάνω βασικές αρχές για την προστασία των προσωπικών δεδομένων βασίστηκε, μεταξύ άλλων, και η ανάπτυξη της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ , η οποία παρουσιάζεται στη συνέχεια.

1.3 Οι συνθήκες που οδήγησαν στη Θέσπιση Νέου Κανονισμού για τα Προσωπικά Δεδομένα

Ο τομέας των Προσωπικών Δεδομένων και η σοβαρότητα αυτού απασχόλησε τους Ευρωπαίους νομοθέτες από το 1995 όπου και εισήγαγαν σημαντικές νομολογίες για τα κράτη – μέλη της Ένωσης. Στόχος αυτού ήταν η διασφάλιση των δεδομένων των φυσικών προσώπων αλλά και η διευκόλυνση της κυκλοφορίας αυτών με στόχο την οικονομική και κοινωνική πρόοδο (Σ Ε Β, 2018).

Ωστόσο, και παράλληλα με την πάροδο του χρόνου και τις εξελίξεις σε οικονομικό και τεχνολογικό επίπεδο, δύο ήταν οι βασικές παράμετροι οι οποίες κατέστησαν αναγκαία τη θέσπιση ενός νέου κανονιστικού πεδίου, ώστε να ενισχυθεί η αποτελεσματικότητα των θεσμών σε ότι αφορά τα προσωπικά δεδομένα. Αφενός, πρόκειται για τη ραγδαία τεχνολογική εξέλιξη που κατέστησε την προηγούμενη οδηγία παρωχημένη και αφετέρου την ασυμμετρία εφαρμογής της οδηγίας από τα κράτη – μέλη και το έλλειμμα της προστασίας της ιδιωτικότητας που αποδείχθηκε να υφίσταται στην πράξη.

Όπως είναι αντιληπτό, η ραγδαία εξέλιξη της τεχνολογίας, μαζί με την οικονομική ανάπτυξη, διευκόλυνε και την παραβίαση των προσωπικών δεδομένων με ποικίλους τρόπους. Για τον παραπάνω λόγο, ο νέος κανονισμός, υποχρεώνει όλα τα κράτη – μέλη με τη συμμόρφωση τους ειδικότερα σε ότι αφορά τα μέτρα ασφάλειας των συστημάτων δικτύου και πληροφοριών (Σ Ε Β, 2018). Ακόμη, συζητείται ιδιαίτερα έντονα, ο κίνδυνος μίας νέας «ψηφιακής δικτατορίας» η οποία φυσικά θα αντλεί τη δύναμή της από τον τεράστιο όγκο δεδομένων που θα συλλέγεται στα χέρια των λίγων. Στα παραπάνω έρχεται να προστεθεί και η αποτυχία της ευρωπαϊκής πολιτικής να αποτρέψει τον κατακερματισμό του τρόπου εφαρμογής των διατάξεων για την προστασία των προσωπικών δεδομένων στην ΕΕ, προκαλώντας ανασφάλεια δικαίου εξαιτίας της ύπαρξης αποκλίσεων, κατά την εκτέλεση και εφαρμογή της, μεταξύ των κρατών-μελών (Σ Ε Β, 2018).

Οι διαφορετικές πολιτικές που εφαρμόστηκαν από τα κράτη – μέλη, όχι μονάδα δεν κατάφεραν να προστατέψουν τα φυσικά πρόσωπα αλλά θεωρήθηκαν και μία τεράστια τροχοπέδη σε ότι αφορά την ψηφιακή επανάσταση. Για το λόγο αυτό, ο νεοσύστατος κανονισμός εστιάζει στη συνεκτική εφαρμογή του σε ολόκληρη την Ένωση.

2.1 Γενικός Κανονισμός για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα

Σήμερα έχει ταυτιστεί με τη συντομογραφία GDPRπου αφορά στη συντόμευση των λέξεων General Data Privacy Regulation. Πρόκειται για το Γενικό Κανονισμό για την Προστασία Προσωπικών Δεδομένων ο οποίος έχει θεσμοθετηθεί από την Ευρωπαϊκή Ένωση αποσκοπώντας στην προστασία των προσωπικών δεδομένων των πολιτών και στη θεσμοθέτηση των προϋποθέσεων εκείνων με τις οποίες θα γίνεται χρήση, επεξεργασία και διαβίβαση των ευαίσθητων αυτών δεδομένων (Υπουργείο Δικαιοσύνης, 2018).

Όπως περιγράφηκε παραπάνω, η ανάγκη προστασίας των δεδομένων προσωπικού χαρακτήρα, προέκυψε πολύ νωρίτερα και συνδέθηκε άμεσα με την εξέλιξη της τεχνολογίας καθώς οι προσωπικές πληροφορίες των υποκειμένων των δεδομένων άρχισαν να αποτελούν προϊόν εκμετάλλευσης.

Η εν λόγω κοινωνική και ηθική απαίτηση θεσμοθέτησης ενός νομικού πλαισίου που θα περιλαμβάνει την προστασία των προσωπικών δεδομένων εν συνόλω, αναφέρεται χαρακτηριστικά στο βιβλίο «EU General Data Protection Regulation (GDPR) : An Implementation and Compliance Guide», 2017, σ. 11, MLA (Σύγχρονη Γλώσσα) IT Διακυβέρνηση (Οργάνωση), και Ευρωπαϊκή Ένωση: «Το GDPR είναι το τελευταίο βήμα της συνεχιζόμενης παγκόσμιας αναγνώρισης της αξίας και της σημασίας των προσωπικών πληροφοριών. Παρόλο που η αγορά των προσωπικών πληροφοριών υπήρχε ήδη για κάποιο χρονικό διάστημα, η πραγματική αξία των προσωπικών δεδομένων μόλις έγινε πιο προφανής. Η διαδικτυακή κλοπή δεδομένων προσωπικού χαρακτήρα εκθέτει τους πολίτες της Ε.Ε. σε σημαντικούς προσωπικούς κινδύνους. Μεγάλες τεχνικές ανάλυσης δεδομένων επιτρέπουν στους οργανισμούς να ανιχνεύουν και να προβλέπουν την ατομική συμπεριφορά, η οποία μετέπειτα δύναται να αναπτυχθεί σε αυτοματοποιημένη λήψη αποφάσεων. Ο συνδυασμός όλων αυτών των ζητημάτων, σε συνδυασμό με τη συνεχή εξέλιξη της τεχνολογίας και τις ανησυχίες σχετικά με την κατάχρηση των προσωπικών δεδομένων από τις κυβερνήσεις και τις επιχειρήσεις, οδήγησε σε νέο νόμο της Ε.Ε. για τη διευκρίνιση των δικαιωμάτων των πολιτών της Ε.Ε. και για την εξασφάλιση κατάλληλου επιπέδου προστασίας των προσωπικών δεδομένων.»(EuropeanUnion, 2017)

Καθ’ ότι πρόκειται για ένα νομικό κείμενο, ο Κανονισμός περιλαμβάνει ιδιαίτερο λεξιλόγιο και κάνει χρήση εννοιών που δεν είναι εύκολα κατανοητές στο πλήρες φάσμα τους. Εκ

τούτου, παρακάτω επεξηγείται το εννοιολογικό πλαίσιο αυτών των λέξεων/ εκφράσεων (Υπουργείο Δικαιοσύνης, 2018):

- «**Επεξεργασία**»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή

- «**Περιορισμός της Επεξεργασίας**»: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον

- «**Κατάρτιση Προφίλ**»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου

- «**Ψευδωνυμοποίηση**»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο
- «**Σύστημα Αρχειοθέτησης**»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση

- «**Υπεύθυνος Επεξεργασίας**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον

διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους

- «**Εκτελών την Επεξεργασία**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

- «**Αποδέκτης**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες· η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας

- «**Τρίτος**»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα
- «**Συγκατάθεση**» του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν

- «**Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα**»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία

- «**Δεδομένα Ειδικών Κατηγοριών**»: δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την

υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό

- «**Κύρια Εγκατάσταση**»: α) ο τόπος της κεντρικής διοίκησης του υπευθύνου β) όταν πρόκειται για εκτελούντα την επεξεργασία η εγκατάσταση του εκτελούντος την επεξεργασία στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας

- «**Εποπτική Αρχή**»: ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51 του ΓΚΠΔ

Το περιεχόμενο του Γενικού Κανονισμού για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα, αποτελεί πόνημα χρόνιων διαβουλεύσεων και συμβιβασμού όλων των εμπλεκόμενων σε αυτόν μερών. Έτσι λοιπόν, πρόκειται για έναν μακροσκελέστατο κανονισμό 5 φορές μεγαλύτερο από την Οδηγία, με 99 άρθρα, εκ των οποίων τα 28 αφήνουν περιθώριο παρέκκλισης για τα κράτη-μέλη(Calder, 2016).

Ο νέος κανονισμός εισάγει δύο πολύ ουσιώδεις αρχές που αφορούν στη λογοδοσία, το βάρος της οποίας μεταφέρεται στο ρυθμιζόμενο/ελεγχόμενο. Ο υπεύθυνος επεξεργασίας θα είναι σε κάθε περίπτωση εκείνος που θα πρέπει να αποδείξει ότι έλαβε όλα εκείνα τα απαραίτητα μέτρα ώστε να τηρούνται οι αρχές της προστασίας προσωπικών δεδομένων και η Εποπτική Αρχή να αναλάβει δράση σε δεύτερο χρόνο. Επιπρόσθετα, ανανεώνονται τα δικαιώματα των υποκειμένων το οποίο σημαίνει πως οι άνθρωποι πλέον έχουν ενισχυμένα δικαιώματα και οι υπεύθυνοι επεξεργασίας είναι υποχρεωμένοι να προσαρμοστούν σε αυτά και να προσαρμόσουν ανάλογα τις λειτουργίες των συστημάτων τους(Calder, 2016).

Οι βασικές αρχές οι οποίες απαιτείται να τηρούνται κατά την επεξεργασία των προσωπικών δεδομένων από τους Υπεύθυνους Επεξεργασίας και τους Εκτελούντες αυτήν, είναι, σύμφωνα με το άρθρο 5 του Κανονισμού οι εξής (Υπουργείο Δικαιοσύνης, 2018):

- ✓ **Η αρχή της νόμιμης, αντικειμενικής και διαφανούς επεξεργασίας** που επιβάλει την σύννομη, θεμιτή και με διαφανή τρόπο επεξεργασία αναφορικά με το υποκείμενο των δεδομένων. **Η νομιμότητα** της επεξεργασίας διασφαλίζεται, σύμφωνα με το άρθρο 6 του Κανονισμού, στις περιπτώσεις στις οποίες α) έχει ληφθεί η προηγούμενη συναίνεση του υποκειμένου στην επεξεργασία των δεδομένων του για έναν ή περισσότερους συγκεκριμένους σκοπούς, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης ή για τη συμμόρφωση με έννομη υποχρέωση του Υπευθύνου Επεξεργασίας που απορρέει από άλλο κανόνα δικαίου, γ) η επεξεργασία είναι απαραίτητη για την διαφύλαξη ζωτικού συμφέροντος ή για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας

ανατεθειμένης στον Υπεύθυνο Επεξεργασίας και τέλος, δ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο Υπεύθυνος Επεξεργασίας εκτός αν υποκείμενο είναι παιδί, περίπτωση στην οποία υπερισχύει το έννομο συμφέρον προστασίας του τέκνου. Η **διαφάνεια** εξασφαλίζεται μέσω της παροχής κάθε πληροφορίας και ανακοίνωσης σχετικά με την επεξεργασία με **συνοπτικό, διαφανή και κατανοητό τρόπο και σε εύκολα προσβάσιμη μορφή**. Για την παροχή πληροφόρησης ή την διατύπωση της ανακοίνωσης, ιδίως εάν πρόκειται για ενημέρωση ανηλίκων, πρέπει να γίνεται χρήση **σαφούς και απλής διατύπωσης**. Η πληροφορία πρέπει να δίνεται στο υποκείμενο των δικαιωμάτων εντός προθεσμίας ενός μήνα από την παραλαβή του σχετικού αιτήματός του (με δυνατότητα παράτασης για δύο μήνες) ενώ στην περίπτωση που η παροχή της πληροφορίας δεν είναι εφικτή, ο Υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο για την αδυναμία αυτή καθώς και να το πληροφορήσει για τη δυνατότητα υποβολής καταγγελίας στην αρμόδια εποπτική αρχή και για τη δυνατότητα άσκησης δικαστικής προσφυγής

- ✓ **Η αρχή του σκοπού** που εκπληρώνεται όταν η συλλογή και η επεξεργασία γίνονται με στόχο σαφή και καθορισμένο που δεν επιτρέπει την υποβολή των δεδομένων σε περαιτέρω επεξεργασία. Μόνη επιτρεπτή εξαίρεση συνιστά η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης που εξυπηρετούν το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας, ή στατιστικούς σκοπούς υπό τον όρο ότι οι χρησιμοποιούμενες μέθοδοι αποκλείουν την ταυτοποίηση των υποκειμένων των δεδομένων και παρέχουν τις κατάλληλες εγγυήσεις για την προστασία των δεδομένων τους.
- ✓ **Η αρχή ελαχιστοποίησης των δεδομένων** η οποία πρέπει να εφαρμόζεται τόσο στον όγκο των δεδομένων όσο και στη διάρκεια τήρησης αυτών και βάσει της οποίας τα δεδομένα που τηρούνται πρέπει να είναι κατάλληλα, συναφή και περιορισμένα στα απολύτως απαραίτητα αναφορικά με τους σκοπούς για τους οποίους εκτελείται η επεξεργασία.
- ✓ **Η αρχή της ακρίβειας** σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται ενώ το υποκείμενο θα πρέπει να έχει επαρκή ενημέρωση ως προς τα προσωπικά του δεδομένα τα οποία υφίστανται επεξεργασία. Παράλληλα, 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.

- ✓ **Η αρχή του περιορισμού της περιόδου αποθήκευσης,** δηλαδή την τήρηση των αρχείων των δεδομένων για όσο διάστημα χρειάζεται για την επίτευξη του σκοπού της επεξεργασίας. Εξαίρεση προβλέπεται στην περίπτωση κατά την οποία η επεξεργασία γίνεται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς και λαμβάνονται τα κατάλληλα οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.
- ✓ **Η αρχή της ακεραιότητας και εμπιστευτικότητας** που καλεί για την υποβολή των δεδομένων σε επεξεργασία κατά τρόπο ώστε να 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.
- ✓ **Η αρχή της αναλογικότητας** που επιβάλλει να υπάρχει συνάφεια ανάμεσα στα δεδομένα που τηρούνται και στο σκοπό για τον οποίο αυτά συλλέγονται, καθώς και να είναι τα δεδομένα αυτά πρόσφορα και αναγκαία για την εκπλήρωση του σκοπού αυτού. Με τον τρόπο αυτό, η αρχή της αναλογικότητας οδηγεί πρακτικά στην ελαχιστοποίηση των τηρούμενων δεδομένων, αφού το πιθανότερο είναι πως οι προϋποθέσεις αυτές δεν ισχύουν για το σύνολο των δεδομένων που συλλέγονται από τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία.
- ✓ **Η αρχή της λογοδοσίας** υπό την οποία ο Υπεύθυνος Επεξεργασίας και ο εκτελών την επεξεργασία φέρουν την ευθύνη να αποδείξουν όχι μόνο την συμμόρφωση στις υποχρεώσεις που θέτει ο Κανονισμός αλλά και την ετοιμότητά τους να συμμορφωθούν. Οι υποχρεώσεις τους δεν είναι προκαθορισμένες και σταθερές αλλά διαμορφώνονται ανάλογα με τον κίνδυνο που ενδέχεται να προκύψει από την επεξεργασία, όπως ο κίνδυνος αυτός εκτιμάται ήδη πριν την έναρξη της επεξεργασίας, βάσει της Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων.

Αυτό λοιπόν, το οποίο θα πρέπει να υπερτονιστεί στο σημείο αυτό είναι πως ο νέος κανονισμός επιβάλει ιδιαίτερα αυστηρές κυρώσεις στην περίπτωση της μη συμμόρφωσης, κυρίως διότι η διάχυση της πληροφορίας είναι ταχύτατη και οι υποχρεώσεις των υπευθύνων επεξεργασίας ιδιαίτερα αυξημένες. Η προ υπάρχουσα οδηγία, άφηνε το θέμα της θέσπισης πολιτικών στη διακριτική ευχέρεια των κρατών μελών γεγονός το οποίο οδηγούσε σε αποκλίσεις μεταξύ των κρατών σε ότι αφορά στην παραπάνω προσέγγιση. Αντίθετα, ο νέος κανονισμός, επιβάλλει ενιαίες και αυστηρά διοικητικές κυρώσεις. Έτσι λοιπόν, προβλέπεται

2% πρόστιμο για διοικητικές / γραφειοκρατικές παραλείψεις ενώ για υπαίτιες παραβάσεις προβλέπεται η δυνατότητα επιβολής προστίμου ίσου με το 4% του ετήσιου παγκόσμιου τζίρου της επιχείρησης(Bird&Bird, 2017).

Το άρθρο 84 του κανονισμού, προβλέπει για όλα τα κράτη – μέλη τη θέσπιση κυρώσεων ακόμη και της μορφής της φυλάκισης ή και κάθειρξης καθώς και χρηματικές ποινές που μπορεί να φτάσουν τις €300.000 (Σ Ε Β, 2018).

Σύμφωνα με τα οριζόμενα στον Κανονισμό, υπεύθυνος επεξεργασίας είναι κάθε επιχείρηση ή οργανισμός ανεξαρτήτως μεγέθους που συλλέγει και επεξεργάζεται προσωπικά δεδομένα για ίδιο λογαριασμό.

Στην περίπτωση που η επεξεργασία δεν εκτελείται από την ίδια αλλά γίνεται από κάποιο τρίτο μέρη για λογαριασμό της, το μέρος αυτό είτε πρόκειται για φυσικό είτε για νομικό πρόσωπο είναι ο «εκτελών την επεξεργασία» προς τον οποίο ο υπεύθυνος επεξεργασίας οφείλει να περιγράψει το σκοπό και τον τρόπο σύμφωνα με τον οποίο επιθυμεί να εκτελείται η επεξεργασία(Calder, 2016). Ως τρίτο μέρος νοείται επιχείρηση ή φυσικό πρόσωπο το οποίο δεν αποτελεί μέρος του οργανισμού του Υπεύθυνου επεξεργασίας, όπως οι εργαζόμενοι μιας επιχείρησης που, στο πλαίσιο της εργασίας τους επεξεργάζονται δεδομένα προσωπικού χαρακτήρα (Σ Ε Β, 2018).

Σημαντικό είναι να τονιστεί, ότι αποκλειστική ευθύνη του υπεύθυνου επεξεργασίας είναι η τήρηση των διατάξεων του κανονισμού αλλά και η εποπτεία των εκτελούντων, στους οποίους έχει αναθέσει την επεξεργασία, προκειμένου να διασφαλίζει το σύννομο των ενεργειών τους. Ωστόσο, βάσει της Οδηγίας για την επιβολή κυρώσεων και επιδίκαση αποζημίωσης στον υπεύθυνο επεξεργασίας απαιτούνταν να συντρέχουν σωρευτικά, οι ακόλουθες προϋποθέσεις (Υπουργείο Δικαιοσύνης, 2018):

- Συμπεριφορά (πράξη ή παράλειψη) που παραβιάζει τις διατάξεις του ν.2472/1997 ή (και) των κατ' εξουσιοδότηση αυτού κανονιστικών πράξεων της Αρχής
- Ηθική βλάβη
- Αιτιώδη συνάφεια μεταξύ της συμπεριφοράς και της ηθικής βλάβης»
- Υπαιτιότητα, ήτοι γνώση ή υπαίτια άγνοια, αφενός των περιστατικών που συνιστούν την παράβαση και αφετέρου της πιθανότητας να επέλθει η ηθική βλάβη.

Ο νέος κανονισμός από την άλλη, συνυπολογίζει το δόλο ή την αμέλεια στον υπολογισμό του προστίμου και άρα όταν αυτοί εντοπιστούν επιβάλλεται η επιβολή των κυρώσεων από την εποπτική αρχή. Επιπρόσθετα, ζητείται από τον υπεύθυνο επεξεργασίας, η αλλαγή της

φιλοσοφίας και της κουλτούρας του οργανισμού, ώστε να δημιουργηθούν σχέσεις άρρηκτης εμπιστοσύνης μεταξύ αυτού και των υποκειμένων.

