ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων
Κατεύθυνση : Ασφάλεια Ψηφιακών Συστημάτων

Διπλωματική Εργασία

«ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ»

Φοιτητής : **Σταματόπουλος Δημήτριος (ΜΤΕ 1536)**

Επιβλέπων Καθηγητής : **Λαμπρινουδάκης Κωνσταντίνος**

Πειραιάς, Μάιος 2018

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένεια μου, η οποία με στήριξε και συνεχίζει να με στηρίζει με όλες τις δυνάμεις της σε κάθε ακαδημαϊκό και επαγγελματικό μου βήμα. Επίσης οφείλω να ευχαριστήσω θερμά τον Καθηγητή του Τμήματος Ψηφιακών Συστημάτων κ. Λαμπρινουδάκη Κωνσταντίνο, για την ανάθεση της εν λόγω εργασίας που αποτέλεσε για εμένα εφαλτήριο διεύρυνσης των γνώσεων μου σε έναν δυναμικά εξελισσόμενο πεδίο. Τέλος, θα ήθελα να ευχαριστήσω θερμά τον επιστημονικό συνεργάτη του Τμήματος Ψηφιακών Συστημάτων κ. Νικόλαο Λουκά, για την αμέριστη υποστήριξη και καθοδήγηση καθ' όλη τη διάρκεια εκπόνησης της παρούσας διπλωματικής μεταπτυχιακής εργασίας .

Πειραιάς, Οκτώβριος 2017

Σταματόπουλος Δημήτριος

Περίληψη

Οι ψηφιακές υπηρεσίες υγεία έχουν επηρεάσει τον τομέα υγειονομικής περίθαλψης εισάγοντας μεγάλες καινοτομίες, βελτιώνοντας την ποιότητα της περίθαλψής και ενισχύοντας τη σχέση ιατρού-ασθενούς. Ωστόσο, λόγω της φύση τους, οι υπηρεσίες αυτές συλλέγουν και διαχειρίζονται εξαιρετικά ευαίσθητα δεδομένα και ως εκ τούτο πρέπει να συμμορφώνονται με τις απαιτήσεις ασφάλειας και προστασίας της ιδιωτικής ζωής που ορίζονται από τους νόμους περί προστασίας δεδομένων. Η ανάπτυξη της τεχνολογίας διαχείρισης των συλλεγόμενων δεδομένων σύμφωνα με τους νόμους και ειδικά για τον νέο κανονισμό που θεσπίστηκε για την προστασία δεδομένων προσωπικού χαρακτήρα αποτελεί μια κρίσιμη, δαπανηρή και δυνητικά εξαιρετικά επικίνδυνη δραστηριότητα λόγω της πιθανότητας απώλειας δεδομένων, κλοπών και κυρώσεων. Επιπλέον, το νομικό πλαίσιο της Ευρωπαϊκής Ένωσης είναι εξελισσόμενο. Αυτό το καθιστά δύσκολο ως προς τη κατανόηση, όπως και η εφαρμογή των απαιτήσεων που αυτό ορίζει σε πολλές περιπτώσεις είναι δύσκολο να μεταφραστούν ορθά ώστε να εξασφαλίσουν τη συμμόρφωση.

Στο πλαίσιο αυτής τη μελέτης είναι ο καθορισμός, η παρουσίαση και η ανάλυση των αρχικών βημάτων που θα μπορούσαν να ακολουθήσουν οι πάροχοι ψηφιακών υπηρεσιών υγείας, προκειμένου να προετοιμαστούν σύμφωνα με τις νέες απαιτήσεις και δεσμεύσεις που εισήχθησαν από τον γενικό κανονισμό για την προστασίας δεδομένων (GDPR). Αυτή η μελέτη επιδίωξε να παράσχει μια λεπτομερή προσέγγιση και μεθοδολογία για την (1) καταγραφή –ροή δεδομένων (2) εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων (3) ανάλυση αποκλίσεων. Για την καλύτερη παρουσίαση του θεωρητικού μέρους που εισάγετε από τον κανονισμό, θα χρησιμοποιήσω ένα σενάριο μελέτης περίπτωσης βασισμένο σε μια εταιρεία που δραστηριοποιείται στις υπηρεσίες υγειονομικής περίθαλψης αναπτύσσοντας εφαρμογές για την παροχή βοήθειας σε χρόνιους ασθενείς και ηλικιωμένους.

Λέξεις κλειδιά: GDPR, ιδιωτικότητα δεδομένων, ευαίσθητα δεδομένα, καταγραφή δεδομένων, ροή δεδομένων, ανάλυση αποκλίσεων, αξιολόγηση αντικτύπου δεδομένων προσωπικού χαρακτήρα

Abstract

Digital health services are disrupting the healthcare sector by injecting huge innovation, improving the quality of care and strengthening the doctor-patient relationship. However, by their very nature, such services collect and manage extremely sensitive data and therefore need to comply with security and privacy requirements defined by data protection laws. To develop the technology for managing collected data in accordance with laws and especially for the new introduced regulation for the data privacy represents a painful, costly, and potentially extremely risky activity due to the possibility of data loss, thefts and penalties. Moreover, the EU legal framework is very fragmented and rapidly evolving. This makes it very difficult to understand, not to mention extracting and implementing data protection requirements to ensure compliance.