Στο σημείο αυτό, κρίνεται άξιο αναφοράς το γεγονός ότι ο υπεύθυνος επεξεργασίας είναι και αυτός που θα ορίσει τις προθεσμίες που θα αφορούν στη διαγραφή των δεδομένων ή στην περιοδική επανεξέτασή τους όταν και εάν αυτό κρίνεται αναγκαίο.

Ο κύριος ρόλος του Υπεύθυνου Επεξεργασίας των Προσωπικών δεδομένων, δεν είναι η προστασία του ίδιου του οργανισμού στον οποίο απασχολείται, αλλά η προστασία των προσώπων τα δεδομένα των οποίων συλλέγονται και επεξεργάζονται από τον οργανισμό (Σ Ε Β, 2018).

Η υποχρέωση ορισμού ΥΠΔ ισχύει εφόσον συντρέχουν συγκεκριμένες προϋποθέσεις (Σ Ε Β, 2018).:

α) Ο Υπεύθυνος επεξεργασίας είναι Δημόσια αρχή ή φορέας, με την εξαίρεση των δικαστηρίων όταν αυτά ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα. Ο Κανονισμός δεν περιλαμβάνει ορισμό της έννοιας της Δημόσιας αρχής ή του δημόσιου φορέα, αντίθετα καταλείπεται στην σφαίρα της πρωτοβουλίας του εκάστοτε κράτους μέλους να προβεί στον προσδιορισμό αυτό.

β) Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας συνιστούν επεξεργασία που απαιτεί την τακτική και συστηματική παρακολούθηση των δεδομένων σε μεγάλη κλίμακα.«Βασικές δραστηριότητες» είναι εκείνες οι οποίες αποτελούν αναπόσπαστο κομμάτι για την επίτευξη των στόχων του υπευθύνου επεξεργασίας/ εκτελούντα την επεξεργασία.

γ) Οι βασικές δραστηριότητες του υπευθύνου συνιστούν μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων ή δεδομένων σχετικών με ποινικές καταδίκες και αδικήματα.

δ) Προβλέπεται από το δίκαιο κράτους-μέλους.

Στην Ελληνική Επικράτεια, αρμόδια για την προστασία των δεδομένων προσωπικού χαρακτήρα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή, η οποία ιδρύθηκε με το Νόμο 2472/1997 που ενσωμάτωνε την Ευρωπαϊκή Οδηγία 95/46/ΕΚ.

Σε Ευρωπαϊκό επίπεδο, ο κανονισμός προβλέπει τη σύσταση ενός ανεξάρτητου οργάνου, του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων το οποίο ως ανεξάρτητο όργανο Ένωσης, συμβάλλει στη συνεκτική εφαρμογή του Κανονισμού σε ολόκληρη την ΕΕ, μεταξύ άλλων παρέχοντας συμβουλές στην Επιτροπή, ιδίως για το επίπεδο προστασίας σε τρίτες χώρες ή σε διεθνείς οργανισμούς, και προωθώντας τη συνεργασία των εποπτικών αρχών σε ολόκληρη την ΕΕ (Καλαντζής , 2017).

Το Συμβούλιο απαρτίζεται από τον προϊστάμενο μίας εποπτικής Αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων ή τους αντίστοιχους εκπροσώπους τους, ενώ σε αυτήν προβλέπεται συμμετοχή εκπροσώπου της Επιτροπής. Αποφασίζει με απλή πλειοψηφία των μελών του.

Κύριο καθήκον του Συμβουλίου είναι η διασφάλιση της συνεκτικής εφαρμογής του Κανονισμού. Ειδικότερα, το Συμβούλιο ακολουθεί και διασφαλίζει την ορθή εφαρμογή του Κανονισμού, με την επιφύλαξη των καθηκόντων των εθνικών εποπτικών αρχών (Σ Ε Β, 2018).:

- Συμβουλεύει την Επιτροπή για κάθε ζήτημα σχετικό με την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ένωση, συμπεριλαμβανομένης κάθε προτεινόμενης τροποποίησης του Κανονισμού.
- Συμβουλεύει την Επιτροπή σχετικά με τον μορφότυπο και τις διαδικασίες για την ανταλλαγή πληροφοριών μεταξύ υπευθύνων επεξεργασίας, εκτελούντων την επεξεργασία και εποπτικών αρχών για τους δεσμευτικούς εταιρικούς κανόνες.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές σχετικά με τις διαδικασίες για τη διαγραφή συνδέσμων, αντιγράφων ή αναπαραγωγών δεδομένων προσωπικού χαρακτήρα από υπηρεσίες επικοινωνιών διαθέσιμες στο κοινό.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές, με σκοπό να ενθαρρύνει τη συνεκτική εφαρμογή του Κανονισμού.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για τον περαιτέρω προσδιορισμό των κριτηρίων και των προϋποθέσεων για τη λήψη αποφάσεων που βασίζονται σε κατάρτιση προφίλ
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές σχετικά με τη διαπίστωση των παραβιάσεων των δεδομένων προσωπικού χαρακτήρα και τον καθορισμό της δράσης του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές όσον αφορά στις συνθήκες υπό τις οποίες η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για τον περαιτέρω προσδιορισμό των κριτηρίων και των απαιτήσεων για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα που βασίζονται σε δεσμευτικούς εταιρικούς κανόνες που τηρούν οι υπεύθυνοι επεξεργασίας και δεσμευτικούς εταιρικούς κανόνες

που τηρούν οι υπεύθυνοι επεξεργασίας και των περαιτέρω αναγκαίων απαιτήσεων, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα των οικείων υποκειμένων των δεδομένων.

- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για τους σκοπούς του περαιτέρω προσδιορισμού των κριτηρίων και των απαιτήσεων για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα.
- Εκπονεί κατευθυντήριες γραμμές για τις εποπτικές αρχές όσον αφορά την εφαρμογή των μέτρων και τον καθορισμό διοικητικών προστίμων.
- Εξετάζει την πρακτική εφαρμογή των κατευθυντήριων γραμμών, των συστάσεων και των βέλτιστων πρακτικών που προαναφέρθηκαν για την εκπόνηση κοινών διαδικασιών.
- Ενθαρρύνει την κατάρτιση κωδίκων δεοντολογίας και τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων.
- Εκτελεί τη διαπίστευση των φορέων πιστοποίησης και την περιοδική επανεξέτασή της και τηρεί δημόσιο μητρώο των διαπιστευμένων φορέων.
- Προσδιορίζει τις απαιτήσεις προκειμένου για τη διαπίστευση των φορέων πιστοποίησης και γνωμοδοτεί στην Επιτροπή σχετικά με τις απαιτήσεις πιστοποίησης.
- Παρέχει στην Επιτροπή γνωμοδότηση για την εκτίμηση της επάρκειας του επιπέδου προστασίας σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένης της εκτίμησης του κατά πόσο μια τρίτη χώρα, ένα έδαφος ή ένας ή περισσότεροι συγκεκριμένοι τομείς στην εν λόγω τρίτη χώρα ή ένας διεθνής οργανισμός δεν διασφαλίζει πλέον επαρκές επίπεδο προστασίας. Για τον σκοπό αυτό, η Επιτροπή παρέχει στο Συμβούλιο όλη την απαραίτητη τεκμηρίωση, συμπεριλαμβανομένης της αλληλογραφίας με την κυβέρνηση της τρίτης χώρας, όσον αφορά την εν λόγω τρίτη χώρα, το έδαφος ή τον συγκεκριμένο τομέα ή τον διεθνή οργανισμό.
- Εκδίδει γνώμες για σχέδια αποφάσεων των εποπτικών αρχών δυνάμει του μηχανισμού συνεκτικότητας.
- Προωθεί τη συνεργασία και την αποτελεσματική διμερή και πολυμερή ανταλλαγή πληροφοριών και βέλτιστων πρακτικών μεταξύ των εποπτικών αρχών.
- Προωθεί κοινά προγράμματα κατάρτισης και διευκολύνει τις ανταλλαγές υπαλλήλων μεταξύ εποπτικών αρχών και, κατά περίπτωση, με τις εποπτικές αρχές τρίτων χωρών ή με διεθνείς οργανισμούς.

- Προωθεί την ανταλλαγή γνώσεων και τεκμηρίωσης σχετικά με τη νομοθεσία και την πρακτική στον τομέα της προστασίας δεδομένων με τις εποπτικές αρχές προστασίας δεδομένων ανά τον κόσμο.
- Γνωμοδοτεί επί των κωδίκων δεοντολογίας που εκπονούνται σε επίπεδο ΕΕ.
- Διατηρεί δημόσια προσβάσιμο ηλεκτρονικό μητρώο των αποφάσεων που λαμβάνονται από τις εποπτικές αρχές και τα δικαστήρια για ζητήματα που εξετάζονται στο πλαίσιο του μηχανισμού συνεκτικότητας.

3.2 Αποτύπωση μεθοδολογιών αποτίμησης αντικτύπου από απώλεια προστασίας ιδιωτικότητας (Data Protection Impact Assessment - DPIA)

Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων στο άρθρο 33 ορίζει ότι «…κάθε δημόσιος ή ιδιωτικός οργανισμός που επεξεργάζεται συγκεκριμένα προσωπικά δεδομένα, υποχρεούται να εκτελεί μια εκτίμηση για τις πιθανές επιπτώσεις των κινδύνων που ενδέχεται να προκύψουν από την επεξεργασία των δεδομένων αυτών» (Σασιάκος, Αναστασίου, & Τούντας, 2017). Παράλληλα, αυτός ορίζει την Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία των δεδομένων, (Data Protection Impact Assessment – DPIA) όμως πολύ περιληπτικά και χωρίς να ορίζει συγκεκριμένες γραμμές και να αφήνει περιθώρια διαμόρφωσης.

Όπως είναι αντιληπτό, η εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων αποτελεί μία διαδικασία που εκτελείται κατά το αρχικό στάδιο σχεδίασης όλων των εφαρμογών και πολιτικών που θα λάβουν χώρα σε έναν οργανισμό. Αποτέλεσμα αυτής, είναι φυσικά η σύνταξη μιας έκθεσης που θα παρουσιάζει όλα τις πτυχές της επεξεργασίας, την εκτίμηση των πιθανών κινδύνων και τα μέτρα ασφαλείας ώστε να αποφευχθούν οι ενδεχόμενοι κίνδυνοι (Σασιάκος, Αναστασίου, & Τούντας, 2017). Καθώς ο κανονισμός ορίζει την ύπαρξη και μιας αρμόδιας αρχής, η αρχή αυτή είναι υποχρεωμένη να ελέγξει την έκθεση και να κάνει εκτίμηση του κινδύνου σύμφωνα με τα όσα παρουσιάζει η επιχείρηση. Η DPIA πρέπει να θεωρείται ένα κομμάτι από μια ευρύτερη διαδικασία διαχείρισης κινδύνων (risk management) που οφείλει να εφαρμόζει ένας οργανισμός (European Commission – Directorate General Justice, 2012).

Οι Σιασικάκος, Αναστασίου και Τούντας, προτείνουν μία διαδικασία εκτέλεσης της εκτίμησης DPIAπου θα ακολουθεί τα παρακάτω βήματα (Σασιάκος, Αναστασίου, & Τούντας, 2017):

- Καθορισμός της ανάγκης για την διενέργεια της DPIA (Τι είδους προσωπικά δεδομένα επεξεργάζονται; Ποιος ο υπεύθυνος επεξεργασίας; Ενδέχεται να υπάρξουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα; Έχουν ληφθεί μέτρα προστασίας;)
- Προσδιορισμός της ομάδας εκτέλεσης της DPIA
- Αναγνώριση και περιγραφή της εφαρμογής / διαδικασίας (Περιγραφή του σχεδιασμού της εφαρμογής και των διεπαφών της με άλλα συστήματα και της διαδικασίας, της

ροής των δεδομένων, των εμπλεκόμενων χρηστών και των επιμέρους υποσυστημάτων της εφαρμογής)

- Σύσκεψη με τους εμπλεκόμενους (Άτομα από το εσωτερικό και εξωτερικό του οργανισμού επισημαίνουν τους κινδύνους που αφορούν το δικό τους πεδίο εξειδίκευσης)
- Αναγνώριση των σχετικών κινδύνων (Αναγνώριση των συνθηκών και των πιθανών κινδύνων που μπορεί να απειλήσουν τα προσωπικά δεδομένα των ατόμων και να επηρεάσουν την ιδιωτικότητά τους), διαχείριση των κινδύνων (Αξιολόγηση των ενδεχόμενων απειλών και των δυσμενών γεγονότων που έχουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα, Λήψη μέτρων αντιμετώπισης και ασφάλειας)
- Έλεγχος νομοθετικής συμμόρφωσης
- Τεκμηρίωση και ολοκλήρωση της σχετικής έκθεσης
- Εξωτερικός έλεγχος και ανασκόπηση.

Η DPIA, εκτιμάται πάντα πως θα έχει ένα πιθανό κόστος το οποίο φυσικά θα εξαρτάται από τους παρακάτω παράγοντες (Σασιάκος, Αναστασίου, & Τούντας, 2017):

- Μέγεθος της εκτίμησης
- Αυστηρότητα της νομοθεσίας
- Συμμετοχή των εμπλεκόμενων μερών,
- Πρόσληψη ειδικού στελέχους για την εκτέλεση της εκτίμησης

Εάν λοιπόν, ληφθούν υπόψη όλες οι παραπάνω παράμετροι, άμεσα η DPIA εισάγει για τον οργανισμό ένα σημαντικό κόστος γεγονός που καθιστά αμφίβολο το εάν για το κόστος αυτό η χρησιμότητά της καθίσταται αναγκαία. Βέβαια, σε καμία περίπτωση δε θα μπορούσε κανείς να αμφισβητήσει πως η DPIA εισάγει σημαντικά πλεονεκτήματα για έναν οργανισμό. Σύμφωνα λοιπόν με την European Commission – Directorate General Justice, 2012 αυτά διαχωρίζονται σε :

- Εσωτερικά:
  - Διαχείριση του κινδύνου (αναγνώριση και περιορισμός)
  - Αποφυγή κοστοβόρων επαναπροσδιορισμών της διαδικασίας επεξεργασίας αλλά και της ίδιας της εφαρμογής εάν από την αρχή έχουν προσδιοριστεί οι ενδεχόμενοι κίνδυνοι και απειλές
  - Αποφυγή επιβολής κυρώσεων αλλά και αποφυγή της διακοπής ή απαγόρευσης του εγχειρήματος από την αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων λόγω μη συμμόρφωσης στους υφιστάμενους κανονισμούς και στη νομοθεσία της Ε.Ε

- Βελτίωση της προστασίας των προσωπικών δεδομένων και της αποδοτικότητας της συγκεκριμένης υπηρεσίας
- Βελτίωση του τρόπου διαχείρισης των δεδομένων γνωρίζοντας τις πιθανές απειλές και αστοχίες
- Αύξηση της ασφάλειας του συστήματος όσον αφορά την προστασία των δεδομένων και των γενικότερων λειτουργιών του οργανισμού που βασίζονται σε αυτό
- Βελτίωση της τεχνογνωσίας σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριακών συστημάτων
  - Εξωτερικά:
- Ενίσχυση της αξιοπιστίας του οργανισμού από την πλευρά των εμπλεκόμενων μερών και προώθηση του e-government,
- Υπόδειξη συμμόρφωσης με την νομοθεσία περί προστασίας προσωπικών δεδομένων και επιβεβαίωση ότι η ασφάλεια λαμβάνεται σοβαρά υπόψη

Ο Κανονισμός για την προστασία των δεδομένων προσωπικού χαρακτήρα εισάγει μία μοναδική καινοτομία η οποία καταργεί τη γενική υποχρέωση του υπεύθυνου επεξεργασίας της γνωστοποίησης προς την αρχή ελέγχου. Έτσι λοιπόν, οι υπεύθυνοι επεξεργασίας δεν είναι πλέον υποχρεωμένοι ώστε να τηρούν αρχεία για κάθε δραστηριότητα επεξεργασίας, αλλά ούτε και οι εκτελούντες την επεξεργασία να τηρούν σχετικά αρχεία με κάθε μορφή επεξεργασίας που έχει πραγματοποιηθεί. Ακόμη, οι υπεύθυνοι επεξεργασίας δεν είναι υποχρεωμένοι ώστε να διενεργούν εκτίμηση αντικτύπου σε συγκεκριμένες κατηγορίες επεξεργασιών (Calder, 2016).

Η υποχρέωση της διενέργειας της DPIA, εισάγεται ως ένα μέτρο συμμόρφωσης προς τις διατάξεις του κανόνα, η οποία λαμβάνει πάντα υπόψη της την ύψιστη ανάγκη της αντιμετώπισης όλων των κινδύνων που ενδεχόμενα να προκύψουν κατά την επεξεργασία της πληροφορίας. Ο υπεύθυνος επεξεργασίας έχει λοιπόν την υποχρέωση, ώστε να αξιολογεί όλες εκείνες τις παραμέτρους που ενδεχόμενα να εισάγουν κίνδυνο ώστε να είναι πιο αποτελεσματική η προστασία των δεδομένων.

Ο υπεύθυνος επεξεργασίας, σύμφωνα με τον καινούριο κανονισμό οφείλει ώστε να διενεργήσει DPIA, ιδιαίτερα όταν η επεξεργασία γίνεται με τη χρήση νέων τεχνολογιών (Γιαννόπουλος, 2017). Η DPIA, σε πολλές περιπτώσεις ενδέχεται να μην αφορά μεμονωμένη επεξεργασία αλλά ένα σύνολο πράξεων επεξεργασίας για τις οποίες εισάγεται ο ίδιος κίνδυνος.

Εκτελούμενη κατ' αρχήν από υπεύθυνο επεξεργασίας δεδομένων, η DPIAαποσκοπεί στο να δημιουργηθεί και να αποδεχθεί τόσο η εφαρμογή των αρχών για την προστασία της ιδιωτικότητας όσο και να γνωστοποιείται στα υποκείμενα ο έλεγχος των προσωπικών τους δεδομένων. Μάλιστα, προορίζεται για τους υπεύθυνους εκείνους των δεδομένων που στοχεύουν στο να αποδείξουν εμπράκτως μία συμμόρφωση ως προς τα μέτρα που επέλεξαν αλλά και για τους παρόχους υπηρεσιών που και αυτοί με της σειρά τους επιθυμούν να επιδείξουν σεβασμό ως προς την αρχή της ιδιωτικότητας. Ο καινούριος κανονισμός λοιπόν, είναι χρήσιμος προς όλους εκείνους τους ενδιαφερόμενους φορείς που εμπλέκονται στη διαδικασία της επεξεργασίας των δεδομένων με όποια μορφή και εάν λαμβάνει αυτή. Ειδικότερα σε (ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων, 2016):

❑ Αρχές λήψης αποφάσεων οι οποίες αναθέτουν και επικυρώνουν τη δημιουργία νέων επεξεργασιών προσωπικών δεδομένων ή προϊόντων

❑ Ιδιοκτήτες έργων, οι οποίοι πρέπει να διενεργούν αξιολόγηση των κινδύνων για τα συστήματά τους και να ορίζουν τους στόχους ασφαλείας

❑ Κύριους εργολάβους, οι οποίοι πρέπει να προτείνουν λύσεις για την αντιμετώπιση των κινδύνων σύμφωνα με τους στόχους που προσδιορίζονται από τους ιδιοκτήτες έργων

❑ Υπεύθυνους προστασίας δεδομένων (ΥΠΔ), οι οποίοι πρέπει να υποστηρίζουν τους ιδιοκτήτες έργων και τις αρχές λήψης αποφάσεων στον τομέα της προστασίας των προσωπικών δεδομένων

❑ Υπεύθυνους ασφάλειας κεντρικών συστημάτων πληροφορικής (ΥΑΚΠ – CISO), οι οποίοι πρέπει να υποστηρίξουν τους ιδιοκτήτες έργων στον τομέα της ασφάλειας των πληροφοριών (IS).

Ο GDPR, θέλοντας να υπερτονίσει τη σημαντικότητα των επεξεργασιών και των κινδύνων που εισάγονται σε αυτές, καθιστά την DPIAυποχρεωτική στους παρακάτω τρεις τύπους επεξεργασιών (ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων, 2016):

1. Της συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών των υποκειμένων, που βασίζεται σε αυτοματοποιημένη επεξεργασία (συμπεριλαμβανομένης της τεχνικής profiling) και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα για τα υποκείμενα αυτά ή τα επηρεάζουν σε σημαντικό βαθμό
2. Της μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παρ. 1 ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 (δηλαδή, σχετικών με ευαίσθητα δεδομένα προσωπικού χαρακτήρα)

3. Της συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

Πέραν των παραπάνω τύπων επεξεργασίας, κάθε αρχή προστασίας δεδομένων προσωπικού χαρακτήρα, οφείλει να δημοσιοποιεί έναν κατάλογο στον οποίο να συμπεριλαμβάνονται οι τύποι επεξεργασίας των δεδομένων οι οποίοι υπόκεινται στην υποχρέωση ώστε να διενεργείται η DPIA. Τόσο ο κατάλογος, με τους τύπους επεξεργασίας για τους οποίους απαιτείται η διενέργεια DPIA, όσο και ο κατάλογος με εκείνους που εξαιρούνται από τη διενέργεια DPIA, ανακοινώνονται από την αρμόδια αρχή προστασίας δεδομένων προσωπικού χαρακτήρα στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (European Union, 2017).

Το ελάχιστο περιεχόμενο της DPIA, που διενεργείται υποχρεωτικά σύμφωνα με τον νέο κανονισμό συνίσταται σε (ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων, 2016):

1. *Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών αυτών, καθώς και του εννόμου συμφέροντος που επιδιώκει, κατά περίπτωση, ο υπεύθυνος επεξεργασίας*
2. *Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς τους*
3. *Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων*
4. *Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς το ΓΚΠΔ, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα τόσο των υποκειμένων των δεδομένων όσο και άλλων ενδιαφερόμενων προσώπων*

Ο νέος κανονισμός, εισάγει μία ακόμη καινοτομία σχετικά με την DPIA, σύμφωνα με την οποία όλοι οι υπεύθυνοι επεξεργασίας αλλά και οι εκτελούντες την εργασία οφείλουν να ορίσουν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer–DPO). Η θέση και τα καθήκοντα των DPO προβλέπονται ρητά στο νέο κανόνα, καθιστώντας το θεσμό ως μία από τις σημαντικότερες εγγυήσεις για τη διασφάλιση της προστασίας των υποκειμένων των δεδομένων προσωπικού χαρακτήρα.

Ο κανονισμός, θεσπίζει ρητά την εμπλοκή του DPO στη διενέργεια DPIA, σε δύο διατάξεις (ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων, 2016):

(α) στο άρθρο 35 παρ. 2 θεσπίζεται ρητά η υποχρέωση για τον υπεύθυνο επεξεργασίας να ζητεί τη γνώμη του DPO, εφόσον αυτός έχει οριστεί, κατά τη διενέργεια DPIA σχετικά με την προστασία δεδομένων

(β) στο άρθρο 39 παρ. 2 θεσπίζεται ρητά, ανάμεσα στα καθήκοντα του DPO, και εκείνο του να «παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και [να] παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35».

Όπως είναι αντιληπτό η DPIA, αποτελεί το μέσο εκείνο με το οποίο θα συντελεστούν όλες οι συμμορφώσεις προς το γενικό κανονισμό. Αποτελεί επίσης αυτή, το τεχνικό και νομικό εργαλείο με το οποίο θα διασφαλιστεί ουσιαστικά η προστασία των προσώπων από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

HDPIA διενεργείται πάνω σε δύο βασικούς πυλώνες ιδιαίτερα σημαντικούς και καίριας σημασίας σε κάθε περίπτωση. Αφενός, βασίζεται στα θεμελιώδη δικαιώματα του ανθρώπου τα οποία σε κάθε περίπτωση είναι μια διαπραγματεύσιμα και ιδιαίτερα σοβαρά και αφετέρου στη διαχείριση οποιουδήποτε κινδύνου προκύψει για την ιδιωτική ζωή των υποκειμένων (Bird & Bird, 2017). Η μέθοδος αυτή, καταβάλλει κάθε προσπάθεια και επιβάλλει τα μέτρα εκείνα για την προστασία των προσωπικών δεδομένων και την ακεραιότητα αυτών. Άρα λοιπόν, για να διενεργηθεί μια DPIA, θα πρέπει αρχικά να καθοριστούν οι περιστάσεις και λόγου της επεξεργασίας των δεδομένων και στη συνέχεια να παρουσιασθούν και να αναλυθούν τα μέτρα εκείνα τα οποία εγγυώνται την σε κάθε περίπτωση εξασφάλιση και προστασία των δικαιωμάτων των υποκειμένων. Επιπρόσθετα, η DPIA, είναι αυτή η οποία και θα αξιολογήσει όλους εκείνους τους κινδύνους που προκύπτουν και αφορούν άμεσα την ασφάλεια των δεδομένων και την ίδια στιγμή θα προτείνει τους ενδεδειγμένους τρόπους αντιμετώπισης (Μήτρου, 2017).

Πρόκειται λοιπόν, για μία διαδικασία η οποία συνεχώς βελτιώνεται έως ότου φτάσει στο σημείο εκείνο όπου το σύστημα προστασίας θα είναι αποδεκτό και θα επικαιροποιείται καθώς με την πάροδο του χρόνου προκύπτουν νέοι κίνδυνοι. Η όποια προσέγγιση, καλό θα είναι να υλοποιείται τη στιγμή που θα σχεδιάζεται και η επεξεργασία των δεδομένων και όχι σε ύστερο διάστημα καθώς θα εισάγει κόστος αλλά και αμφισβήτηση σχετικά με τις επιλογές που έχουν γίνει. Οι κίνδυνοι, θα πρέπει να μελετώνται λεπτομερώς και να καταγράφεται η όποια πιθανή επίπτωση στην ιδιωτικότητα από την εισαγωγή κινδύνου. Ακόμη, θα πρέπει σε κάθε περίπτωση να εκτιμάται η σοβαρότητα του κάθε κινδύνου αλλά και ο επιζήμιος χαρακτήρας αυτού καθώς τα μέτρα που θα ληφθούν ενδέχεται με βάση το εν λόγω κριτήριο να χρειάζεται να τροποποιηθούν (Μήτρου, 2017). Τέλος, θα πρέπει σε κάθε περίπτωση να μελετάται η πιθανότητα του να συμβεί ο κάθε κίνδυνος και αυτός να εξετάζεται ανάλογα και να λαμβάνει ανάλογο χώρο στην DPIA.

Για να επικυρωθεί η μέθοδος αυτή, θα πρέπει αρχικά να γίνει η παρουσίασή της, δηλαδή η παρουσίαση των μέτρων που έχουν επιλεγεί τόσο για να υπάρχει συμμόρφωση προς τις αρχές όσο και για της συμβολή στην ασφάλεια των δεδομένων, και έπειτα να χαρτογραφηθούν οι κίνδυνοι ανάλογα πάντα με τη σοβαρότητα και την πιθανότητα εμφάνισής τους. Στη συνέχεια, θα πρέπει να καταρτιστεί το σχέδιο δράσης, και για κάθε μέτρο να καθοριστεί ο υπεύθυνος υλοποίησής του.

Όταν τα επιλεγμένα μέτρα, οι υπολειπόμενοι κίνδυνοι αλλά και το σχέδιο δράσης θα είναι αποδεκτά, τότε η DPIA θεωρείται επικυρωμένη. Στον παρακάτω πίνακα, παρουσιάζονται αναλυτικά τα βήματα της DPIA, όπως αυτά ορίζονται από τα άρθρα του κανονισμού.

Κριτήρια των [Κατευθυντήριων Γραμμών της OE29]	**Σύνοψη**	**Κεφάλαιο σε αυτόν τον οδηγό**
Παρέχεται συστηματική περιγραφή της επεξεργασίας (άρθρο 35 παράγραφος 7 στοιχείο α): - λαμβάνεται υπόψη η φύση, το πεδίο εφαρμογής, οι περιστάσεις και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)· - καταγράφονται τα προσωπικά δεδομένα, οι παραλήπτες και η περίοδος για την οποία θα αποθηκεύονται τα προσωπικά δεδομένα· - παρέχεται λειτουργική περιγραφή της διαδικασίας της επεξεργασίας· - εντοπίζονται τα στοιχεία στα οποία βασίζονται τα προσωπικά δεδομένα (υλισμικό, λογισμικό, δίκτυα, άνθρωποι, χαρτί ή κανάλια μετάδοσης έγχαρτων εγγράφων)· - λαμβάνεται υπόψη η συμμόρφωση με τους εγκεκριμένους κώδικες δεοντολογίας (Άρθρο 35 παράγραφος 8).	☑	1. Μελέτη των περιστάσεων
Αξιολογείται η αναγκαιότητα και η αναλογικότητα (Άρθρο 35 παράγραφος 7 στοιχείο β): - καθορίζονται τα μέτρα που προβλέπονται για τη συμμόρφωση με τον Κανονισμό (Άρθρο 35 παράγραφος 7 στοιχείο δ και αιτιολογική σκέψη 90), λαμβάνοντας υπόψη: - τα μέτρα που συμβάλλουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας με βάση: - καθορισμένους, ρητούς και νόμιμους σκοπούς (Άρθρο 5 παράγραφος 1 στοιχείο β)· - τη νομιμότητα της επεξεργασίας (Άρθρο 6)· - προσωπικά δεδομένα κατάλληλα, συναφή και περιορισμένα στο αναγκαίο (Άρθρο 5 παράγραφος 1 στοιχείο γ)· - περιορισμένη διάρκεια αποθήκευσης (Άρθρο 5 παράγραφος 1 στοιχείο ε)· - μέτρα που συμβάλλουν στα δικαιώματα των υποκειμένων των δεδομένων: - πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (Άρθρα 12, 13 και 14)· - δικαιώματα πρόσβασης και φορητότητας (Άρθρα 15 και 20)· - δικαιώματα διόρθωσης και διαγραφής (Άρθρα 16 και 17)· - δικαιώματα εναντίωσης και περιορισμού της επεξεργασίας (Άρθρα 16 και 21)· - εκτελούντες την επεξεργασία (Άρθρο 28)· - εγγυήσεις που αφορούν στις διεθνείς διαβιβάσεις (Κεφάλαιο V).	☑	2. Μελέτη των θεμελιωδών αρχών
Γίνεται διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (άρθρο 35 παράγραφος 7 στοιχείο γ): - αξιολογούνται η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (βλέπε αιτιολογική σκέψη 84) ή, ειδικότερα, για κάθε κίνδυνο (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων) από την οπτική γωνία των υποκειμένων των δεδομένων: - λαμβάνονται υπόψη οι πηγές κινδύνου (αιτιολογική σκέψη 90)· - προσδιορίζονται οι πιθανές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περίπτωση αθέμιτης πρόσβασης, ανεπιθύμητης τροποποίησης και εξαφάνισης δεδομένων· - εντοπίζονται απειλές που θα μπορούσαν να οδηγήσουν σε αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων· - εκτιμάται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90)· - καθορίζονται τα μέτρα που προβλέπονται για την αντιμετώπιση αυτών των κινδύνων (Άρθρο 35 παράγραφος 7 στοιχείο δ και αιτιολογική σκέψη 90).	☑	3. Μελέτη των κινδύνων ασφάλειας δεδομένων
Συμμετέχουν τα ενδιαφερόμενα μέρη: - ζητείται η συμβουλή του ΥΠΔ (Άρθρο 35 παράγραφος 2)· - ζητούνται οι απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους (Άρθρο 35 παράγραφος 9).	☑	4. Επικύρωση της PIA

3.3 Η Μέθοδος CNIL

Η μέθοδος DPIA που θα χρησιμοποιηθεί στην παρούσα διπλωματική είναι αυτή η οποία προτείνεται από τη Γαλλική Εθνική Επιτροπή για την Πληροφορική και τις Ελευθερίες, (Commission Nationale del' Informatique et des Libertés – CNIL), και αποτελεί μία ιδιαίτερα σοβαρή προσπάθεια υλοποίησης του κανόνα στο τομέα της ψηφιακής δικαιοσύνης. Στόχος της προτεινόμενης αυτής μεθόδου, είναι να διευκολύνει τους υπεύθυνους προστασίας των δεδομένων ώστε αυτή να μπορούν να αποδείξουν συμμόρφωση με το γενικότερο κανόνα, εκπονώντας πάντα σύμφωνα με τα όσα αυτός πρεσβεύει μεθόδους DPIA(CNIL, 2020).

Το λογισμικό προσφέρεται σε όλες τις γλώσσες της Ευρωπαϊκής Ένωσης με εκδόσεις αυτού να διευκολύνουν την εγκατάσταση, όποιο λειτουργικό σύστημα και εάν χρησιμοποιεί ο χρήστης. Σύμφωνα με τη CNIL, από την αρχή της εφαρμογής του Γενικού Κανονισμού, το ανοιχτό λογισμικό DPIA, έχει βοηθήσει, μεταξύ άλλων, 24.500 φορείς, Αρχές Προστασίας Δεδομένων στην Ευρώπη, να ορίσουν υπεύθυνους προστασίας δεδομένων, με την Γαλλική Αρχή να έχει δεχτεί πάνω από 600 ειδοποιήσεις παραβίασης δεδομένων που αφορούν περίπου 15 εκατομμύρια άτομα, ενώ 3 εκατομμύρια επισκέψεις καταγράφηκαν στο site της, με 150.000 downloads της εφαρμογής. Για τον παραπάνω λόγο, η CNILέχει λάβει ανάλογα βραβεία σε συνέδρια σχετικά με την ασφάλεια σε όλη την Ευρώπη(CNIL, 2020).

Το εν λόγω λογισμικό, περιλαμβάνει τρείς διαφορετικές κατηγορίες οδηγιών που τελικά καταλήγουν σε ένα πεδίο διασυνδεδεμένων αντικειμένων. Οι οδηγίες λοιπόν αυτές περιλαμβάνουν (CNIL, 2020):

1. ***Γνωσιακή Βάση (Knowledge Base) :*** Η βάση αυτή περιέχει όλες τις τεχνικές και νομικές γνώσεις που απαιτούνται και αποτελεί ένα χρήσιμο εργαλείο που εξασφαλίζει τόσο τη νομιμότητα της διαδικασίας όσο και τα δικαιώματα των υποκειμένων των δεδομένων τα οποία χρησιμοποιούντα καθ όλο το σχεδιασμό της DPIA. Ειδικότερα σε αυτή περιλαμβάνονται βάσεις γνώσης που αφορούν την τυπολογία των προσωπικών δεδομένων τα οποία διαχωρίζονται σε συνηθισμένα, προσωπικά και ευαίσθητα. Οι κατηγορίες στις οποίες διαχωρίζονται τα προσωπικά δεδομένα είναι οι παρακάτω :
    - Αστική κατάσταση, ταυτότητα, στοιχεία ταυτότητας
    - Προσωπική ζωή (συνήθειες διαβίωσης, οικογενειακή κατάσταση - χωρίς ευαίσθητα ή επικίνδυνα δεδομένα)

- Επαγγελματική ζωή (βιογραφικό σημείωμα, εκπαίδευση και επαγγελματική κατάρτιση)
- Οικονομικές και χρηματοοικονομικές πληροφορίες (εισόδημα, οικονομική κατάσταση, φορολογική κατάσταση)
- Δεδομένα σύνδεσης (διευθύνσεις IP, αρχεία καταγραφής συμβάντων)
- Δεδομένα τοποθεσίας (ταξίδια, δεδομένα GPS, δεδομένα GSM)
- Αριθμός κοινωνικής ασφάλισης
- Βιομετρικά δεδομένα
- Δεδομένα τραπεζών
- Φιλοσοφικές, πολιτικές, θρησκευτικές και συνδικαλιστικές απόψεις, σεξουαλική ζωή, δεδομένα για την υγεία, φυλετική ή εθνοτική καταγωγή.
- Αδικήματα, καταδίκες, ποινικό μητρώο

Οι κίνδυνοι που ελλοχεύουν για τα προσωπικά δεδομένα, συνήθως προέρχονται είτε από εσωτερικές όπως το οι εργαζόμενοι, οι διαχειριστές, και οι διευθυντές είτε εξωτερικές όπως οι παραλήπτες προσωπικών δεδομένων, οι πάροχοι υπηρεσιών, οι επισκέπτες κλπ ανθρώπινες πηγές(CNIL, 2020). Σε πολλές περιπτώσεις, άμεσα υπεύθυνος για τον κίνδυνο των δεδομένων προσωπικού χαρακτήρα δεν είναι ο ανθρώπινος παράγοντας, αλλά πηγές όπως τα κακόβουλα λογιστικά ή οι φυσικές καταστροφές.

Το κάθε συμβάν, κρίνεται εάν είναι εξαιρετικά επικίνδυνο ή όχι ανάλογα πάντα με τις συνέπειες που θα επιφέρει όταν συμβεί. Έτσι λοιπόν, οποιαδήποτε αθέμιτη σύμβαση σε προσωπικά δεδομένα μπορεί απλά να δώσει πρόσβαση σε ανθρώπους που δε χρειάζεται να τα γνωρίζουν, να δώσει αυτούς το δικαίωμα της αντιγραφής και της αποθήκευσής τους, αλλά και να διευκολύνει την περαιτέρω ανακατανομή τους χωρίς να υπάρχει κανένας απολύτως έλεγχος σε αυτό(CNIL, 2020). Δυστυχώς, εντός των κινδύνων συμπεριλαμβάνεται και αυτή της χρήσης των δεδομένων για σκοπούς κακόβουλους ή εμπορία αυτών με στόχο να επιτευχθεί ακριβώς αυτό το αποτέλεσμα. Επιπρόσθετα, δύναται φυσικά και η κακόβουλη επεξεργασία των δεδομένων με τρόπο τέτοιο ώστε να προκληθούν σφάλματα και σοβαρές δυσλειτουργίες σε αυτά. Το σημαντικότερο όλων βέβαια είναι η εξαφάνιση αυτών καθώς κανείς δεν είναι σε θέση να γνωρίζει εάν έχουν υποκλαπεί ή εάν έχουν διαγραφεί.

Το μέγεθος ενός κινδύνου φυσικά συνδέεται άρρηκτα με τη σοβαρότητα που αυτός αντιπροσωπεύει. Εκτιμάται, κατ' αρχάς, όσο αφορά την έκταση των δυνητικών επιπτώσεων στα πρόσωπα στα οποία αναφέρονται τα δεδομένα, λαμβάνοντας υπόψη υπάρχοντες, προγραμματισμένους ή συμπληρωματικούς ελέγχους. Εντός αυτού, εντάσσεται και η

πιθανότητα που αντιπροσωπεύει τη σκοπιμότητα ενός κινδύνου να συμβεί. Η πλέον χρησιμοποιούμενη κλίμακα εκτίμησης της πιθανότητας εμφάνισης των απειλών είναι η παρακάτω(CNIL, 2020) :

1. Αμελητέα: δε φαίνονται οι επιλεγμένες πηγές κινδύνου να υλοποιούν την απειλή.

2. Περιορισμένη: φαίνεται δύσκολο να υλοποιηθεί η απειλή.

3. Σημαντική: φαίνεται ότι μπορεί να υλοποιηθεί η απειλή.

4. Μέγιστη: φαίνεται εξαιρετικά εύκολο να υλοποιηθεί η απειλή.

Έτσι λοιπόν, προσδιορίζεται το επίπεδο του κινδύνου και το επίπεδο πιθανότητας να συμβεί αυτός με τη συμπερίληψη πρόσθετων παραγόντων όπως(CNIL, 2020) :

• Το άνοιγμα στο Διαδίκτυο ή σε κλειστό σύστημα.

• Οι ανταλλαγές δεδομένων με ξένες χώρες ή όχι.

• Οι διασυνδέσεις με άλλα συστήματα ή χωρίς διασύνδεση.

• Η ετερογένεια ή ομοιογένεια του συστήματος.

• Η μεταβλητότητα ή σταθερότητα του συστήματος.

• Η εικόνα της οργάνωσης.