In the scope of this study was to define, present and analyze the first steps a digital health services provider might be follow in order to be prepared under the new requirements and commitments introduced from the GDPR. This study also sought to produce a detailed approach and methodology for (1) Data Inventorying - Flows (2) Data Protection Impact Assessment and (3) Gap Analysis. For the purpose of modeling and visualizing the theoretical models on to practical and better understanding outputs with countable results, I am using a case study scenario based on a startup company operates on the healthcare services by developing mobile applications for helping chronic patients and seniors .

Keywords: GDPR, data privacy, sensitive data, data inventorying, data flow, Gap analysis, Data Protection Impact Assessment,

Πίνακας Περιεχομένων

Κεφάλαιο 1. Εισαγωγή

1.1 Δεδομένα υγείας και ψηφιακές υπηρεσίες

Οι ψηφιακές υπηρεσίες υγείας που εξελίσσονται από τους παρόχους υπηρεσιών υγείας, πλέον δίνουν την δυνατότητα μέσω εφαρμογών για έξυπνα κινητά τηλέφωνα αλλά και διαδικτυακών πλατφορμών, στους χρήστες τους να παρακολουθούν τα δεδομένα υγείας τους και να τα διαμοιράζονται με νοσοκομεία, γιατρούς αλλά και ασφαλιστικούς παρόχους υγείας για ώστε να βελτιώνονται οι υπηρεσίες υγείας που τους παρέχονται.

Οι εφαρμογές ψηφιακής υγείας είναι κατά βάση σύννεφο-κεντρικές (cloud-based) και χρησιμοποιούνται όλο και περισσότερο από πολίτες, γιατρούς, νοσοκομεία και ασφαλιστικές εταιρείες. Υπάρχουν περίπου 300.000 εφαρμογές υγείας παγκοσμίως και το 60% αυτών αναπτύσσεται από φορείς και νεοσύστατες επιχειρήσεις. Το αποτέλεσμα είναι: "Το 92% των παρόχων υγειονομικής περίθαλψης χρησιμοποιεί ήδη μια υπηρεσία στο σύννεφο"[1]

Αυτή η τάση παράγει τεράστιες ποσότητες δεδομένων υγείας που αποθηκεύονται, επεξεργάζονται και μεταφέρονται μέσω του cloud. Αυτή η μετάβαση στις τεχνολογίες που προσφέρει το cloud αποτελεί πρόκληση για όλους τους εμπλεκόμενους παράγοντες: από τις κυβερνήσεις οι οποίες θα πρέπει να αλλάξουν τους εγχώριους νόμους, μέχρι τους προγραμματιστές και τις εταιρείες που σχεδιάζουν και υλοποιούν εφαρμογές υγείας. Πλέον όλοι έχουν να αντιμετωπίσουν και τις νέες προκλήσεις που εισάγονται μέσω του νέου γενικού κανονισμού της ΕΕ για την προστασίας των δεδομένων (GDPR) .

[1] “83% Of Healthcare Organizations Are Using Cloud-Based Apps Today”, Forbes, https://goo.gl/QHe9JW

1.2 Αντικείμενο διπλωματικής

Μέσω της παρούσας διπλωματικής εργασίας, θα γίνει η προσπάθεια να αποτυπωθούν οι μεθοδολογίες καθώς και οι πρακτικές που ακολουθήθηκαν και εφαρμόσθηκαν στην περίπτωση νεοσύστατης εταιρείας καινοτομίας που δραστηριοποιείται στον κλάδο της ανάπτυξης εφαρμογών και ηλεκτρονικών υπηρεσιών υγείας, ώστε να προετοιμαστεί και να θέσει τις βάσεις που θα την φέρουν πιο κοντά στην συμμόρφωση με τον νέο γενικό κανονισμό για τη προστασία των δεδομένων (GDPR) της ΕΕ. Η ανάπτυξη συγκεκριμένων μεθοδολογιών για την σωστή πορεία της εταιρείας ή του οργανισμού προς την εκπλήρωση συμμόρφωσης με τον κανονισμό, αποτελεί ξεκάθαρο στόχο ο οποίος για να εκπληρωθεί θα πρέπει να βασιστεί σε μεθοδολογίες και πρακτικές που σχεδιάζονται, δημιουργούνται και εφαρμόζονται με βάση τα άρθρα του GDPR και όπως αυτά ερμηνεύονται στο σύνολο του κανονισμού. Για αυτό το σκοπό η παρούσα εργασία θα περιγράψει και θα παρουσιάσει: α) Μεθοδολογία καταγραφής και αποτύπωσης δεδομένων (Data Inventorying) η οποία αποτελεί βασικό και πρωτεύον σημείο εκκίνησης για την κατανόηση σχετικά με τον τύπο και την χρησιμότητα των δεδομένων που συλλέγει η εν λόγω εταιρεία και χρησιμοποιεί για την δημιουργία ηλεκτρονικών υπηρεσιών, β) Μεθοδολογία εκτίμησης των επιπτώσεων σχετικά με την προστασία των δεδομένων (DPIA), τα αποτελέσματα της οποίας δίνουν την δυνατότητα στην επιχείρηση να αντιληφθεί τον αντίκτυπο σε πιθανά σενάρια μη τήρησης ορθών πρακτικών για την προστασία των προσωπικών δεδομένων όπως αυτά ορίζονται από τον κανονισμό, γ) ανάλυση αποκλίσεων (GAP Analysis) σύμφωνα με την οποία η εταιρεία θα μπορεί να αξιολογήσει το βαθμό εκπλήρωσης των προ απαιτούμενων όπως αυτά ορίζονται από τον κανονισμό.