Με στόχο να προστατευθούν με κάθε τρόπο τα δεδομένα προσωπικού χαρακτήρα, χρησιμοποιούνται διάφορες τεχνικές που βασίζονται κυρίως σε μεθόδους της πληροφορικής. Μία από αυτές είναι η ανωνυμία που αποσκοπεί στην κατάργηση των χαρακτηριστικών αναγνώρισης από τα προσωπικά δεδομένα και στην εφαρμογή πρακτικών τέτοιων που οφείλουν να ακολουθούνται σε κάθε περίπτωση που η μέθοδος αυτή υλοποιηθεί. Ιδιαίτερα χρήσιμη είναι και η τεχνική της αρχειοθέτησης, η οποία ορίζει πως θα πρέπει να αρχειοθετούνται και να διαχειρίζονται τα ηλεκτρονικά αρχεία που περιέχουν τα προσωπικά εκείνα δεδομένα που θα πρέπει να προστατευθούν. Οι σημαντικότερες πρακτικές που θα πρέπει να ακολουθούνται είναι(CNIL, 2020) :

i. Επιβεβαίωση ότι έχουν οριστεί οι διαδικασίες διαχείρισης αρχείων όπως ο διαχωρισμός της μεταφοράς, της αποθήκευσης, της διαχείρισης περιγραφικών δεδομένων, των διαδικασιών διαβούλευσης - επικοινωνίας και της διοίκησης, σε σχέση με τα γραφεία προέλευσης, την τεχνολογική και νομική παρακολούθηση αλλά και την αναβάθμιση μέσων και μορφών.

ii. Επιβεβαίωση ότι έχουν αναγνωριστεί οι ρόλοι αρχειοθέτησης, όπως ο διαχωρισμός των πηγών προέλευσης (γραφεία), οι μεταβιβάσιμες υπηρεσίες, οι αρχές αρχειοθέτησης (υπεύθυνες για τη συντήρηση) και οι οργανισμοί επιθεώρησης (ασκώντας τον επιστημονικό και τεχνικό έλεγχο των δημόσιων αρχείων).

iii. Επιβεβαίωση ότι τα μέτρα μπορούν να εξασφαλίσουν, εάν είναι αναγκαίο, τον προσδιορισμό και την εξακρίβωση της προέλευσης των αρχείων, την ακεραιότητα, τη σαφήνεια, την αναγνωσιμότητα, τη διαθεσιμότητα και την προσβασιμότητα των αρχείων, πόσο χρόνο πρέπει να διατηρούνται τα αρχεία και την ιχνηλασιμότητα των εργασιών σχετικά με τα αρχεία (συμπεριλαμβανομένης της μεταφοράς, της διαβούλευσης, της μετανάστευσης, της διαγραφής κ.λ.π.) και να λάβουν πρόσθετα μέτρα, εάν αυτό δεν συμβαίνει.

iv. Προσδιορισμός των μεθόδων προστασίας της εμπιστευτικότητας των αρχειοθετημένων προσωπικών δεδομένων, βάσει των εντοπισθέντων κινδύνων. Συστηματική κρυπτογράφηση των ευαίσθητων δεδομένων.

v. Επιβεβαίωση ότι οι αρχές αρχειοθέτησης διαθέτουν πολιτική αρχειοθέτησης και, ειδικότερα, εάν το έγγραφο τεκμηριώνει επισήμως τους νομικούς, λειτουργικούς και τεχνικούς περιορισμούς που πρέπει να τηρούν οι διάφοροι ενδιαφερόμενοι ώστε η ηλεκτρονική αρχειοθέτησή του να μπορεί να θεωρηθεί αξιόπιστη και μόνιμη.

vi. Επιβεβαίωση ύπαρξης δήλωσης πρακτικών αρχειοθέτησης, εάν δηλαδή το έγγραφο περιγράφει όλες τις διαδικασίες που έχουν τεθεί για την επίτευξη των στόχων που τίθενται στην πολιτική αρχειοθέτησης.

Σε πληθώρα περιπτώσεων, χρησιμοποιείται ο ιδιαίτερα ευφυής αλγόριθμος της κρυπτογράφησης που έχει ως στόχο να καταστήσει τα δεδομένα ακατανόητα και απροσπέλαστα από όποιον τα προσεγγίσει. Καλό είναι στην περίπτωση αυτή, να προσδιορίζονται τα δεδομένα που θα πρέπει να κρυπτογραφηθούν και στη συνέχεια και να επιλέγεται ο ανάλογος αλγόριθμος που θα χρησιμοποιηθεί με βάση πάντα τους κινδύνους που αναμένεται να αντιμετωπιστούν.

Σε κάθε περίπτωση, θα πρέπει να υφίσταται πάντα ένας φυσικός έλεγχος πρόσβασης καθώς είναι ο μόνος που εμποδίζει τη φυσική πρόσβαση σε μη εξουσιοδοτημένα πρόσωπα μέσω της (CNIL, 2020):

- Κατηγοριοποίησης των χώρων των κτιρίων ανάλογα με το πόσο ευάλωτοι είναι, με σκοπό την οριοθέτηση περιοχών προσιτών στο κοινό.
- Επιλογής μεθόδων πιστοποίησης των υπαλλήλων.
- Καθιέρωσης ελέγχου ταυτότητας επισκεπτών.
- Ορισμού ενεργειών που πρέπει να ακολουθούνται σε περίπτωση που αποτύχει ο έλεγχος ταυτότητας (η ταυτότητα δεν μπορεί να επιβεβαιωθεί ή έλλειψη εξουσιοδότησης για την είσοδο σε μια περιοχή ασφαλείας), κάτι που συνεπάγεται την άρνηση εισόδου στον επισκέπτη και την ειδοποίηση του υπεύθυνου ασφαλείας.
- Τήρησης αρχείου πρόσβασης με καταγραφή της ταυτότητας των επισκεπτών, ημερομηνία και ώρα άφιξης και αναχώρησης.
- Εγκατάστασης συστήματος προειδοποίησης, σε ιδιαίτερα ευαίσθητες περιοχές, όπου διατηρούνται ή επεξεργάζονται δεδομένα (computer room, αρχείο).

Καθώς σε κάθε DPIAσυμπεριλαμβάνεται και ένας σημαντικός αριθμός συσκευών που ελέγχονται αποκλειστικά από ανθρώπους, σημαντικό είναι να περιοριστεί η πρόσβαση σε όλους αυτούς οι οποίοι δεν είναι εξουσιοδοτημένοι και δε θα έπρεπε να έχουν πρόσβαση σε δεδομένα όπως προφίλ χρηστών ή και πολιτικές των κωδικών πρόσβασης(CNIL, 2020).

Οι χρήστες που θα έχουν πρόσβαση σε προσωπικά δεδομένα θα πρέπει να έχουν συγκεκριμένα προφίλ τα οποία θα προστατεύονται με πολλούς και ποικίλους τρόπους. Αφενός, θα πρέπει να διαχωριστούν οι τομείς ευθύνης που θα έχει ο κάθε χρήστης έτσι ώστε να περιορίζεται με κάθε τρόπο και η πρόσβαση σε συγκεκριμένα ιδιαίτερα ευαίσθητα δεδομένα. Επίσης, η πρόσβαση θα πρέπει να γίνεται με τη χρήση ενός μοναδικού και μόνο αναγνωριστικού που θα δίνει δικαιώματα στο χρήστη αλλά και την ίδια στιγμή θα καταγράφει τις δραστηριότητες αυτού. Ακόμη, ο αριθμός των χρηστών που θα έχουν πρόσβαση στα δεδομένα θα πρέπει να είναι και αυτός περιορισμένος και ακόμη πιο περιορισμένο των αριθμό αυτών που θα έχουν δικαιώματα διαχειριστή στη συσκευή.

Είναι αντιληπτό πως σε κάθε περίπτωση πρόσβασης ανθρώπων σε προσωπικά δεδομένα θα πρέπει να ακολουθείται πρωτόκολλο το οποίο θα διασφαλίζεται είτε με χρήση κωδικού πρόσβασης εάν οι κίνδυνοι δεν είναι ιδιαίτερα αυξημένοι ή με χρήση κωδικού που θα αλλάζει κάθε φορά λόγω υψηλών κινδύνων. Επιπρόσθετα, σε περίπτωση που ο έλεγχος ταυτότητας αποτύχει, ενδείκνυται να αποκλείεται ο λογαριασμός ή να αυξάνεται ο χρόνος αναμονής μεταξύ προσπαθειών σύνδεσης και ταυτόχρονα οι ενέργειες αυτές να καταγράφονται σε ανάλογο log file (CNIL, 2020). Συνίσταται μάλιστα, η διαδικασία της δεύτερης επαλήθευσης

ταυτότητας για την απόκτηση της πρόσβασης σε εφαρμογές με ευαίσθητα δεδομένα οι οποίες βρίσκονται σε περιβάλλοντα με όχι επαρκή ασφάλεια.

Για να διασφαλιστεί σε κάθε περίπτωση η ακεραιότητα των δεδομένων αλλά και για να μειωθεί η πιθανότητα των κινδύνων, θα πρέπει τα δεδομένα να μη διατηρούνται πέραν του αναγκαίου χρονικού διαστήματος. Οι συνηθέστερες πρακτικές ώστε να επιτευχθεί αυτό είναι αφενός ο καθορισμός της περιορισμένης χρονικής διάρκειας αποθήκευσης και αφετέρου η δημιουργία ενός αυτόματου μηχανισμού ώστε να εκτελείται πλήρης έλεγχος κατά την επεξεργασία των δεδομένων(CNIL, 2020). Επιπρόσθετα, κρίνεται η ανάπτυξης μιας διαδικασίας τέτοιας πλήρους διαγραφής των δεδομένων αλλά και των ιχνών αυτών αμέσως μετά τη λήξη της περιόδου αποθήκευσης.

Σε πολλές περιπτώσεις, οι κίνδυνοι για τα δεδομένα ενδέχεται να μην προέρχονται από τον ίδιο τον άνθρωπο αλλά από το περιβάλλον και έτσι καλή θα ήταν η αποθήκευση επικίνδυνων υλικών συμπεριλαμβανομένων των εύφλεκτων, διαβρωτικών, εκρηκτικών και υγρών αντικειμένων, σε κατάλληλες περιοχές αποθήκευσης και σε ασφαλή απόσταση από τις περιοχές επεξεργασίας των προσωπικών δεδομένων.

Απαραίτητη συνθήκη για την ορθή υλοποίηση της προστασίας των προσωπικών δεδομένων, είναι η συμμόρφωση με τα άρθρα 5 & 6 του γενικού κανονισμού (GDPR), προς αποφυγή ασυμβίβαστων χρήσεων και φαινόμενων κατάχρησης. Ειδικότερα, θα πρέπει να προβλεφθεί(CNIL, 2020):

- Ηλεπτομερής περιγραφή των σκοπών της επεξεργασίας δεδομένων και η αιτιολόγηση της νομιμότητάς τους.
- Η ανάλυση των σκοπών της ανταλλαγής με τρίτους καθώς και της επεξεργασίας δεδομένων για τη βελτίωση της λειτουργίας της υπηρεσίας.
- Η αποσαφήνιση συγκεκριμένων όρων υπό τους οποίους θα γίνεται η επεξεργασία.

Πέραν της όποιας φυσικής πρόσβασης, άμεσο κίνδυνο για κάθε υπολογιστή αποτελεί πάντα το κάθε μορφής επικίνδυνο λογισμικό. Στόχος είναι η προστασία της πρόσβασης σε δημόσια και μη ελεγχόμενα δίκτυα, σταθμούς εργασίας και διακομιστές από κακόβουλους κώδικες που θα μπορούσαν να επηρεάσουν την ασφάλεια των προσωπικών δεδομένων όπως antivirus, firewall, proxy, anti-spyware. Για το λόγο αυτό, κρίνεται χρήσιμη (CNIL, 2020):

• Η εγκατάσταση και η συνεχής ενημέρωση antivirus/ antimalware προγραμμάτων, σε διακομιστές και σταθμούς εργασίας, με ταυτόχρονη εξασφάλιση της ανάλυσης του

συστήματος σε πραγματικό χρόνο, σύμφωνα με τους κανόνες που ορίζονται από το τμήμα πληροφορικής του φορέα.

• Η εφαρμογή μέτρων φιλτραρίσματος ως προς τις εισροές και εκροές δικτύου, δηλαδή χρήση κάποιου firewall.

• Η καταγραφή και μεταφορά των συμβάντων προστασίας από ιούς σε κεντρικό διακομιστή για στατιστική ανάλυση και διαχείριση των προβλημάτων, όπως ο εντοπισμός του μολυσμένου διακομιστή ή του ιού που έχει ανιχνευθεί και δεν εξαλείφεται από το antivirus.

Το πλέον σημαντικό στοιχείο της προστασίας των δεδομένων είναι η δημιουργία ενός κώδικα δεοντολογίας που θα ορίζει τα μέτρα και τους κανόνες προστασίας, το σχέδιο δράσης αλλά και την επανεξέταση αυτής. Ο κώδικας δεοντολογίας θα πρέπει να διαμοιράζεται σε όλους εκείνους που συμμετέχουν στην προστασία των δεδομένων και με κάθε τρόπο να παρακολουθείται εφαρμογή του με τακτικό έλεγχο της τήρησης των κανόνων αυτού.

Τα δεδομένα, θα πρέπει να διατηρούνται σε αντίγραφα ασφαλείας για ένα εύλογο χρονικό διάστημα ώστε σε περίπτωση απώλειας να υπάρχει πρόσβαση σε αυτά με την προϋπόθεση όμως πάντα πως θα διατηρείται η εμπιστευτικότητά τους. Καλή πρακτική είναι σε αυτά να εφαρμόζεται κάποιος μηχανισμός κρυπτογράφησης αλλά και να τους γίνεται τακτικός έλεγχος ώστε να διασφαλίζεται η ακεραιότητά τους. Επίσης, σημαντικό είναι να θεσπιστεί και μία διαδικασία με την οποία θα επαναλαμβάνεται κάθε φορά που ο υπεύθυνος ασφαλείας θα προβαίνει στη δημιουργία δημιουργίας αντιγράφων ασφαλείας(CNIL, 2020).

Όταν πρόκειται για τη μεταφορά αρχείων μέσω ηλεκτρονικής αλληλογραφίας θα πρέπει αφενός να υπάρχει ενημέρωση των χρηστών ώστε αυτοί να μην ανοίγουν αρχεία αγνώστου προέλευσης ή αρχεία με επεκτάσεις όπως .pif, .com, .bat, .exe, .vbs και .lnk.

2. ***Μεθοδολογία (Methodology)***

Πρόκειται για τη μέθοδο εκείνη η οποία εξηγεί άμεσα το πώς μπορεί να υλοποιηθεί η διαδικασία της "Εκτίμησης του Αντίκτυπου" (PIA), σύμφωνα με τα κριτήρια και τα πρότυπα για τη διαχείριση των κινδύνων που καθορίζει η εκάστοτε εποπτική αρχή και ο υπεύθυνος επεξεργασίας δεδομένων (DPO). Βασικός άξονας της μεθοδολογίας, κρίνεται η άμεση υποχρέωση του φορέα ώστε αυτός να εμπλέκεται τόσο στη δημιουργία όσο και στη βελτίωση της επεξεργασίας των δεδομένων. Σύμφωνα με τον κανονισμό συμμόρφωσης λοιπόν, ο φορέας θα πρέπει να προβαίνει σε διαρκή λήψη αποφάσεων και επικύρωση αυτών κατά την επεξεργασία των προσωπικών δεδομένων, θα πρέπει να θεσπίζει τα κριτήρια εκείνα με βάση τα οποία θα αξιολογούνται οι κίνδυνοι, να προτείνει μέτρα για την αντιμετώπιση των

κινδύνων, να ορίζει τους υπευθύνους προστασίας δεδομένων που θα υποστηρίζουν συνολικά το έργο και να προσλαμβάνει το ανάλογα καταρτισμένο προσωπικό που επιβλέπει και θα υποστηρίζει τα πρωτόκολλα της ασφάλειας των πληροφοριών(CNIL, 2020).

Οι πυλώνες οι οποίοι στηρίζουν την προσέγγιση συμμόρφωσης που εφαρμόζεται κατά τη διαδικασία της δημιουργίας της Εκτίμησης του Αντικτύπου είναι (CNIL, 2020):

- **1ος Πυλώνας**: θεμελιώδη δικαιώματα και αρχές το οποία είναι «αδιαπραγμάτευτα», θεσπίζονται με νόμο και πρέπει να τηρούνται ανεξάρτητα από τη φύση, τη σοβαρότητα και την πιθανότητα κινδύνων.
- **2ος Πυλώνας**: διαχείριση των κινδύνων ιδιωτικής ζωής των υποκειμένων των δεδομένων, η οποία καθορίζει τους κατάλληλους τεχνικούς και οργανωτικούς ελέγχους για την προστασία των προσωπικών δεδομένων .

Συνοψίζοντας, για την ολοκλήρωση της εκτέλεσης μιας PIA είναι απαραίτητο(CNIL, 2020):

1. Να καθορίζεται και να περιγράφεται το πλαίσιο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που εξετάζει.
2. Να αναλύονται οι έλεγχοι που εγγυώνται τη συμμόρφωση με τις θεμελιώδεις αρχές όπως την αναλογικότητα και την αναγκαιότητα επεξεργασίας καθώς και την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα
3. Να αξιολογούνται και να περιγράφονται επακριβώς οι κίνδυνοι που σχετίζονται με την ιδιωτική ζωή και που συνδέονται με την ασφάλεια των δεδομένων και να διασφαλίζεται ότι αυτοί αντιμετωπίζονται κατάλληλα.
4. Να τεκμηριώνεται επισήμως η επικύρωση της Εκτίμησης του Αντίκτυπου (PIA), βάσει των προηγούμενων βημάτων ή να αποφασίζεται η αναθεώρησή τους.

Στο στάδιο της μεθοδολογίας, θα πρέπει να εκτελούνται διαρκείς έλεγχοι τόσο για το εάν υπάρχει βελτίωση του τρόπου όσο και για το εάν τα δικαιώματα τα οποία έχουν παραχωρηθεί είναι τα σωστά. Φυσικά θα πρέπει σε κάθε επίπεδο να μελετώνται και να επανεκτιμώνται οι κίνδυνοι, οι πηγές αυτών, οι τρόποι με τους οποίους κάποιος ανιχνεύοντας τα τρωτά σημεία του συστήματος ενδέχεται να έχει κακόβουλη πρόσβαση στα δεδομένα, το πλαίσιο των απειλών αλλά και τελικά το αντίκτυπο των επιπτώσεων που θα έχει μία παραβίαση προσωπικών δεδομένων.

Όπως προαναφέρθηκε, οι έλεγχοι οι οποίοι εκτελούνται, θα πρέπει σε κάθε στάδιο να επανεξετάζονται ώστε να αξιολογείται η αποτελεσματικότητά τους. Ο έλεγχος αυτός λοιπόν, πραγματοποιείται από τον αρμόδιο φορέα και εγκρίνεται από τον υπεύθυνο προστασίας των

δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα η αξιολόγηση θα πρέπει να περιλαμβάνει τα εξής στάδια(CNIL, 2020):

- Ελέγχους που αφορούν συγκεκριμένα δεδομένα που υποβάλλονται σε επεξεργασία, όπως κρυπτογράφηση, ανωνυμία, διαμέριση, έλεγχο πρόσβασης, ανιχνευσιμότητα.
- Γενικούς ελέγχους ασφαλείας σχετικά με το σύστημα στο οποίο πραγματοποιείται η επεξεργασία: ασφάλεια λειτουργίας, δημιουργία αντιγράφων ασφαλείας, ασφάλεια του υλικού.
- Οργανωτικούς ελέγχους (διακυβέρνηση): πολιτική, διαχείριση έργου, προσωπικό διαχείρισης, διαχείριση συμβάντων και παραβάσεων, σχέσεις με τρίτους.

Η οριστική επικύρωση της PIA, σύμφωνα πάντα με την CNIL, πραγματοποιείται από τον υπεύθυνος επεξεργασίας προσωπικών δεδομένων σε συνεργασία πάντα με τον αρμόδιο φορέα ο οποίος άλλωστε έχει και την αποκλειστική ευθύνη να αποδεχθεί ή όχι το πόρισμα που του αποδίδεται από τον έλεγχο και τη μελέτη με βάση πάντα τον ανάλογο κώδικα δεοντολογίας. Συγκεκριμένα αφού συγκεντρωθούν και οριστικοποιηθούν τα ευρήματα της μελέτης θα πρέπει(CNIL, 2020):

1. Να προετοιμαστεί μια οπτική παρουσίαση των ελέγχων που επιλέγονται προκειμένου να εξασφαλιστεί η συμμόρφωση με τις θεμελιώδεις αρχές, ανάλογα με τη συμμόρφωσή τους με το GDPR.

2. Να προετοιμαστεί μια οπτική παρουσίαση των ελέγχων που επιλέγονται για να συμβάλουν στην ασφάλεια των δεδομένων, ανάλογα με τη συμμόρφωσή τους με τις βέλτιστες πρακτικές ασφαλείας.

3. Να παρουσιαστεί μια οπτική χαρτογράφηση των κινδύνων ανάλογα με τη σοβαρότητα και τη πιθανότητα τους.

4. Να καταρτιστεί ένα σχέδιο δράσης με βάση τους πρόσθετους ελέγχους που εντοπίστηκαν κατά τα προηγούμενα βήματα.

3. ***Πρότυπα (Templates)***

Για να είναι εμπεριστατωμένη και πλήρως αποδοτική μία Μελέτη Εκτίμησης Αντικτύπου, θα πρέπει αυτή να βασίζεται σε διάφορα πρότυπα τα οποία με τη σειρά τους θα προσαρμόζονται ανάλογα στο πλαίσιο και στη μεθοδολογία που πρέπει να ακολουθηθεί. Καθώς η διαδικασία αυτή θα πρέπει σε κάθε βήμα της να είναι καθόλα νόμιμη, θα πρέπει να λαμβάνονται υπόψη κριτήρια νομιμότητας όπως(CNIL, 2020) :

- Το υποκείμενο των δεδομένων να έχει δώσει τη συγκατάθεσή του για επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους ειδικούς σκοπούς.
- Η επεξεργασία να κρίνεται απαραίτητη για την εκτέλεση μιας σύμβασης στην οποία συμμετέχει το πρόσωπο, στο οποίο αναφέρονται τα δεδομένα ή για τη λήψη μέτρων κατόπιν αιτήματος του υποκειμένου των δεδομένων πριν από τη σύναψη μιας σύμβασης
- Η επεξεργασία να είναι απαραίτητη για τη συμμόρφωση με μια νομική υποχρέωση.
- Η επεξεργασία να είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου
- Η επεξεργασία να είναι απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας
- Η επεξεργασία να είναι αναγκαία για τους σκοπούς των νόμιμων συμφερόντων που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, εκτός εάν τα συμφέροντα ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του προσώπου στο οποίο αναφέρονται τα δεδομένα, απαιτούν προστασία δεδομένων προσωπικού χαρακτήρα, ιδίως όταν τα δεδομένα αφορούν παιδί.

Η κατηγορία των προτύπων, προβλέπει και αυτή με τη σειρά της αξιολόγηση των ελέγχων ασφαλείας και ελέγχους που αφορούν στα δεδομένα επεξεργασίας όπως η κρυπτογράφηση και ο έλεγχος λογικής πρόσβασης. Οι γενικοί έλεγχοι λοιπόν, σε κάθε περίπτωση, περιλαμβάνουν μεθόδους που προστατεύουν σε κάθε περίπτωση το σύστημα στο οποίο πραγματοποιείται η επεξεργασίας. Έτσι, σε αυτούς συγκαταλέγονται ο περιορισμός του κακόβουλου λογισμικού, η δημιουργία αντιγράφων ασφαλείας, η συντήρηση, η διαρκής παρακολούθησης, ο έλεγχος φυσικής πρόσβασης και φυσικά η ασφάλεια του υλικού(CNIL, 2020).

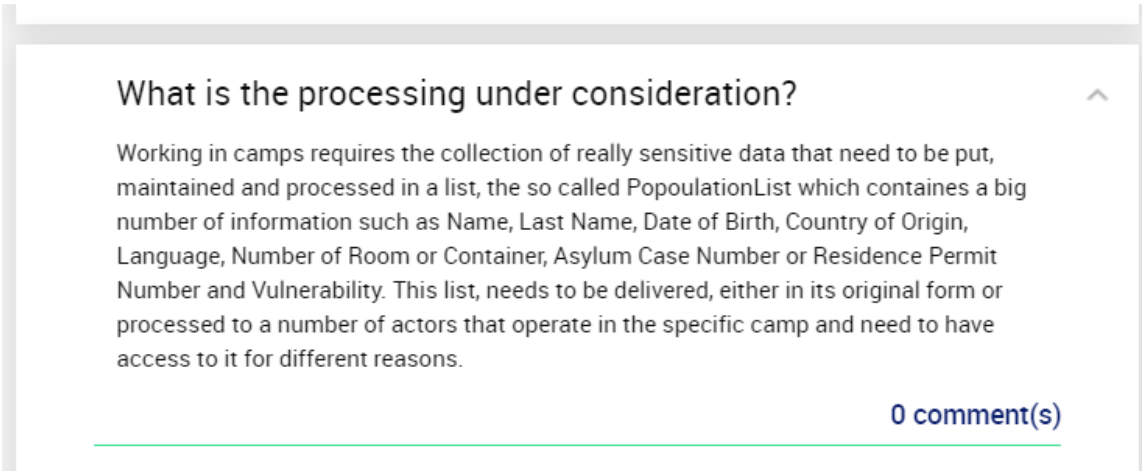
Και στο στάδιο αυτό προβλέπεται ανάλυση και αξιολόγηση του κινδύνου με πιθανότερους κινδύνους να είναι η αθέμιτη πρόσβαση στα δεδομένα αλλά και η ανεπιθύμητη αλλαγή των δεδομένων. Αρμοδιότητα του υπεύθυνου επεξεργασίας λοιπόν στο στάδιο αυτό είναι να προσδιορίσει εάν οι υπάρχοντες ή/και οι προγραμματισμένοι έλεγχοι περιορίζουν στο έπακρο τους κινδύνους αυτούς έτσι ώστε να καταστούν αποδεκτοί.

4.1 Μελέτη Περίπτωσης

Αφού λοιπόν επιλέχθηκε η μέθοδος CNILως η πλέον καταλληλότερη ώστε να εφαρμοστεί, με βάση πάντα τα όσα πλεονεκτήματα αυτής συνοψίζονται παραπάνω, αντικείμενο μελέτης αποτέλεσε η πληθυσμιακή λίστα που συμπληρώνεται από μία ΜΚΟ σε μία δομή φιλοξενίας προσφύγων. Στη ΜΚΟ δόθηκε τυχαία το όνομα MyNGO και ακόμη θεωρήθηκε πως αυτή διαθέτει 50 εργαζόμενους, οι οποίοι σε συνεργασία με άλλους οργανισμούς που δρουν στη δομή παρέχει μία πληθώρα υπηρεσιών σε έναν αριθμό 1500 ατόμων. Ειδικότερα, προσφέρονται υπηρεσίες ψυχοκοινωνικής στήριξης, νομικές υπηρεσίες, τεχνικές υπηρεσίες, εκπαίδευση και σειρά δραστηριοτήτων. Με στόχο να υπάρχουν κάπου καταγεγραμμένοι όλοι όσοι διαμένουν στη δομή, συντάσσεται μία πληθυσμιακή λίστα η οποία περιέχει για τον κάθε ένα από τους ωφελούμενους μία σειρά στοιχείων όπως :

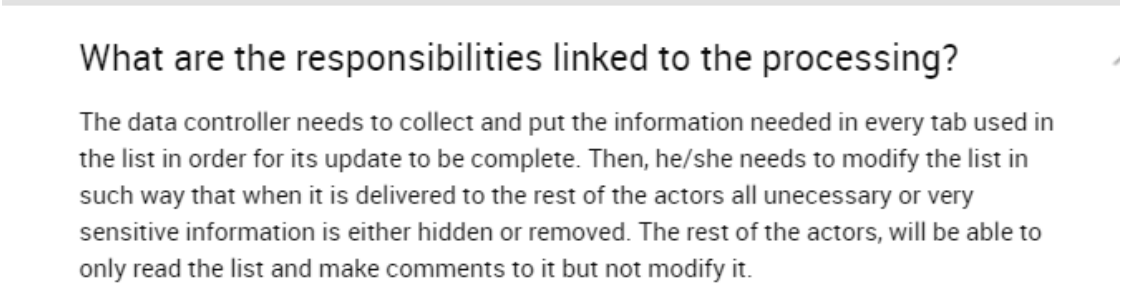
- ***Όνομα***
- ***Επώνυμο***
- ***Ημερομηνία Γέννησης***
- ***Χώρα Καταγωγής***
- ***Γλώσσα***
- ***Οικίσκο Διαμονής***
- ***Ευαλωτότητα***
- ***Αριθμό Υπόθεσης***

Τα παραπάνω στοιχεία χαρακτηρίζουν μονοσήμαντα τον κάθε ωφελούμενο και είναι ιδιαίτερα σημαντικά τόσο για τους οργανισμούς που δραστηριοποιούνται στη δομή όσο και για τους ελληνικούς δημόσιους φορείς, ώστε αυτοί να έχουν μία συνολική εικόνα των ωφελούμενων που διαμένουν στις δομές σε όλη την επικράτεια. Μονάχα έτσι μπορεί να υπάρχει ένας σχεδόν πλήρης έλεγχος όλων ανθρώπων που βρίσκονται εντός του χώρου της δομής ώστε οι οργανώσεις να γνωρίζουν εάν υπάρχουν κενές θέσεις διαμονής αλλά και εάν οι ωφελούμενοι έχουν πάψει ή όχι να διαμένουν εκεί. Η λίστα ανανεώνεται σε μηνιαία βάση και διανέμεται είτε αυτούσια ή με κάποια πεδία αυτής να έχουν αποκρυφθεί σε όλους τους φορείς που δραστηριοποιούνται στη δομή ώστε αυτοί να έχουν άμεση πρόσβαση στην πληροφορία και γνώση σχετική με τα όσα αυτή περιέχει. Η πρώτη ερώτηση του λογισμικού του CNILαφορά αποκλειστικά στα όσα περιγράφηκαν παραπάνω και εμφανίζεται στην εικόνα που ακολουθεί.



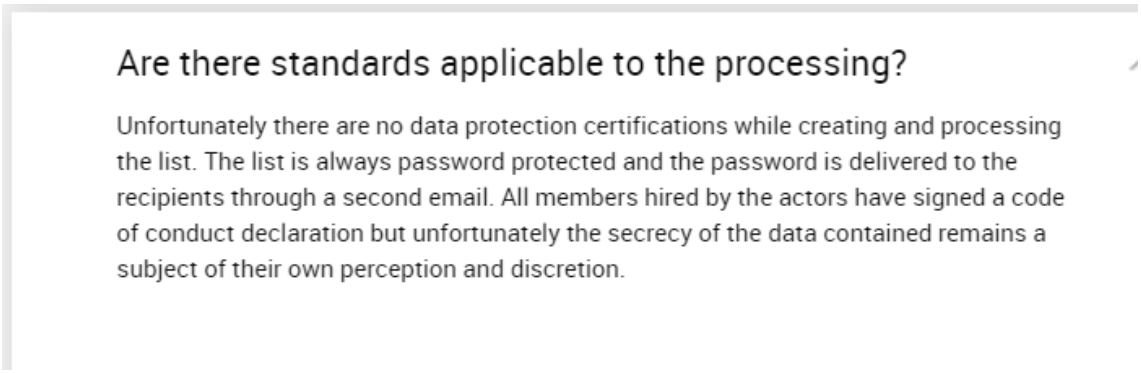
Εικόνα 1 : Αντικείμενο Επεξεργασίας

Ο υπεύθυνος επεξεργασίας οφείλει να συμπληρώσει τη λίστα συλλέγοντας όλα τα απαραίτητα στοιχεία κάθε φορά που έρχονται νέοι ωφελούμενοι στη δομή ή να διαγράψει στοιχεία από αυτή όταν οι ωφελούμενοι αποχωρούν επίσημα λόγω εγκατάστασης αυτών σε διαμερίσματα στην πόλη. Σε κάποιες περιπτώσεις ενδεχόμενα να χρειάζεται να αποκρυφθούν στοιχεία, όπως οι ευαλωτότητες των ωφελούμενων που δε θα πρέπει να είναι γνωστές στο σύνολο των ανθρώπων που έχουν πρόσβαση στη λίστα. Ακόμη, αρμοδιότητα του υπεύθυνου επεξεργασίας είναι να διαμοιράσει τη λίστα κάθε φορά που αυτή θα υποστεί οποιασδήποτε μορφής μορφοποίηση με προσθήκη, αφαίρεση ή μεταβολή δεδομένων.



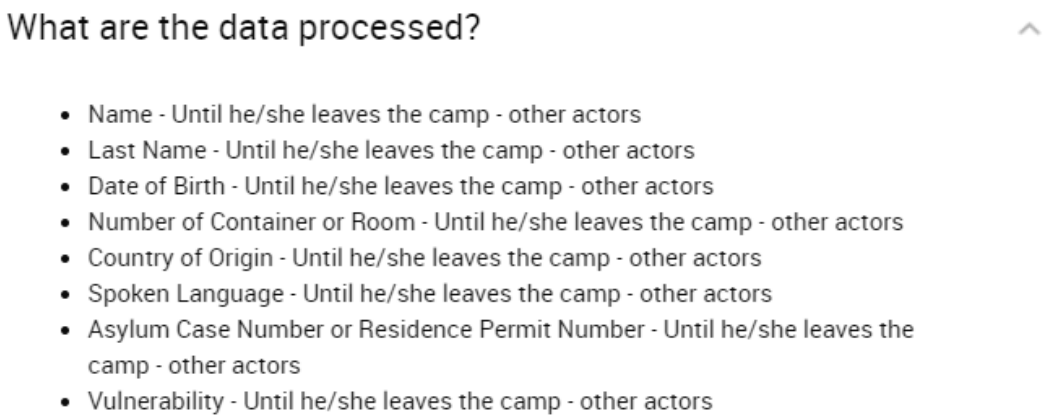
Εικόνα 2 : Αρμοδιότητες που σχετίζονται με τη λίστα

Η λίστα προστατεύεται πάντα από κάποιο passwordπου αλλάζει κάθε φορά που αυτή διανέμεται και αποστέλλεται στους χρήστες που θα έχουν πρόσβαση σε αυτή με ένα δεύτερο mail. Δυστυχώς σε αυτή δεν εφαρμόζονται κάποια άλλα πρωτόκολλα ασφαλείας, αλγόριθμοι ή μηχανισμοί κρυπτογράφησης. Βέβαια, όλοι οι χρήστες οι οποίοι απασχολούνται τόσο σε δημόσιους όσο και σε μη κερδοσκοπικούς οργανισμούς έχουν υπογράψει τον ανάλογο κώδικα δεοντολογίας και δεσμεύονται ηθικά από αυτόν.



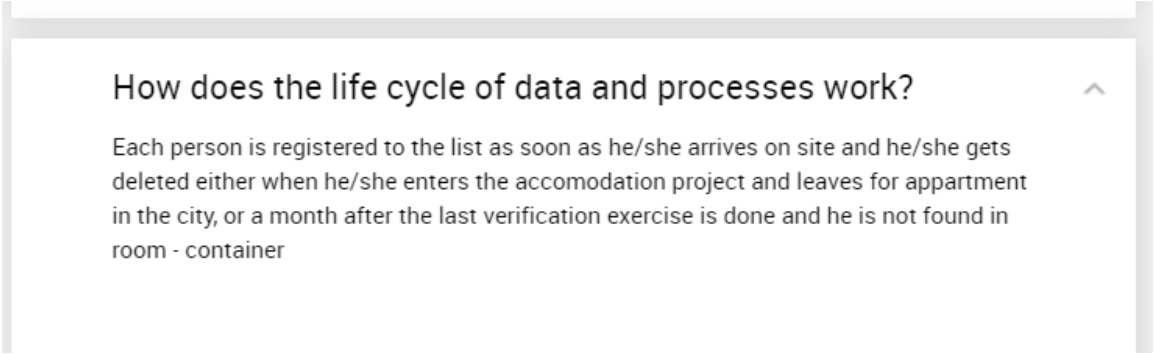
Εικόνα 3 : Πρότυπα που εφαρμόζονται

Τα δεδομένα τα οποία συλλέγονται, όπως αναφέρθηκε και νωρίτερα, αφορούν σε προσωπικά στοιχεία τα οποία στο σύνολό τους χαρακτηρίζουν μονοσήμαντα που ανθρώπους που φιλοξενούνται στη δομή. Καταγράφονται ακριβώς όπως αυτά αναγράφονται στα αστυνομικά δελτία τους και στη συνέχεια καταχωρούνται στη λίστα ώστε να την επικαιροποιήσουν.



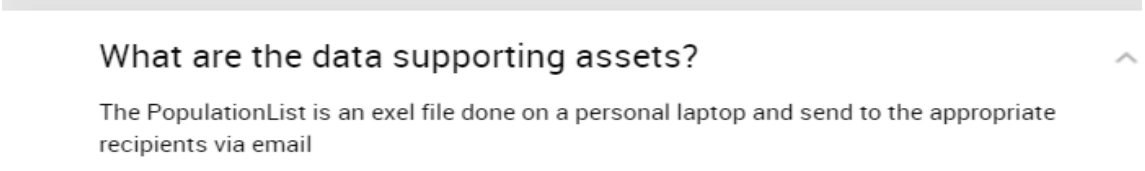
; ικόνα 4 : Δεδομένα που συλλέγονται

Ο κύκλος ζωής των δεδομένων είναι μερικώς απροσδιόριστος, καθώς κανείς δε μπορεί να γνωρίζει εκ προοιμίου το διάστημα κατά το οποίο θα παραμείνει ένας ωφελούμενος στη δομή. Έτσι λοιπόν, οι διαγραφές δε γίνονται σε καμία περίπτωση μαζικά αλλά συνήθως αφορούν σε μεμονωμένες περιπτώσεις ή οικογένειες. Οι ωφελούμενοι παραμένουν στη δομή για το διάστημα που ενδεχομένως αυτοί θα αποφασίσουν ή έως ότου αποκτήσουν δικαίωμα μετακίνησης στον αστικό ιστό λόγω ένταξης σε κάποιο άλλο πρόγραμμα. Άρα, κάποια ονόματα ενδέχεται να παραμένουν στην λίστα για έτη ενώ κάποια άλλα ίσως για μερικές μόνο μέρες.



Εικόνα 5: Κύκλος ζωής των δεδομένων

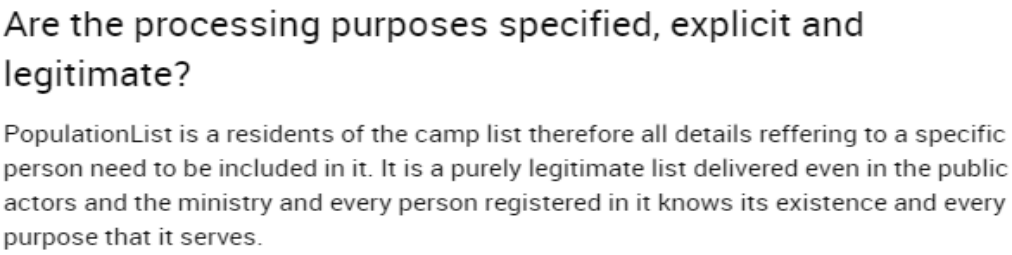
Η πληθυσμιακή λίστα αποτελεί ένα αρχείο EXCELαπλής μορφής, με διαφορετικές στήλες και πολλαπλά φίλτρα. Δημιουργείται στο laptoptου υπεύθυνου επεξεργασίας και στη συνέχεια διανέμεται στους ανάλογους παραλήπτες – χρήστες οι οποίοι με τη σειρά τους την αποθηκεύουν στους δικούς τους προσωπικούς υπολογιστές.



Εικόνα 6 : Αποθήκευση των δεδομένων

4.2 Βασικές Αρχές

Η δημιουργία, η τροποποίηση και η διαγραφή δεδομένων από τη λίστα είναι μια απολύτως νόμιμη διαδικασία καθώς για τη δημιουργία αυτής έχουν δώσει εντολή όλοι οι αρμόδιοι κρατική φορείς, ώστε να είναι σε θέση να γνωρίζουν τόσο τον αριθμό αλλά και την πληθυσμιακή σύνθεση των ανθρώπων που διαμένουν σε δομές. Τα δεδομένα που πρέπει να συμπεριλαμβάνονται σε αυτή είναι ξεκάθαρα και αφορούν σε όσα μπορούν να χαρακτηρίσουν μονοσήμαντα έναν διαμένοντα σε δομή.



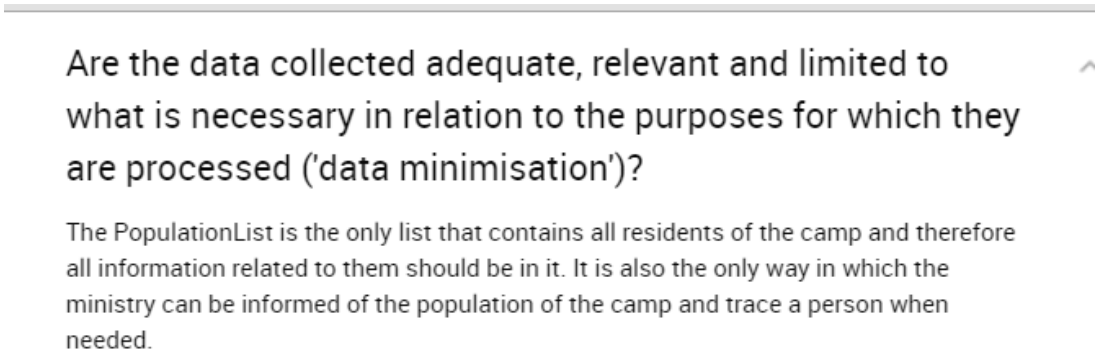
Εικόνα 7 : Νομιμότητα της λίστας

Οι διαμένοντες στη δομή, κατά την άφιξή τους, ενημερώνονται για τη λίστα και υπογράφουν ένα έγγραφο συναίνεσης καταχώρησης των προσωπικών τους δεδομένων σε αυτή. Το έγγραφο είναι μεταφρασμένο στη γλώσσα τους, ώστε να μπορούν να κατανοούν πλήρως τα δεδομένα που καταγράφονται, αλλά και τη σημαντικότητα αυτών. Σε περίπτωση που κάποιος εξ αυτών αδυνατεί να διαβάσει το έγγραφο, τότε του παρέχεται διερμηνέας ο οποίος του εξηγεί με κάθε λεπτομέρεια τα όσα αναγράφονται στο κείμενο.