Η προαναφερθείσα εταιρεία στο εξής θα ονομάζεται ως «*AHealth A.E*» για λόγους διασφάλισης της ανωνυμίας της, καθώς και των στοιχείων που θα παρατεθούν στην εν λόγω εργασία μέσω πινάκων, παραρτημάτων και εικόνων.

1.3 Οργάνωση Κειμένου

Η ανάπτυξη της παρούσας εργασίας γίνεται σε τέσσερα κεφάλαια, στα οποία επιχειρείται αφενός η ορθή ανάπτυξη του θέματος όπως επίσης και η παροχή στον αναγνώστη, του κατάλληλου θεωρητικού υποβάθρου πως θα τον βοηθήσει στην κατανόηση της τελικής μελέτης περίπτωσης.

Στο 1ο Κεφάλαιο γίνεται η αναφορά στο σκοπό της εργασίας, στο αντικείμενο της καθώς και στα θέματα που θα επιχειρηθεί να δοθούν απαντήσεις. Ο σκοπός της εργασίας περιγράφεται σε σχέση με συγκεκριμένα ζητήματα που προκύπτουν από την εφαρμογή του γενικού κανονισμού για την προστασία δεδομένων. Το 2ο Κεφάλαιο είναι βασικό για τον αναγνώστη μιας και δίνεται η δυνατότητα, να γνωρίσει βασικές έννοιες που εισήχθησαν με τον νέο κανονισμό, αποτελώντας το θεωρητικό υπόβαθρο που χρειάζεται ώστε να μπορέσει να κατανοήσει τις μεθοδολογίες και τις αναφορές που θα αναπτυχθούν στην συνέχεια. Οι υπηρεσίες υγείας που αφορούν την μελέτη περίπτωσης που έχει επιλεχθεί, καθώς και οι εξελίξεις στο χώρο των υπηρεσιών αυτών αναπτύσσονται στο 3ο Κεφάλαιο, όπως επίσης και το πως επηρεάζονται από τον νέο κανονισμό προστασίας των δεδομένων. Στο 4ο Κεφάλαιο γίνεται λεπτομερής ανάλυση των μεθοδολογιών για τα θέματα συμμόρφωσης με τον κανονισμό όπως αυτά έχουν αναφερθεί στον σκοπό της εργασίας, οι μεθοδολογίες για την εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων, η καταγραφή - ροές δεδομένων και η ανάλυση αποκλίσεων από τον κανονισμό. Η παρούσα εργασία κλείνει με το Κεφάλαιο 5ο στο οποίο παρουσιάζονται τα αποτελέσματα από την εφαρμογή των μεθοδολογιών και πρακτικών του προηγούμενου κεφαλαίου σε μελέτη περίπτωσης από τον κλάδο των ηλεκτρονικών υπηρεσιών υγείας που έχει επιλεχθεί. Στον επίλογο του Κεφαλαίου 6 συνοψίζουμε τα αποτελέσματα της εργασίας και περιγράφονται τα συμπεράσματα μας από την εκπόνηση.

Κεφάλαιο 2. Θεωρητικό υπόβαθρο

Γενικός κανονισμός προστασίας προσωπικών δεδομένων

Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων (GDPR) είναι ο νέος κανονισμός περί προστασίας των προσωπικών δεδομένων της Ευρωπαϊκής Ένωσης, ο οποίος έρχεται να αντικαταστήσει την οδηγία για την προστασία των δεδομένων (Data Protection Directive), η οποία είναι σε ισχύει από το 1995. Αν και η οδηγία 95/46/ΕΚ έπρεπε να εφαρμοστεί από κάθε κράτος μέλος για την προστασία των δεδομένων και είχε στόχο ένα εναρμονισμένο και σύγχρονο καθεστώς προστασίας δεδομένων σε ολόκληρη την Ευρώπη ο στόχος δεν επιτεύχθηκε πλήρως λόγω των διαφορών στις διάφορες εθνικές εφαρμογές (Hansen, 2016).

Το 2016, περισσότερο από 20 χρόνια αργότερα, ο διάδοχος της οδηγίας για την προστασία των δεδομένων εγκρίθηκε μετά από αρκετά χρόνια συζήτησης και διαπραγμάτευσης ο οποίος ονομάστηκε Γενικός Κανονισμός Προστασίας Δεδομένων – General Data Protection Regulation (GDPR) (Regulation, 2016) με κύριους στόχους ξανά της εναρμόνισης και του εκσυγχρονισμού που επιδιωκόταν. Το GDPR θα τεθεί σε ισχύ στις 25 Μαΐου 2018. Η άμεση εφαρμογή του σε όλα τα κράτη μέλη θα συμβάλει στην ενοποίηση του επιπέδου προστασίας δεδομένων. Ωστόσο, οι περίπου 70 ρήτρες – άλλες υποχρεωτικές και άλλες προαιρετικές – παρέχουν τα μέσα για τις δικές τους εθνικές απαιτήσεις και ως εκ τούτου απόκλιση από μια κοινή στρατηγική σε όλα τα κράτη μέλη (Roßnagel & Nebel, 2016).