Εικόνα 8 : Έγγραφο Συναίνεσης

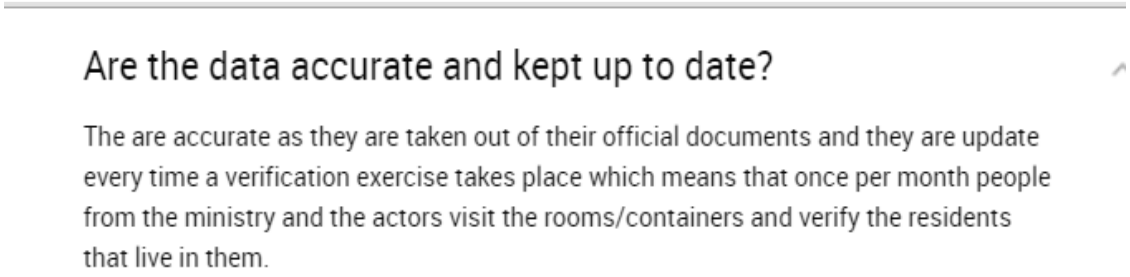
Τα δεδομένα τα οποία συλλέγονται είναι περιορισμένα και είναι τα απολύτως απαραίτητα, τα οποία ορίζονται από το αρμόδιο υπουργείο ώστε να συλλεγούν. Καθώς αντιγράφονται από το

τρίπτυχο που τους έχει επιδοθεί από την Υπηρεσία Ασύλου είναι έγκυρα στο μέγιστο βαθμό τους. Οποιαδήποτε ασάφεια σε αυτά αφορά στην ίδια την υπηρεσία ή στο τμήμα πρώτης υποδοχής, οι οποίοι και καταγράφουν τα στοιχεία και όχι στον υπεύθυνο επεξεργασίας.



Εικόνα 9 : Ακεραιότητα των δεδομένων

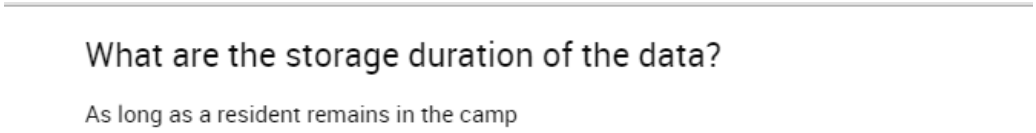
Όπως αναφέρθηκε και παραπάνω, τα δεδομένα εκπορεύονται από οποιοδήποτε δημόσιο έγγραφο τους έχει επιδοθεί από τις ελληνικές αρχές και άρα είναι έγκυρα στο μέγιστο δυνατό βαθμό. Ακόμη, αυτά ανανεώνονται είτε κάθε φορά που γίνεται άσκηση επιβεβαίωσης του πληθυσμού που διαμένει στη δομή. Το προσωπικό της δομής, επισκέπτεται τον κάθε οικίσκο και καταγράφει ηλεκτρονικά όσους διαμένουν σε αυτόν με βάση πάντα τα επίσημα έγγραφά τους.



Εικόνα 10 : Εγκυρότητα και επικαιροποίηση δεδομένων

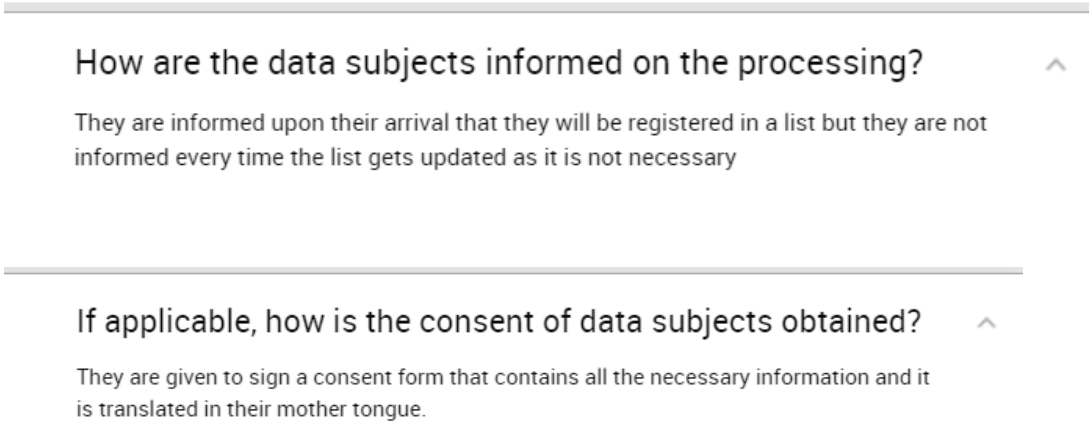
Τα δεδομένα παραμένουν στη λίστα για όσο καιρό ο ωφελούμενος είναι επίσημα εγγεγραμμένος στη δομή και διαμένει σε αυτή. Διαγράφονται όταν αυτός αποχωρήσει επίσημα διαμέσου προγράμματος ένταξης στον αστικό ιστό. Σε περίπτωση που αυτός αποχωρήσει ανεπίσημα, διατηρούνται για ένα μικρό χρονικό διάστημα, ώστε να διασφαλιστεί

το ενδεχόμενο της επιστροφής του και έπειτα διαγράφονται, ώστε αφενός να υπάρχει διαφάνεια και αφετέρου αυτός να πάψει να λαμβάνει το ανάλογο οικονομικό βοήθημα.



Εικόνα 11 : Διαγραφή Δεδομένων

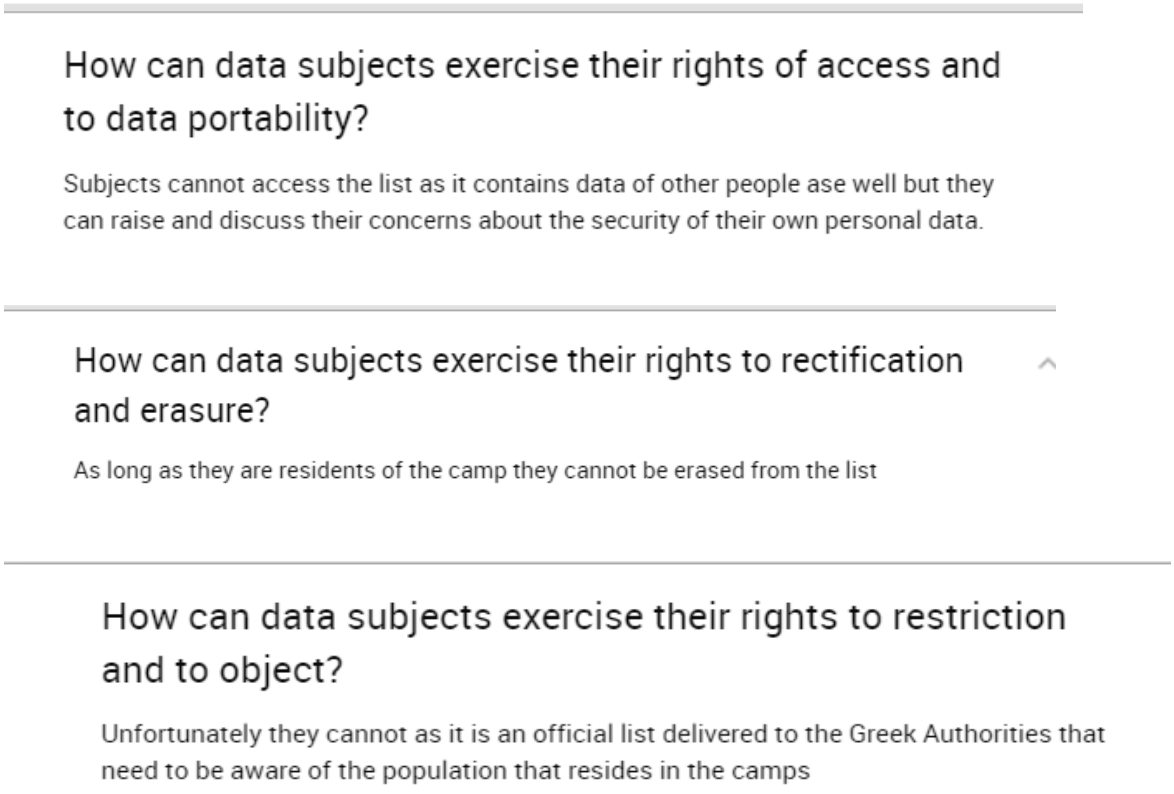
Οι ωφελούμενοι ενημερώνονται κατά την άφιξή τους στη δομή πως θα πρέπει να καταγραφούν και να συμπεριληφθούν στη λίστα των διαμενόντων σε αυτή. Καθώς η λίστα επικαιροποιείται κάθε φορά που κάποιος έρχεται ή φεύγει από τη δομή, οι υπόλοιποι διαμένοντες δε χρειάζεται να γνωρίζουν την όποια επεξεργασία γίνεται σε αυτή. Όπως προαναφέρθηκε, σε αυτούς δίνεται κατά την άφιξή τους έγγραφο που περιγράφει όλες τις λεπτομέρειες που θα καταγραφούν και αυτοί υποβάλλουν την υπογραφή τους στο έγγραφο αυτό.



Εικόνα 12 : Πληροφόρηση και έγγραφη συναίνεση

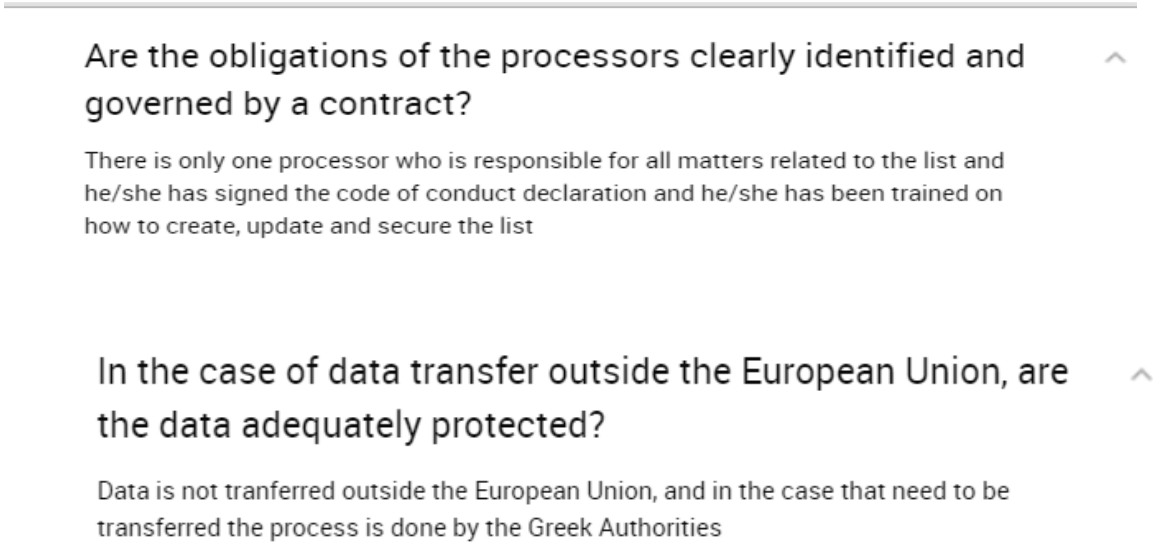
Οι ωφελούμενοι δεν έχουν δικαίωμα πρόσβασης στη λίστα καθώς σε αυτή περιλαμβάνονται προσωπικά δεδομένα άλλων ωφελούμενων τα οποία θα πρέπει σε κάθε περίπτωση να παραμείνουν απόρρητα. Λόγω της σοβαρότητας των δεδομένων και της ανάγκης για ασφάλεια, πρόσβαση στη λίστα έχουν μονάχα οι εξουσιοδοτημένοι χρήστες και κανένας από

τους ωφελούμενους. Επιπρόσθετα, είναι γνωστό και σαφές σε όλους πως για όσο χρόνο παραμένουν στη δομή, είναι υποχρεωτικό να παραμένουν εγγεγραμμένοι σε αυτή και ότι τα ονόματά τους διαγράφονται όταν αυτοί αποχωρήσουν από αυτή. Τέλος, οι ωφελούμενοι δεν έχουν δικαίωμα να ζητήσουν να μην εγγραφούν σε αυτή καθώς πρόκειται για ένα έγγραφο το οποίο αποστέλλεται στις αρμόδιες ελληνικές υπηρεσίες, ώστε να υπάρχει γενικότερη γνώση του πληθυσμού που φιλοξενείται στις δομές.



Εικόνα 13 : Πρόσβαση, διαγραφή, και μη συναίνεση στη λίστα

Ο υπεύθυνος επεξεργασίας της λίστας είναι αυτός ο οποίος έχει και την πλήρη διαχείριση της και προβαίνει σε όποια τροποποίηση σχετικά με αυτή. Ο ίδιος έχει υπογράψει κώδικα δεοντολογίας του φορέα στον οποίο απασχολείται δεσμεύεται ηθικά από αυτόν. Η λίστα επεξεργάζεται σε τοπικό επίπεδο και διαμοιράζεται στους αρμόδιους φορείς και στις ελληνικές υπηρεσίες. Σε καμία περίπτωση δεν ξεπερνά τα σύνορα της χώρας και συν επαγωγικά της Ευρωπαϊκής Ένωσης. Εάν για κάποιο λόγο κάποια πληροφορία θα πρέπει να φύγει εκτός συνόρων, την πλήρη και αποκλειστική ευθύνη για αυτό φέρει το Ελληνικό Κράτος και οι ανάλογοι υπεύθυνοι φορείς.



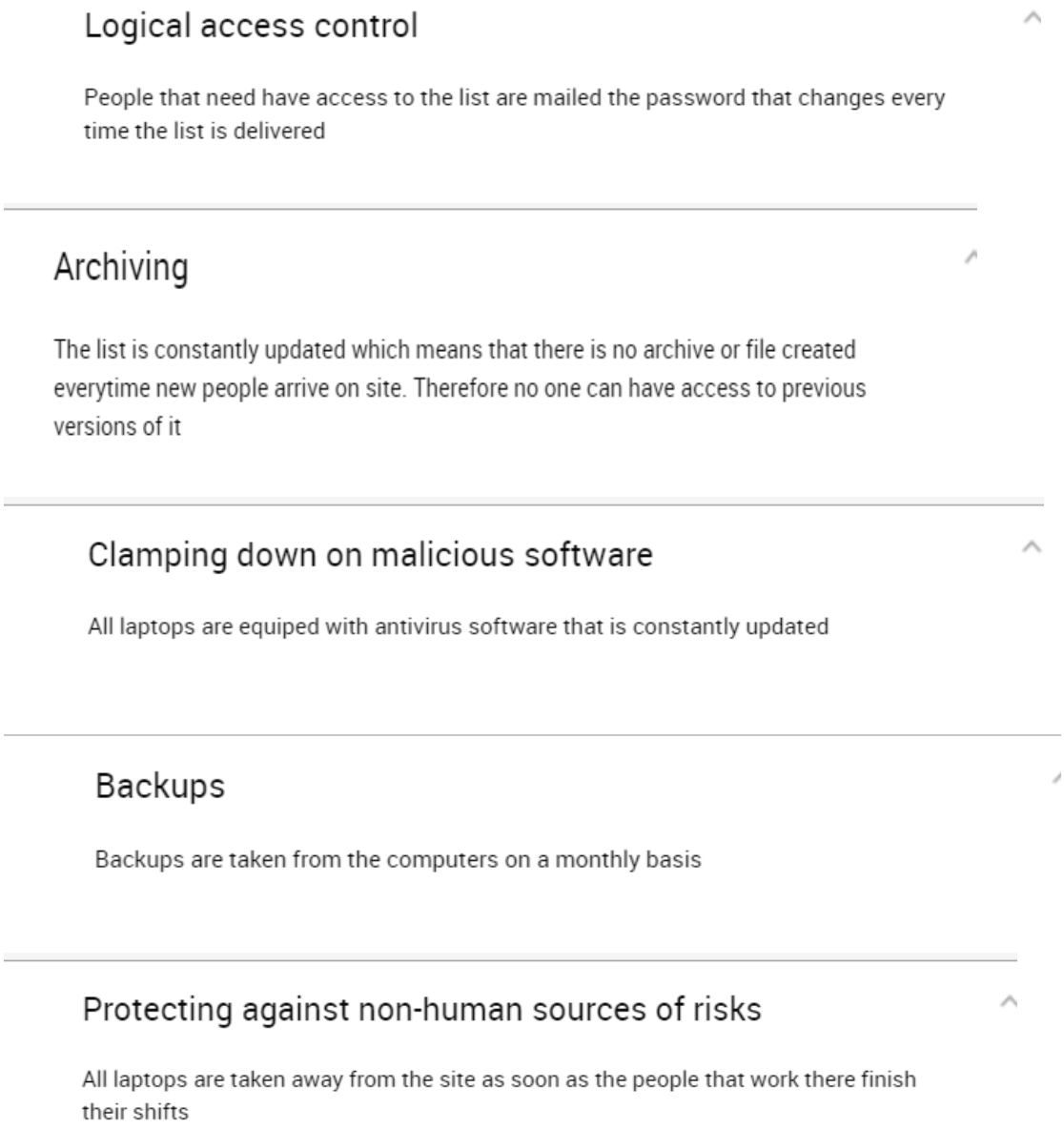
Εικόνα 14 : Διασφάλιση δεδομένων εντός και εκτός της Ευρωπαϊκής Ένωσης

4.3 Κίνδυνοι

Η φυσική πρόσβαση στη λίστα δίνεται σε συγκεκριμένους ανθρώπους ενώ αυτή αποστέλλεται πάντα μέσω emailπροστατευμένη από κάποιο κωδικό ασφαλείας ο οποίος αποστέλλεται στους χρήστες με δεύτερο mail. Ο κωδικός πρόσβασης είναι διαφορετικός για κάθε αποστολή λίστας, περιέχει γράμματα, αριθμούς και ειδικούς χαρακτήρες και σε καμία περίπτωση δεν ομοιάζει με τον προηγούμενο.

Με στόχο να αποφευχθεί οποιαδήποτε πρόσβαση σε απόρρητη πληροφορία, δεν γίνεται αρχειοθέτηση της λίστας παρά μονάχα από τις αρμόδιες ελληνικές αρχές που είναι υπεύθυνες για τον προσφυγικό πληθυσμό. Έτσι, πρόκειται για το ίδιο αρχείο που αφού επεξεργαστεί κατάλληλα διαμοιράζεται στους χρήστες.

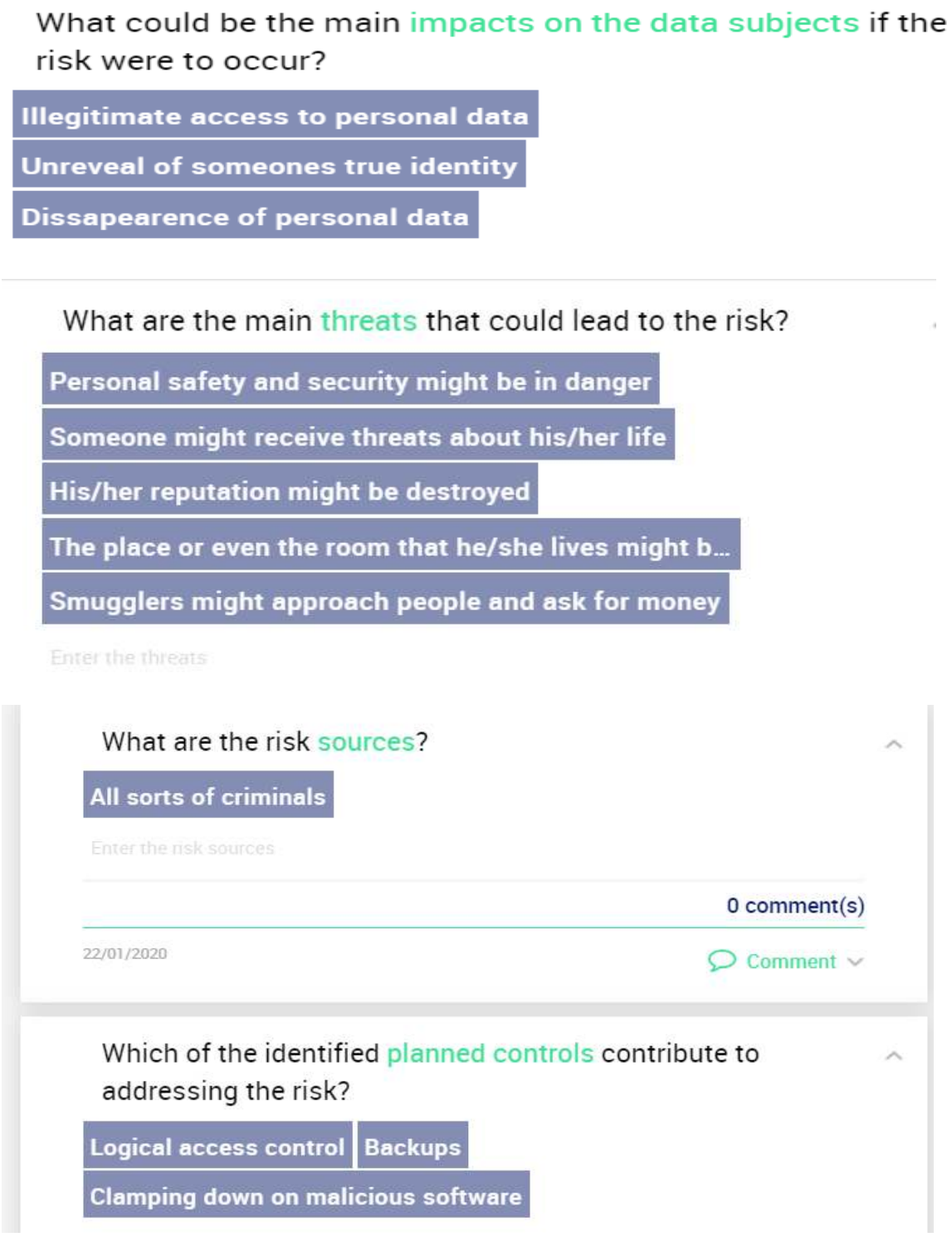
Σε όλους τους υπολογιστές που χρησιμοποιούν το αρχείο αυτό έχει εγκατασταθεί το ανάλογο πρόγραμμα προστασίας από ιούς με στόχο τόσο να αποφευχθεί κάποια κακόβουλη εισβολή όσο και να προστατευθεί το σύστημα από καταστροφή αρχείων ή τομέων στο δίσκο. Παράλληλα, σε μηνιαία βάση, γίνεται backupόλων των υπολογιστών για να διασφαλιστούν τα όποια αρχεία υπάρχουν διαθέσιμα τη στιγμή εκείνη στον υπολογιστή. Τέλος, μετά το πέρας του ωραρίου εργασίας, όλοι οι προσωπικοί υπολογιστές, απομακρύνονται από το πεδίο και φυλάσσονται στις οικίες των εργαζομένων.



Εικόνα 15 : Έλεγχος και προστασία του αρχείου

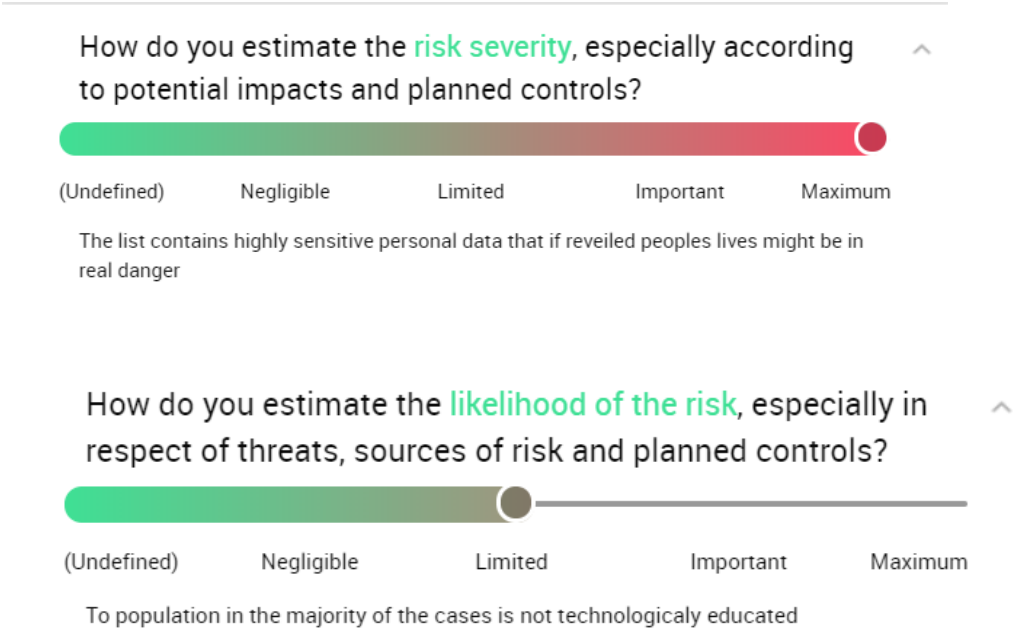
Σε περίπτωση που εκδηλωθεί κάποιος κίνδυνος, και η λίστα ξεφύγει των εξουσιοδοτημένων χρηστών, ενδέχεται να αποκτήσει πρόσβαση σε αυτή κάποιος μη εξουσιοδοτημένος και άρα κακόβουλος. Επιπρόσθετα, ενδέχεται να αποκαλυφθούν ταυτότητες ανθρώπων που θα πρέπει να παραμείνουν μυστικές ή ακόμη και να χαθούν σημαντικά δεδομένα προσωπικού χαρακτήρα. Το παραπάνω, ενδέχεται να εισάγει κίνδυνο για τη σωματική ακεραιότητα ή ακόμα για τη ζωή ενός ανθρώπου. Ακόμη, αυτός ενδέχεται να γίνει στόχος απειλών ή να καταστραφεί με πολλούς και διαφορετικούς τρόπους η αξιοπρέπειά του. Σημαντικό είναι και το γεγονός ότι μπορεί να αποκαλυφθεί σε επιτήδειους ο χώρος διαμονής του ή επίδοξοι

διακινητές να τον πλησιάσουν για να του ζητήσουν χρήματα. Πηγή του κινδύνου είναι κάθε μορφής εγκληματίες που στοχεύουν κατά της ζωής ή της σωματικής και ηθικής ακεραιότητας των ανθρώπων αυτών αλλά και επίδοξοι διακινητές με στόχο αποκλειστικά και μόνο το κέρδος. Με στόχο λοιπόν να υφίσταται η μέγιστη δυνατή ασφάλεια σε ότι αφορά τη λίστα αυτή, το αρχείο προστατεύεται με κωδικό, διανέμεται σε συγκεκριμένους ανθρώπους και τα μηχανήματα που το φιλοξενούν ελέγχονται τακτικά για ιούς και παραβάσεις.



Εικόνα 16 : Κίνδυνοι, απειλές κα έλεγχος του αρχείου

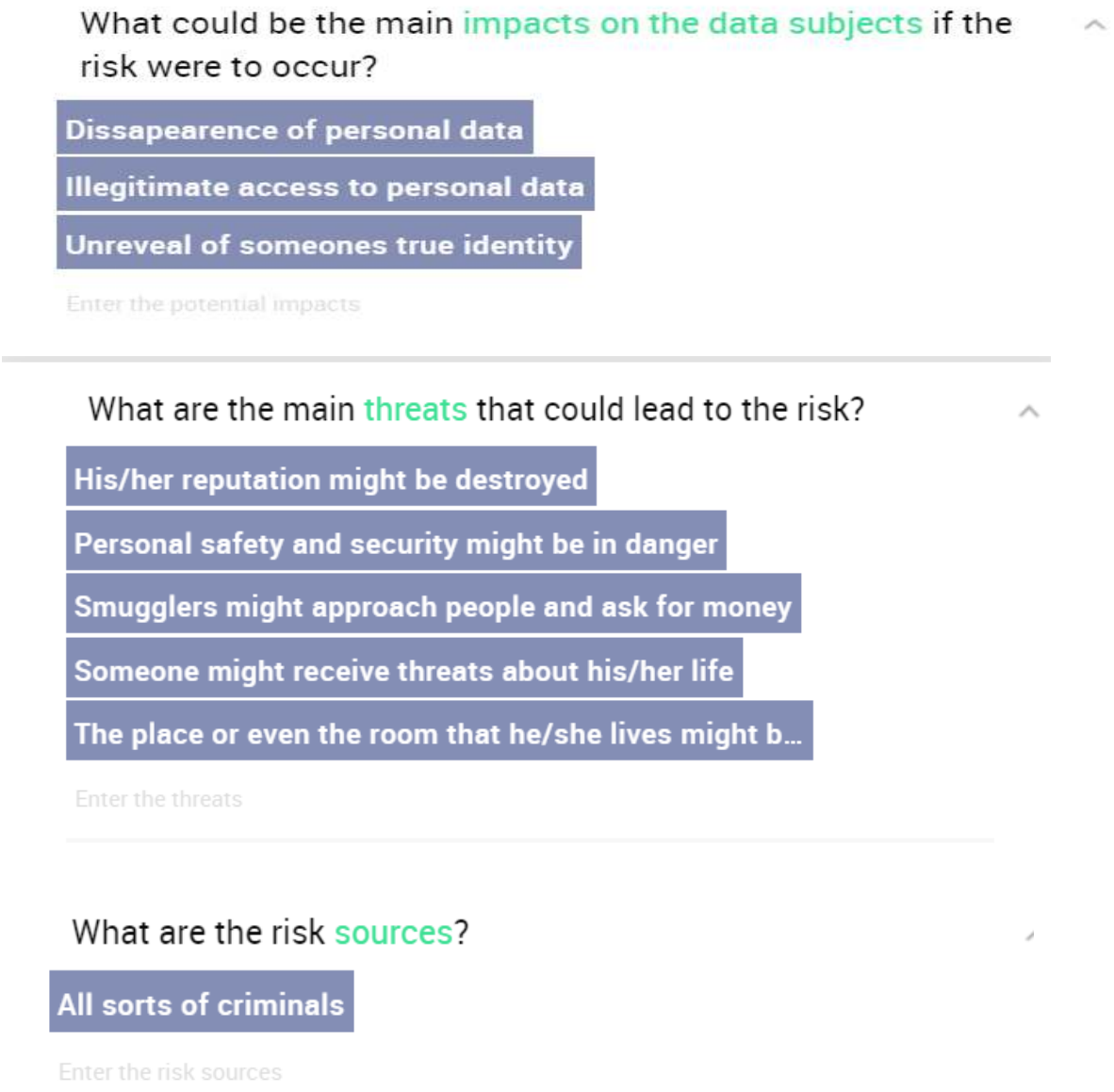
Δεδομένου λοιπόν, των κινδύνων που μόλις περιγράφηκαν, θα μπορούσε κανείς να πει ότι η σοβαρότητα αυτών είναι ιδιαίτερα αυξημένη καθώς πρόκειται για έναν ιδιαίτερα ευαίσθητο πληθυσμό και σε πολλές περιπτώσεις δύναται κανείς να μιλά ακόμη και για απειλή κατά της ίδιας της ζωής. Η έως τώρα εμπειρία έχει δείξει πως οι επίδοξοι και πάσης φύσεως κακόβουλοι δεν έχουν προσπαθήσει να έχουν πρόσβαση σε αυτού του τύπου τις λίστες παρόλο που γνωρίζουν την ύπαρξή τους. Επιπρόσθετα, σε πολλές περιπτώσεις το γνωστικό επίπεδο σε σχέση με την τεχνολογία είναι αρκετά χαμηλό. Ακόμη, ο υπεύθυνος επεξεργασίας αλλά και οι χρήστες, δεδομένων των μέσων που διαθέτουν αλλά και των τεχνικών τους γνώσεων, καταβάλλουν τη μέγιστη δυνατή προσπάθεια ώστε να διαφυλάξουν τα δεδομένα.

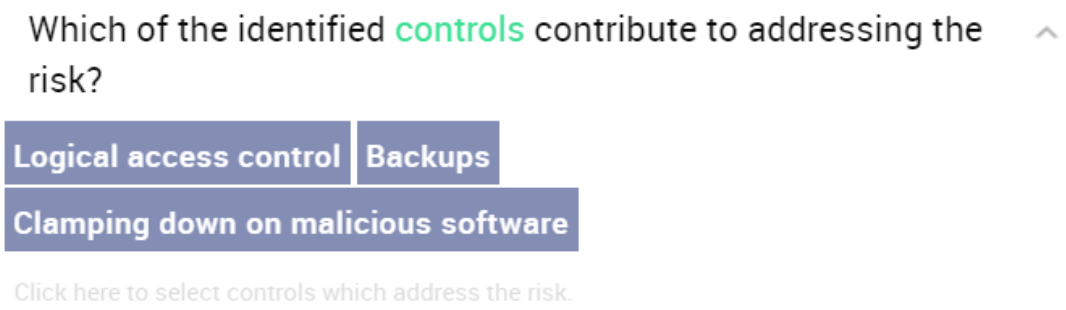


Εικόνα 17 : Μέγεθος και πιθανότητα κινδύνου

Σε περίπτωση που υπάρχει ανεπιθύμητη επεξεργασία και διαμόρφωση των δεδομένων, τα αποτελέσματα για τα υποκείμενα θα είναι σχεδόν ίδια καθώς και πάλι ενδέχεται να επηρεαστεί η φήμη ενός ανθρώπου, η πρόσβαση σε αυτά να γίνει με παράνομο τρόπο και τέλος να εμφανισθεί δημόσια η πραγματική ταυτότητα ενός ανθρώπου. Οι άνθρωποι αυτοί τυγχάνουν διεθνούς προστασίας και έτσι οποιοδήποτε δεδομένο σχετίζεται με αυτούς θα

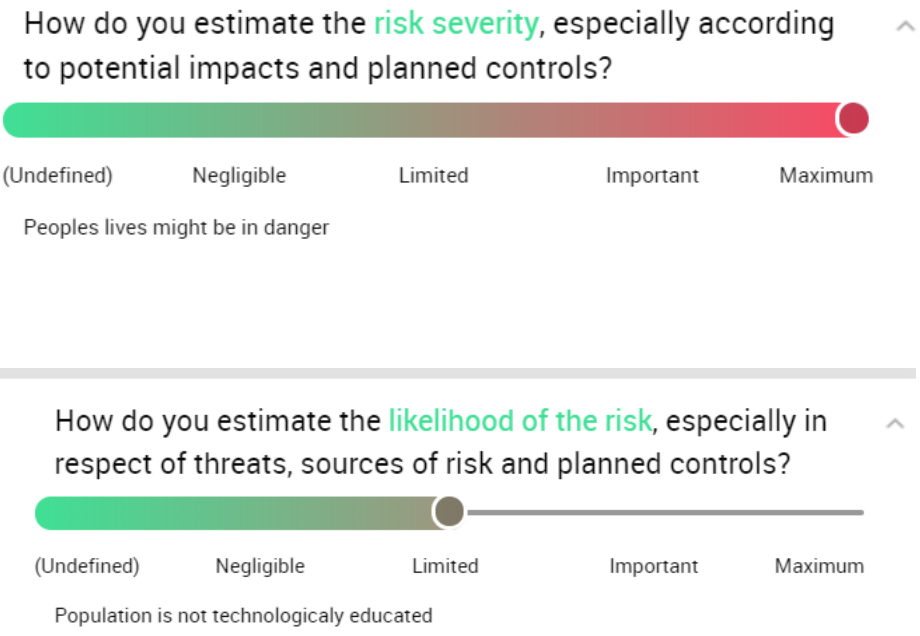
πρέπει να παραμένει ακέραιη και ανέπαφη. Άλλωστε αυτή διευκολύνει και τη δουλειά της ελληνικής υπηρεσίας ασύλου, η οποία θα πρέπει να γνωρίζει τα πλήρη στοιχεία του κάθε ωφελούμενου. Μία αλλοίωση δεδομένων αυτών πιθανά να οδηγήσει και σε υπόθαλψη εγκληματία και για το λόγω αυτό η διαφύλαξή τους με κάθε τρόπο και μέσο είναι ιδιαίτερα σημαντική. Πηγές κινδύνου και στην περίπτωση αυτή είναι κατά βάση επίδοξοι εγκληματίες που αποσκοπούν είτε σε εκμαίευση χρημάτων με δόλιο τρόπο είτε σε απειλές κατά της σωματικής ακεραιότητας και της ζωής. Με στόχο να προστατευθούν τα δεδομένα αυτά λοιπόν, γίνεται φυσικός έλεγχος του χρήστη ο οποίος έχει ένα μοναδικό κωδικό για τον υπολογιστή του και στη συνέχεια δίδεται μυστικός κωδικός για πρόσβαση στη λίστα. Επιπρόσθετα γίνονται συχνά backups και ελέγχονται οι υπολογιστές για ενδεχόμενες βλάβες από κακόβουλο λογισμικό.





Εικόνα 18 : Κίνδυνοι, απειλές κα έλεγχος του αρχείου

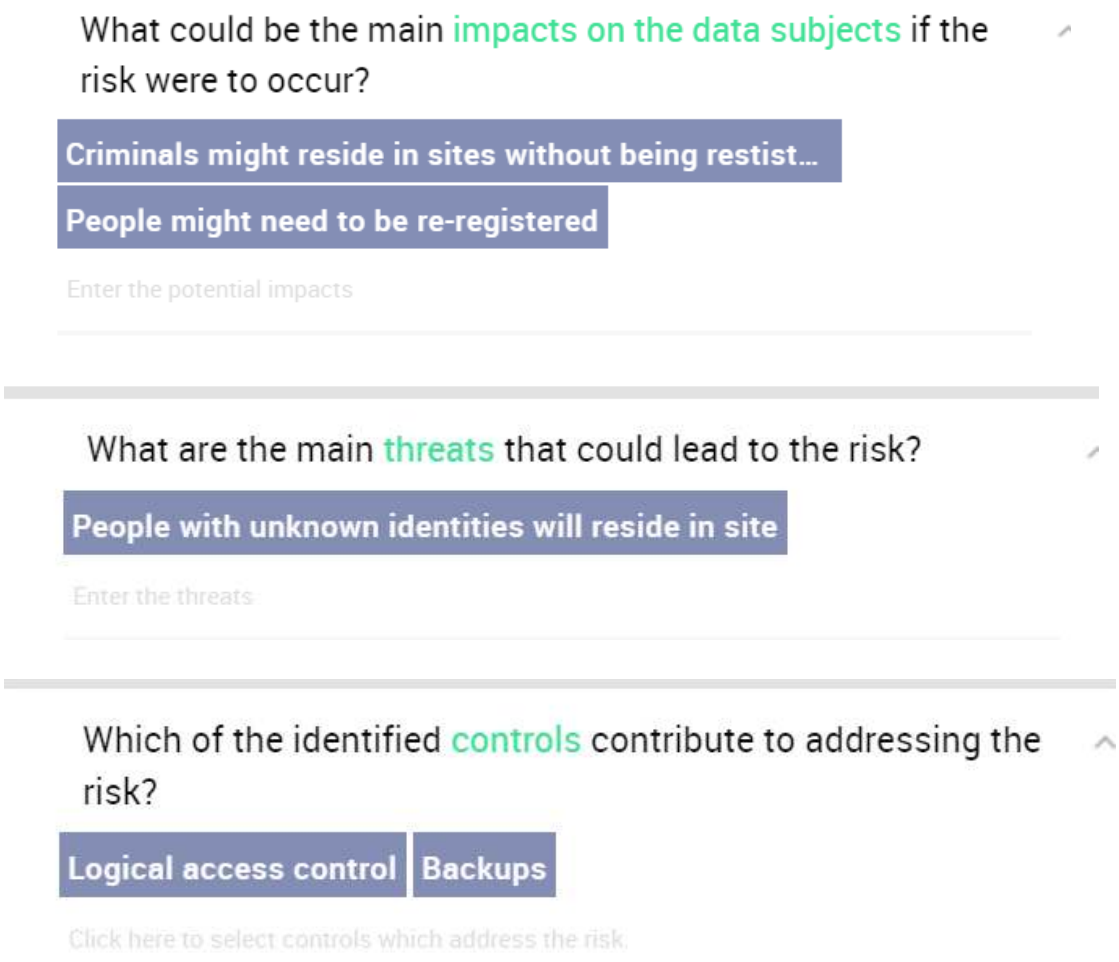
Η σοβαρότητα του κινδύνου είναι προφανώς και πάλι ιδιαίτερα μεγάλη, καθώς πρόκειται για δεδομένα ανθρώπων που αιτούνται διεθνούς προστασίας. Παρόλα αυτά, μέχρι στιγμής η πιθανότητα ανεπιθύμητης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι μεσαίας έως και μικρής πιθανότητας καθώς δεν έχουν σημειωθεί προσπάθειες απώλειας της λίστας ανά την επικράτεια, ενώ την ίδια στιγμή το γνωστικό επίπεδο των ανθρώπων αυτών σε θέματα τεχνολογίας φαίνεται να παραμένει χαμηλό.