Το περιεχόμενο του κανονισμού οργανώνεται ως εξής: Στο 2ο τμήμα του σκιαγραφούνται οι σημαντικές ιδιότητες του Ευρωπαϊκού Κανονισμού για την Γενική Προστασία Δεδομένων που απορρέει από την ευρωπαϊκή πρωτοβουλία μεταρρύθμισης της προστασίας δεδομένων. Στο 3ο τμήμα παρουσιάζεται η έννοια της "προστασίας της ιδιωτικής ζωής από σχεδιασμό" και παρέχει σύντομες πληροφορίες για το ιστορικό και τους ορισμούς. Στο 4ο και 5ο τμήμα απαριθμούνται οι νομικές υποχρεώσεις σχετικά με την προστασία των δεδομένων από το σχεδιασμό και την προστασία των δεδομένων. Τέλος, στο 6ο και τελευταίο τμήμα συνοψίζονται τα συμπεράσματα και δίνεται ένας επίλογος (Hansen, 2016). Θα πρέπει να σημειωθεί στο σημείο αυτό ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν αποτελεί πανάκεια για την προστασία των δεδομένων, εξάλλου δεν είναι όλα καινούργια στον κανονισμό ενώ τα 99 άρθρα του αφήνουν περιθώρια για ερμηνεία. Η επιλεγμένη αφαίρεση νομικού κειμένου από τον κανονισμό είναι ένα επιδιωκόμενο χαρακτηριστικό και όχι ένα σφάλμα: Οι αφηρημένοι κανόνες πρέπει να

τεκμηριώνονται με τέτοιο τρόπο έτσι ώστε να είναι κατάλληλοι σε σχέση με τους συνεχώς μεταβαλλόμενους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και να είναι αποδεκτοί ως εποπτικές αρχές από τους Ευρωπαίους επιτρόπους προστασίας δεδομένων. Έτσι, ο Γενικός Κανονισμός Προστασίας Δεδομένων ορίζει μια διαδικασία για την επίτευξη συνεκτικής ερμηνείας των νομικών υποχρεώσεων που αφορούν τις περιπτώσεις διασυνοριακών συναλλαγών. Με αυτό, ο κανονισμός μπορεί να καταφέρει να είναι ανθεκτικός στο μέλλον για πολλά χρόνια ή ακόμα και πολλές δεκαετίες - σε αντίθεση με τον προκάτοχό του. Ωστόσο, η συνεχής διαπραγμάτευση σχετικά με την τεκμηρίωση των αφηρημένων κανόνων είναι χρονοβόρα και ενδέχεται να επηρεαστούν από ομάδες πίεσης που δεν μοιράζονται τον ίδιο στόχο σχετικά με την βέλτιστη προστασία των δεδομένων (Hansen, 2016). Πρέπει να σημειωθεί ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν απευθύνεται μόνο σε ευρωπαίους υπευθύνους επεξεργασίας δεδομένων, αλλά αποσκοπεί στην εξασφάλιση της προστασίας των δεδομένων σε ολόκληρη την ευρωπαϊκή αγορά. Η αρχή της θέσης της αγοράς που ορίζεται στο άρθρο 3 του κανονισμού απευθύνεται σε οργανισμούς που προσφέρουν αγαθά ή υπηρεσίες σε άτομα στην ΕΕ ή παρακολουθούν τη συμπεριφορά τους, ακόμη και αν οι οργανώσεις δεν είναι εγκατεστημένες στην επικράτεια της Ευρωπαϊκής Ένωσης. Συγκεκριμένα, οι εταιρείες που δεν είναι μέλη της ΕΕ και κυριαρχούν στην ψηφιακή αγορά πρέπει να συμμορφώνονται με τις απαιτήσεις προστασίας των δεδομένων του κανονισμού (Hansen, 2016).

Εάν ο Γενικός Κανονισμός Προστασίας Δεδομένων θα παράσχει τα κατάλληλα μέσα για την επίτευξη της προστασίας δεδομένων δεν μπορεί να προβλεφθεί σε αυτό το πρώιμο στάδιο. Ωστόσο, σαφώς τα ευρωπαϊκά κράτη μέλη έχουν ένα κοινό σημείο εκκίνησης να το πάρουν από εκεί. Αυτό ισχύει για όλα τα όργανα που περιγράφονται στον κανονισμό π.χ. η προστασία δεδομένων από το σχεδιασμό, η προστασία των δεδομένων από προεπιλογή, η αξιολόγηση των επιπτώσεων στην προστασία δεδομένων, οι κώδικες δεοντολογίας, οι πιστοποιήσεις, οι κυρώσεις ή η εμπλοκή των δικαστηρίων (Hansen, 2016).