Εικόνα 19 : Βαθμός και πιθανότητα κινδύνου

Κίνδυνοι ελλοχεύουν επίσης, εάν για κάποιο λόγο δεδομένα από τη λίστα διαγραφούν. Μάλιστα η πιθανότητα αυτή μπορεί να έχει κάποιες σχετικά μικρές συνέπειες, όπως το ότι

κάποιοι ενδεχόμενα να πρέπει να επαναπροσκομίσουν τα έγγραφά τους, ώστε να επανεγγραφούν σε αυτή, αλλά και κάποιες ιδιαίτερα σοβαρές, όπως το να διαμένουν στη δομή εγκληματίες οι οποίοι δεν είναι εγγεγραμμένοι και άρα δε δύνανται να εντοπιστούν. Όπως και στις άλλες περιπτώσεις, έτσι και στην περίπτωση της διαγραφής των δεδομένων, καταβάλλεται μέγιστη προσπάθεια ώστε η λίστα να είναι προστατευμένη με δικλείδες ασφαλείας και άρα η πρόσβαση σε αυτή να μην είναι μία ιδιαίτερα εύκολη διαδικασία.



Εικόνα 20 : Κίνδυνοι, απειλές κα έλεγχος του αρχείου

Ο βαθμός του κινδύνου στην περίπτωση αυτή είναι μέτριας σημασίας καθώς είναι ιδιαίτερα δύσκολο να διαγραφούν τελείως τα αρχεία και η πιθανότητα αυτού εξίσου μέτρια καθώς δεν έχουν εντοπιστεί προσπάθειες παραβίασης οποιουδήποτε συστήματος.

Εικόνα 21 : Βαθμός και πιθανότητα κινδύνου

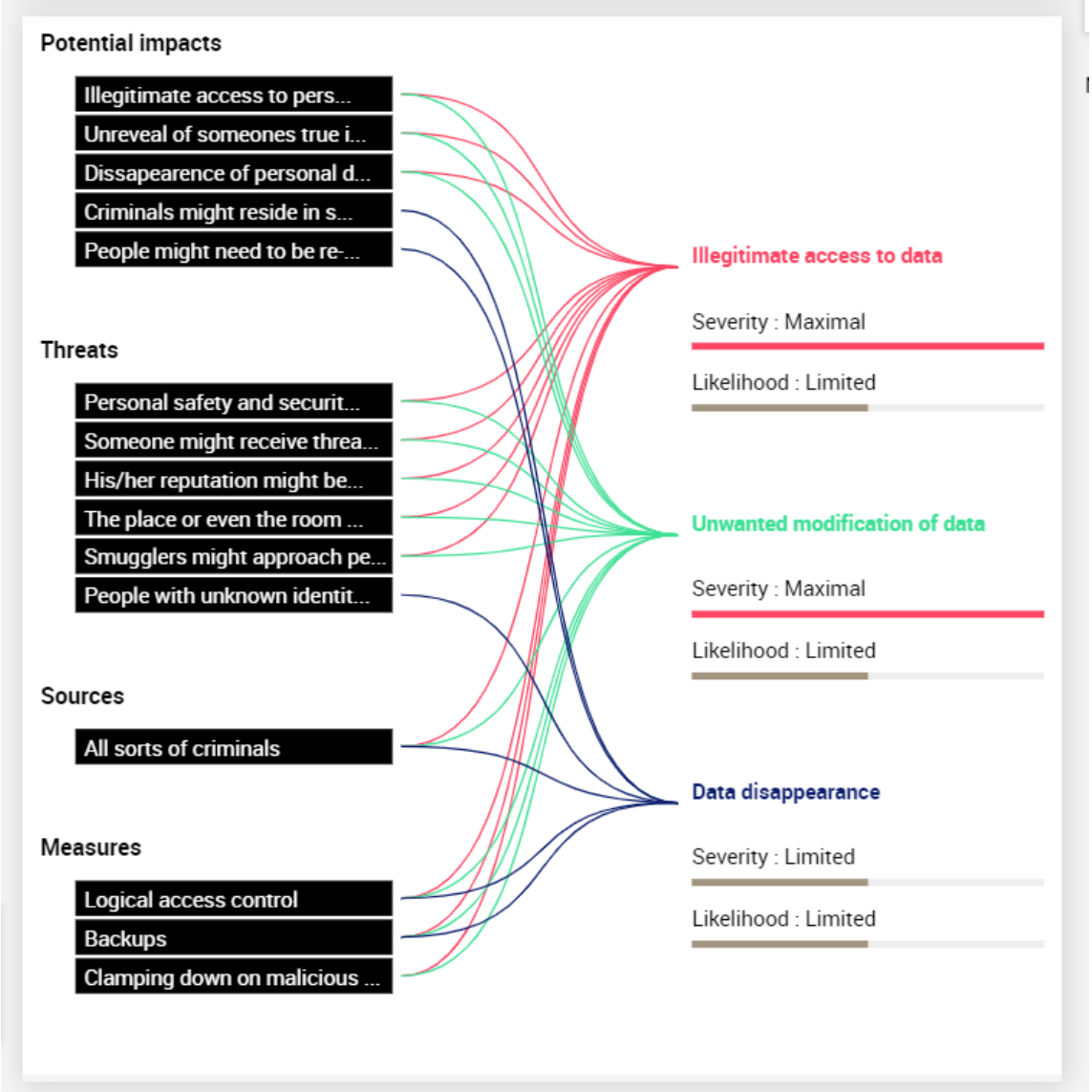
5. Συμπεράσματα

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR - 2016/679) της ΕΕ αποτελεί τη μεγαλύτερη αλλαγή στην νομοθεσία περί προστασίας των δεδομένων τα τελευταία 20 χρόνια και έχει άμεση εφαρμογή σε όλα τα Κράτη-Μέλη από 25/05/2018 χωρίς την προϋπόθεση κρατικής νομοθεσίας. Στόχος της εφαρμογής του κανονισμού αυτού είναι να ενισχύσει το προηγούμενο νομικό πλαίσιο αλλά και να προστατεύσει τα θεμελιώδη δικαιώματα των φυσικών προσώπων με τον ίδιο ακριβώς τρόπο για όλα τα κράτη μέλη. Ο Κανονισμός 2016/679 έχει εφαρμογή σε όλους τους φορείς (ιδιωτικές και δημόσιες επιχειρήσεις, κρατικές αρχές, συλλόγους, κλπ.) που διαχειρίζονται, επεξεργάζονται, αποθηκεύουν και διακινούν δεδομένα προσωπικού χαρακτήρα, είτε έχουν έδρα και δραστηριότητα σε χώρα της Ευρωπαϊκής Ένωσης είτε όχι, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες.

Ιδιαίτερα σημαντική καινοτομία, η οποία εισάγεται από το νέο κανονισμό, είναι το γεγονός ότι πλέον η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει το δικαίωμα του ελέγχου συμμόρφωσης προς τον κανονισμό, αλλά και της επιβολής κυρώσεων σε όποιον δε συμμορφώνεται με αυτό.

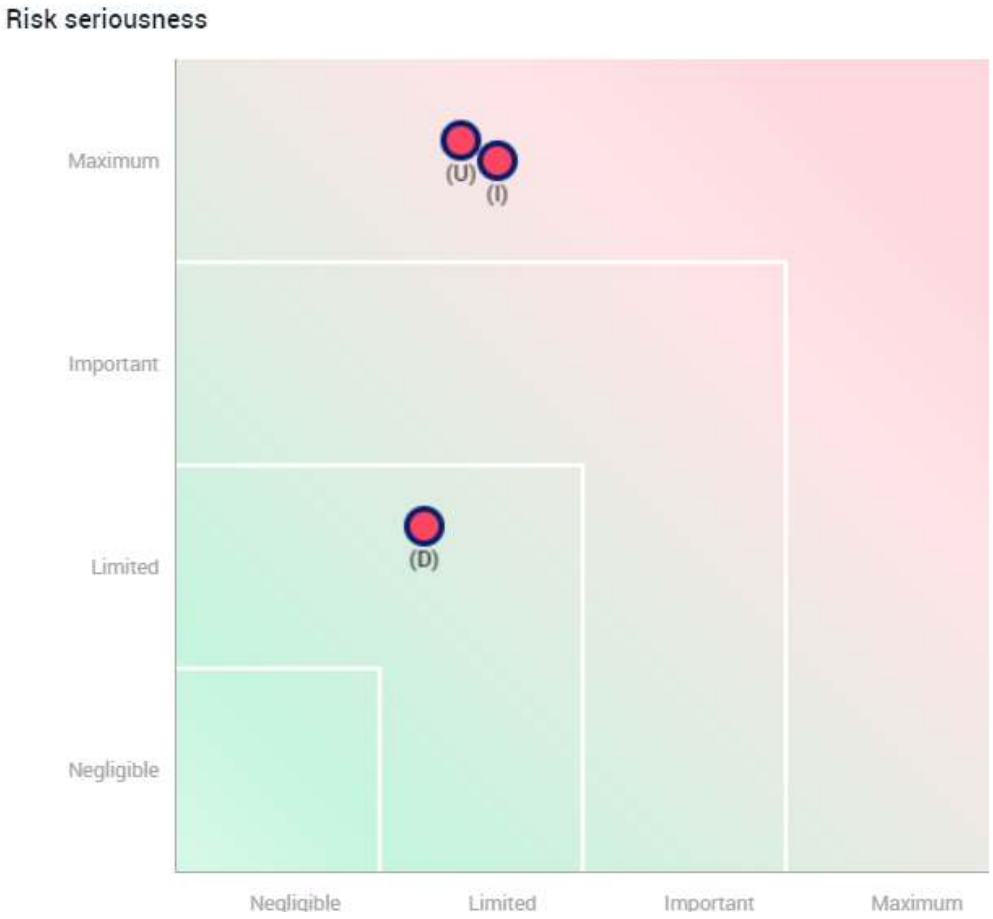
Η παρούσα εργασία, μελετά έναν Μη Κερδοσκοπικό Οργανισμό ο οποίος δραστηριοποιείται σε μία δομή φιλοξενίας προσφύγων και διατηρεί μια πληθυσμιακή λίστα των όσων φιλοξενούνται στη δομή. Ο οργανισμός, παρέχοντας υποστήριξη στη διοίκηση της δομής είναι υποχρεωμένος να διατηρεί και να επεξεργάζεται τη λίστα αυτή η οποία ουσιαστικά καταγράφει τον κάθε ωφελούμενο με στοιχεία που τον χαρακτηρίζουν μονοσήμαντα. Η λίστα, αφού επεξεργαστεί, δηλαδή προστεθούν σε αυτή ωφελούμενοι ή διαγραφούν από αυτή, διαμοιράζεται σε ένα αριθμό χρηστών – λοιπόν φορέων, ώστε αυτοί να έχουν πρόσβαση αυτή και ενημέρωση για αφίξεις – αναχωρήσεις από τη δομή.

Οι κίνδυνοι που προκύπτουν από τη μη εξουσιοδοτημένη πρόσβαση στη λίστα αυτή, αφορούν κυρίως σε απειλές κατά της ζωής και της σωματικής ακεραιότητας των ανθρώπων αυτών ή σε προσβολή αυτών. Ακόμη, σε εξαιρετικές περιπτώσεις ενδέχεται λόγω της διαγραφής ή της μεταποίησης των στοιχείων άνθρωποι με αμφίβολο παρελθόν να κατορθώσουν να κρυφτούν στις δομές. Στην εικόνα που ακολουθεί, παρουσιάζεται μία χαρτογράφηση των κινδύνων και το πως αυτοί συνδέονται με την κάθε κακόβουλη προς τη λίστα.



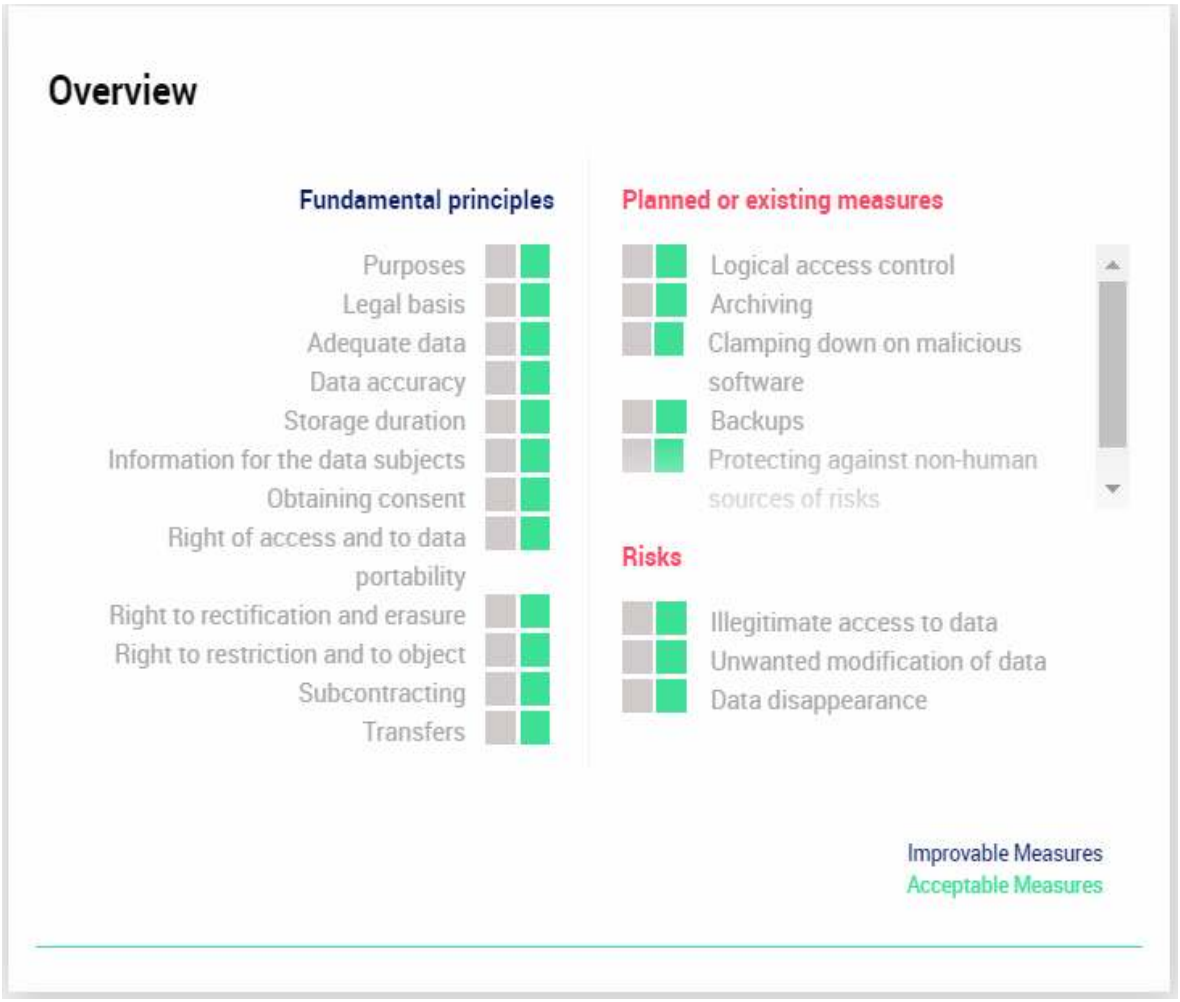
Εικόνα 22 : Χαρτογράφηση κινδύνων

Όπως είναι αντιληπτό, ιδιαίτερα υψηλός είναι ο βαθμός του κινδύνου όταν υπάρχει μη εξουσιοδοτημένη πρόσβαση στη λίστα, αλλά και όταν υπάρχει τροποποίηση αυτής, ενώ λίγο χαμηλότερος είναι ο βαθμός κινδύνου από διαγραφή στοιχείων. Βέβαια, η πιθανότητα να συμβούν τα παραπάνω είναι μέτριου επιπέδου καθώς έως τώρα δεν έχουν σημειωθεί σοβαρές προσπάθειες παραβίασης και υποκλοπής των αρχείων.



Εικόνα 23 : Σοβαρότητα και πιθανότητα κινδύνου

Η τελική αξιολόγηση της μεθόδου και των μέτρων που χρησιμοποιούνται έδειξε πως δεδομένων των πόρων, των τεχνικών γνώσεων του υπευθύνου ασφαλείας αλλά και των τεχνικών γνώσεων των χρηστών, τα μέτρα που έχου ληφθεί είναι επαρκή και προστατεύουν σε έναν αρκετά μεγάλο βαθμό τα δεδομένα προσωπικού χαρακτήρα των όσων διαμένουν στη δομή φιλοξενίας προσφύγων. Μέχρι στιγμής δεν έχουν ανιχνευθεί προσπάθειες παραβίασης ούτε των προσωπικών υπολογιστών των εργαζομένων αλλά ούτε και της ηλεκτρονικής τους αλληλογραφίας ώστε να εφαρμοστούν επιπλέον μέτρα διασφάλισης κινδύνου. Θεωρείται λοιπόν, πως με την πολιτική που ακολουθείται έως σήμερα, τα δεδομένα παραμένουν ασφαλή και διαμοιράζονται ως πρέπει στους εξουσιοδοτημένους χρήστες.



Εικόνα 24 : Τελική αξιολόγηση της μεθόδου

Βιβλιογραφία

Bird, & Bird. (2017). *Guide to the General Data Protection Regulation.*

Calder, A. (2016). *EU GDPR : A Pocket Guide.*

CNIL. (2020). Ανάκτηση από https://www.cnil.fr/

ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων. (2016). https://www.privacy-regulation.eu/el/r71.htm.

European Union. (2017). EU General Data Protection Regulation (GDPR) : An Implementation and Compliance Guide. IT Governance Organization.

Ακριβοπούλου, Χ. (2011). Η ιδιωτικότητα του προσώπου μέσα από τη συνθετική αντίθεση δημόσιου - ιδιωτικού. *Επιστήμη και Κοινωνία* .

Ακριβοπούλου, Χ. (2012). *Το δικαίωμα στην ιδιωτική ζωή.* Αθήνα: Σάκκουλας.

Αλεξανδροπούλου - Αιγυπτιάδου , Ε. (2016). *Προσωπικά Δεδομένα.* Αθήνα: Νομική Βιβλιοθήκη.

Αρκουλή, Κ. (2010). *Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.* Αθήνα: Νομική Βιβλιοθήκη.

Αρμαμέντος, Π., & Σωτηρόπουλος, Β. (2005). *Προσωπικά Δεδομένα - Ερμηνεία Ν.2472/1997.* Αθήνα: Σάκκουλας.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2015). Ετήσια 'Εκθεση.

Αυγουστιανάκης, Μ. (2001). *Προστασία του ατόμου από την επεξεργασία προσωπικών.* Δικαιώματα του Ανθρώπου.

Γιαννακούλα, Α., & Μηλαπίδου, Μ. (2017). *Προσωπικά Δεδομένα.* Αθήνα: Νομική Βιβλιοθήκη.

Γιαννόπουλος, Γ. (2017). Γενικός Κανονισμός Προστασίας Δεδομένων: οι νέες υποχρεώσεις και η ευθύνη του Υπευθύνου Επεξεργασίας. *Εφημερίδα Διοικητικού Δικαίου* , 199-205.

Γκρίτζαλης, Σ., & Γκρίτζαλης, Δ. (2004). *Ασφάλεια Δικτύων Υπολογιστών.* Αθήνα: Πολιτεία.

Γκριτζαλης, Σ., Λαμπρινουδάκης, Κ., Κάτσικας, Σ., & Μήτρου, Λ. (2010). *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και τηλεπικοινωνιών.* Αθήνα: Παπασωτηρίου.

Καλαντζής , Π. (2017). *Στρατηγική συμμόρφωσης με το γενικό κανονισμό προστασίας προσωπικών δεδομένων - A practical guide to GDPR.*

Μήτρου, Λ. (2017). *Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων.* Αθήνα: Σάκκουλα.

Σ Ε Β. (2018). Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR). Αθήνα: Σύνδεσμος Ελλήνων Βιομηχάνων.

Σασιάκος, Κ., Αναστασίου, Σ., & Τούντας, Κ. (2017). Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης.

Υπουργείο Δικαιοσύνης. (2018). Ανάκτηση από http://www.opengov.gr/ministryofjustice/?p=9331