Μεταξύ των πιο αξιοσημείωτων αλλαγών, το GDPR παρέχει στους Ευρωπαίους πολίτες μεγαλύτερο έλεγχο στα προσωπικά δεδομένα και επιβάλει πολλές νέες υποχρεώσεις σε οργανισμούς που συλλέγουν, χειρίζονται ή αναλύουν προσωπικά δεδομένα. Το GDPR παρέχει επίσης στις εθνικές ρυθμιστικές αρχές νέες εξουσίες για την επιβολή σημαντικών προστίμων σε όσους παραβιάζουν τον κανονισμό, ο οποίος θα ενσωματώνεται ως εθνική νομοθεσία στα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Η εφαρμογή του GDPR ξεκινάει στις 25 Μάιου 2018 παρότι ως Ευρωπαϊκή νομοθεσία έχει ψηφιστεί από τον Απρίλιο του 2016. Λόγω των σημαντικών αλλαγών που θα πρέπει προβούν οργανισμοί και εταιρείες, ώστε να ευθυγραμμιστούν με τον κανονισμό, συμπεριλήφθηκε μια μεταβατική περίοδος δυο ετών.

2.2 Κύριες απαιτήσεις του GDPR

Το GDPR επιβάλλει ένα ευρύ φάσμα απαιτήσεων σε οργανισμούς που συλλέγουν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένης της απαίτησης συμμόρφωσης με έξι βασικές αρχές:

- Διαφάνεια, δικαιοσύνη και νομιμότητα στο χειρισμό και τη χρήση προσωπικών δεδομένων. Θα πρέπει να γίνεται σαφές στα άτομα το πώς χρησιμοποιούνται τα προσωπικά τους δεδομένα και θα χρειαστεί επίσης μια "νόμιμη βάση" για την επεξεργασία αυτών των δεδομένων.
- Περιορισμός της επεξεργασίας των προσωπικών δεδομένων σε καθορισμένους, σαφείς και νόμιμους σκοπούς. Δεν θα επιτρέπεται να επαναχρησιμοποιούνται ή να αποκαλύπτονται προσωπικά δεδομένα για σκοπούς που δεν είναι "συμβατοί" με το σκοπό για τον οποίο συλλέχθηκαν αρχικά τα δεδομένα.
- Ελαχιστοποίηση της συλλογής και αποθήκευσης δεδομένων προσωπικού χαρακτήρα σε εκείνα που είναι επαρκείς και σχετικά για τον επιδιωκόμενο σκοπό.
- Εξασφάλιση της ακρίβειας των προσωπικών δεδομένων και της δυνατότητας διαγραφής ή διόρθωσης. Θα χρειαστεί η λήψη μέτρων για να βεβαιωθεί το άτομο ότι τα προσωπικά του δεδομένα είναι ακριβή και μπορούν να διορθωθούν αν προκύψουν σφάλματα.
- Περιορισμός της αποθήκευσης προσωπικών δεδομένων. Θα χρειαστεί η διασφάλιση ότι διατηρούνται προσωπικά δεδομένα μόνο για όσο διάστημα είναι απαραίτητο για την επίτευξη των σκοπών για τους οποίους συλλέχθηκαν τα δεδομένα.
- Διασφάλιση της ασφάλειας, της ακεραιότητας και της εμπιστευτικότητας των προσωπικών δεδομένων. Ο οργανισμός σας πρέπει να λάβει μέτρα για την ασφαλή φύλαξη των προσωπικών δεδομένων μέσω τεχνικών και οργανωτικών μέτρων ασφαλείας.

2.3 Βασικοί όροι και έννοιες

Το άρθρο 4 του GDPR περιλαμβάνει κατάλογο ορισμένων όρων που χρησιμοποιούνται στον κανονισμό. Αρκετοί όροι είναι ιδιαίτερα σημαντικοί και χρειάζεται να εξηγηθούν καθώς θα αναφέρονται στην συνέχεια της εργασίας, και θα πρέπει να γίνονται αντιληπτοί.

1. Υπεύθυνος επεξεργασίας (Controller) : το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, ο οργανισμός ή άλλος φορέας ο οποίος, από μόνος του ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
2. Εκτελών την επεξεργασία (Processor): το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας.
3. Δεδομένα προσωπικού χαρακτήρα (Personal Data): κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.
4. Επεξεργασία (processing): 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.
5. Περιορισμός της επεξεργασίας (restriction of processing) : η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.
6. Κατάρτιση προφίλ (profiling): 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.
7. Ψευδωνυμοποίηση (pseudonymisation): 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

8. Σύστημα αρχειοθέτησης (filing system): 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.
9. Αποδέκτης (recipient): 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.
10. Τρίτος (third party): 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.
11. Συγκατάθεση του υποκειμένου των δεδομένων (consent): κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επιγνώσει, 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.
12. Παραβίαση δεδομένων προσωπικού χαρακτήρα (personal data breach): 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.
13. Γενετικά δεδομένα (genetic data): τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

14. Βιομετρικά δεδομένα (biometric data): δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.
15. Δεδομένα που αφορούν την υγεία (data concerning health): δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.
16. Κύρια εγκατάσταση (main establishment):

    α) όταν πρόκειται για υπεύθυνο επεξεργασίας με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση, εκτός εάν οι αποφάσεις όσον αφορά τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα λαμβάνονται σε άλλη εγκατάσταση του υπευθύνου επεξεργασίας στην Ένωση και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, οπότε ως κύρια εγκατάσταση θεωρείται η εγκατάσταση στην οποία έλαβε τις αποφάσεις αυτές,

    β) όταν πρόκειται για εκτελούντα την επεξεργασία με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση ή, εάν ο εκτελών την επεξεργασία δεν έχει κεντρική διοίκηση στην Ένωση, η εγκατάσταση του εκτελούντος την επεξεργασία στην Ένωση στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία, στον βαθμό που ο εκτελών την επεξεργασία υπόκειται σε ειδικές υποχρεώσεις δυνάμει του παρόντος κανονισμού
17. Εκπρόσωπος (representative): φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση, το οποίο ορίζεται εγγράφως από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία βάσει του άρθρου 27 και εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ως προς τις αντίστοιχες υποχρεώσεις τους δυνάμει του παρόντος κανονισμού.
18. Επιχείρηση (enterprise): φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα, ανεξάρτητα από τη νομική του μορφή, περιλαμβανομένων των προσωπικών εταιρειών ή των ενώσεων που ασκούν τακτικά οικονομική δραστηριότητα.
19. Όμιλος επιχειρήσεων (group of undertakings): μια ελέγχουσα επιχείρηση και οι ελεγχόμενες από αυτήν επιχειρήσεις.

20. Δεσμευτικοί εταιρικοί κανόνες (binding corporate rules): οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις ή δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα.
21. Εποπτική αρχή (supervisory authority): ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51.
22. Ενδιαφερόμενη εποπτική αρχή (supervisory authority concerned): εποπτική αρχή την οποία αφορά η επεξεργασία δεδομένων προσωπικού χαρακτήρα, διότι:

    α) ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος στο έδαφος του κράτους μέλους της εν λόγω εποπτικής αρχής,

    β) τα υποκείμενα των δεδομένων που διαμένουν στο κράτος μέλος της εν λόγω εποπτικής αρχής επηρεάζονται ή ενδέχεται να επηρεαστούν ουσιωδώς από την επεξεργασία ή

    γ) έχει υποβληθεί καταγγελία στην εν λόγω εποπτική αρχή,
23. Διασυνοριακή επεξεργασία (cross-border processing):

    α) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη ή

    β) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη
24. Σχετική και αιτιολογημένη ένσταση (relevant and reasoned objection): ένσταση ως προς την ύπαρξη ή μη παράβασης του παρόντος κανονισμού, ή ως προς τη συμφωνία με τον παρόντα κανονισμό της προβλεπόμενης ενέργειας σε σχέση με τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, η οποία καταδεικνύει σαφώς τη σημασία των κινδύνων που εγκυμονεί το σχέδιο απόφασης όσον αφορά τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, κατά περίπτωση, την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης.

25. Υπηρεσία της κοινωνίας των πληροφοριών (information society service) : υπηρεσία κατά την έννοια του άρθρου 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου1.
26. Διεθνής οργανισμός (international organisation) : οργανισμός και οι υπαγόμενοι σε αυτόν φορείς που διέπονται από το δημόσιο διεθνές δίκαιο ή οποιοσδήποτε άλλος φορέας που έχει ιδρυθεί δυνάμει ή επί τη βάσει συμφωνίας μεταξύ δύο ή περισσότερων χωρών.

2.4 Η έννοια της συγκατάθεσης

Η έννοια της συγκατάθεσης, όπως χρησιμοποιείται στην οδηγία για την προστασία δεδομένων (οδηγία 95/46/ΕΚ) καθώς και στην ισχύουσα οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, έχει εξελιχθεί. Το GDPR διευκρινίζει και εξειδικεύει περαιτέρω τις απαιτήσεις απόκτησης και απόδειξης έγκυρης συγκατάθεσης. Οι εν προκειμένω κατευθυντήριες γραμμές επικεντρώνονται σε αυτές τις αλλαγές, παρέχοντας πρακτική καθοδήγηση με σκοπό τη διασφάλιση συμμόρφωσης με τον GDPR και εξελίσσοντας την Γνωμοδότηση 15/2011 αναφορικά με τη συγκατάθεση. Η συγκατάθεση παραμένει η μία από τις έξι νόμιμες βάσεις για την επεξεργασία προσωπικών δεδομένων, σύμφωνα με την κατηγοριοποίηση του άρθρου 6 του GDPR. Κατά την έναρξη δραστηριοτήτων που εμπεριέχουν επεξεργασία προσωπικών δεδομένων, ένας υπεύθυνος επεξεργασίας πρέπει πάντα να αφιερώνει χρόνο για να αξιολογήσει εάν η κατάλληλη νόμιμη βάση για την επικείμενη επεξεργασία είναι η συγκατάθεση ή εάν αντίθετα μία άλλη βάση πρέπει να επιλεγεί. Γενικά, η συγκατάθεση μπορεί να αποτελέσει κατάλληλη νόμιμη βάση εάν σε ένα υποκείμενο δεδομένων προσφέρεται έλεγχος και προσφέρεται μία γνήσια επιλογή αναφορικά με την αποδοχή ή απόρριψη των όρων που έχουν προσφερθεί ή απόρριψη αυτών χωρίς ζημία. Όταν αιτείται συγκατάθεση, ένας ελεγκτής έχει καθήκον να αξιολογήσει κατά πόσο αυτό πληροί όλες τις απαιτήσεις για την απόκτηση έγκυρης συγκατάθεσης. Σε περίπτωση απόκτησης σε πλήρη συμμόρφωση με τον GDPR, η συγκατάθεση είναι ένα εργαλείο που δίνει στα υποκείμενα δεδομένων τον έλεγχο σχετικά με το κατά πόσο ή όχι τα προσωπικά δεδομένα που τους αφορούν θα υποστούν επεξεργασία. Σε αντίθετη περίπτωση, ο έλεγχος του υποκειμένου δεδομένων καθίσταται πλασματικός και η συγκατάθεση θα αποτελεί μία άκυρη βάση για επεξεργασία, καθιστώντας την δραστηριότητα επεξεργασίας παράνομη. Οι υπάρχουσες γνωμοδοτήσεις της Ομάδας Εργασίας του άρθρου 29 (WP29) σχετικά με τη συγκατάθεση παραμένουν σχετικές, όπου είναι συνεπείς με το νέο νομικό πλαίσιο, καθώς ο GDPR κωδικοποιεί την υπάρχουσα καθοδήγηση και γενική καλή πρακτική της WP29 και τα περισσότερα από τα καθοριστικά στοιχεία της συγκατάθεσης παραμένουν τα ίδια υπό το καθεστώς του GDPR. Για το λόγο αυτό, σε αυτό το έγγραφο, η WP29 επεκτείνει και ολοκληρώνει προηγούμενες Γνωμοδοτήσεις σε συγκεκριμένα

θέματα που περιλαμβάνουν αναφορά στη συγκατάθεση υπό το καθεστώς της οδηγίας 95/46/ΕΚ, χωρίς να τις αντικαθιστά.

Όπως αναφέρεται στην Γνωμοδότηση 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, η πρόσκληση σε άτομα για αποδοχή μίας πράξης επεξεργασίας δεδομένων θα πρέπει να υπόκειται σε αυστηρές απαιτήσεις, καθώς αφορά τα θεμελιώδη δικαιώματα των υποκειμένων δεδομένων και ο ελεγκτής επιθυμεί να εμπλακεί σε μία πράξη επεξεργασίας που ενδέχεται να είναι παράνομη χωρίς τη συγκατάθεση του υποκειμένου επεξεργασίας. Ο κρίσιμος ρόλος της συγκατάθεσης υπογραμμίζεται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Επιπλέον, η απόκτηση συγκατάθεσης επίσης δεν αρνείται ή με οποιονδήποτε τρόπο δεν υποβαθμίζει τις υποχρεώσεις του ελεγκτή να τηρεί τις αρχές της επεξεργασίας που κατοχυρώνονται στον GDPR, ιδίως το άρθρο 5 του GDPR αναφορικά με την αντικειμενικότητα, την αναγκαιότητα και την αναλογικότητα, καθώς και με την ποιότητα των δεδομένων. Ακόμα και αν η επεξεργασία των προσωπικών δεδομένων βασίζεται στη συγκατάθεση του υποκειμένου δεδομένων, αυτό δε νομιμοποιεί τη συλλογή δεδομένων η οποία δεν είναι αναγκαία σε σχέση με ένα συγκεκριμένο σκοπό επεξεργασίας και είναι θεμελιωδώς αθέμιτη.

2.5 Ορισμός υπευθύνου προστασίας

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν Υπεύθυνο Προστασίας Δεδομένων (DPO) σε κάθε περίπτωση στην οποία:

1. Η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας.
2. Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα.
3. Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

Όμιλος επιχειρήσεων μπορεί να διορίσει ένα μόνο υπεύθυνο προστασίας δεδομένων, υπό την προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων.

Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή ή δημόσιος φορέας, ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές τέτοιες αρχές ή πολλούς τέτοιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους.

Σε περιπτώσεις πλην των αναφερόμενων στην παράγραφο 1, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να ορίζουν υπεύθυνο προστασίας δεδομένων ή, όπου απαιτείται από το δίκαιο της Ένωσης ή του κράτους μέλους, ορίζουν υπεύθυνο προστασίας δεδομένων. Ο υπεύθυνος προστασίας δεδομένων μπορεί να ενεργεί για τις εν λόγω ενώσεις και τους άλλους φορείς που εκπροσωπούν υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία. Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39.

Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και τα ανακοινώνουν στην εποπτική αρχή. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. 4.5.2016 L 119/55 Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης EL.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία στηρίζουν τον υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων που αναφέρονται στο άρθρο 39 παρέχοντας απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων. Δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του. Ο υπεύθυνος προστασίας δεδομένων λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους δυνάμει του παρόντος

κανονισμού. Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους. Μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζουν ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων.

Ο υπεύθυνος προστασίας δεδομένων έχει τουλάχιστον τα ακόλουθα καθήκοντα:

1. Ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων.
2. Παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων.
3. Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35.
4. Συνεργάζεται με την εποπτική αρχή.
5. Ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

2.6 Εκτίμηση επιπτώσεων

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων και πιο συγκεκριμένα σύμφωνα με αυτά που ορίζονται στο Άρθρο 33, «…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». Η διαδικασία της «Εκτίμησης των Επιπτώσεων σχετικά με

την Προστασία των Δεδομένων - (Data Protection Impact Assessment – DPIA) ορίζεται πολύ περιληπτικά στον τελευταίο Γενικό Κανονισμό, χωρίς όμως να ακολουθεί συγκεκριμένες γραμμές, αφήνοντας μεγάλα περιθώρια διαμόρφωσης. Η εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων αποτελεί στην ουσία μια διαδικασία η οποία διενεργείται κυρίως κατά το αρχικό στάδιο σχεδίασης της εφαρμογής. Αποτέλεσμα αυτής της διαδικασίας είναι η σύνταξη μιας έκθεσης στην οποία περιέχονται όλα τα στοιχεία και χαρακτηριστικά της επεξεργασίας, η εκτίμηση των πιθανών κινδύνων καθώς και προτεινόμενα μέτρα ασφαλείας ώστε να επιτυγχάνεται ο περιορισμός ή η εξάλειψη αυτών. Η έκθεση αυτή υπόκειται σε έλεγχο από την εκάστοτε Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ώστε να εκδώσει την απαραίτητη άδεια επεξεργασίας των συγκεκριμένων δεδομένων, όπως προβλέπεται από τον Γενικό Κανονισμό για την Προστασία των Δεδομένων. Αυτή η ex-ante εκτίμηση του όλου εγχειρήματος της επεξεργασίας ενισχύει την πιθανότητα επιρροής της DPIA στην σχεδίαση της εφαρμογής, πληρώντας με αυτό τον τρόπο το κριτήριο της ιδιωτικότητας κατά την σχεδίαση (privacy by design). 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).

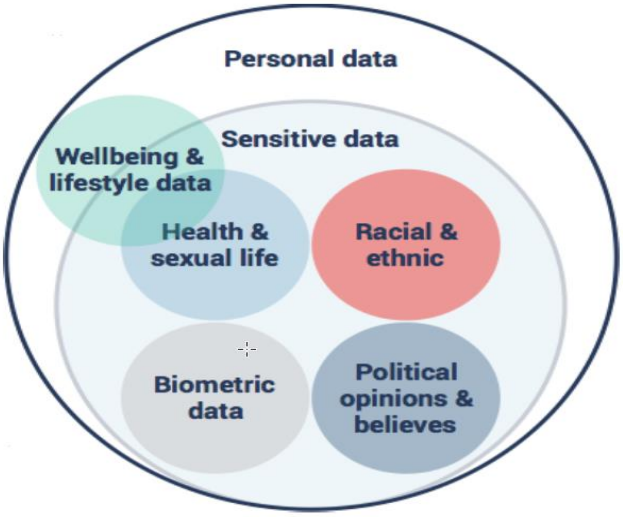
2.7 Δεδομένα που αφορούν την υγεία

Ο νέος γενικός κανονισμός για την προστασία δεδομένων της ΕΕ (GDPR) είναι εκτενής, αλλά όχι εξαντλητικός στον ορισμό για το πια είναι δεδομένα υγείας λέγοντας πως είναι όλα τα δεδομένα που σχετίζονται με την κατάσταση υγείας ενός υποκειμένου και συλλέγονται για τους σκοπούς που προσδιορίζουν την υγειονομική κατάσταση κάποιου.

Η ομάδα εργασίας για την προστασία των δεδομένων του άρθρου 29 λειτουργώντας ως συμβουλευτικός παράγοντας στην Ευρωπαϊκή Ένωση παρέχει έναν πιο λεπτομερή ορισμό ο οποίος ορίζει τα δεδομένα για την υγεία ως εξής :

- Ιατρικά δεδομένα που παρέχουν πληροφορίες σχετικά με την κατάσταση σωματικής ή ψυχικής υγείας κάποιου(το υποκείμενο των δεδομένων), που παράγεται σε επαγγελματικό ιατρικό πλαίσιο.
- Ακατέργαστα δεδομένα που συλλέγονται από εφαρμογές ή συσκευές που μπορούν να χρησιμοποιηθούν για την επαγωγή, μεμονωμένα ή συγκεντρωτικά με άλλους, την κατάσταση υγείας ενός ατόμου ή τον κίνδυνο για την υγεία.
- Δεδομένα που μπορούν να επιτρέψουν σε κάποιον να συναγάγει την κατάσταση υγείας ή τον κίνδυνο ενός ατόμου, ανεξάρτητα από αυτό την ακρίβεια, τη νομιμότητα ή την επάρκεια.

Αν και αυτός ο ορισμός φαίνεται σαφής, εξακολουθούν να υπάρχουν "γκρίζες περιοχές", όπως στην περίπτωση των εφαρμογών υγείας (wellbeing apps), όπου ο ορισμός είναι συχνά εξαιρετικά δύσκολος στην ερμηνεία του.



Εικόνα 1

Ένα παράδειγμα για τον προηγούμενο ορισμό αποτελούν οι εφαρμογές υγείας και μέτρησης της φυσικής κατάστασης συλλέγοντας βιοσήματα και μετρήσεις από το άτομο. Για παράδειγμα εφαρμογή φυσικής κατάστασης που μετρά τα βήματα ενός ατόμου. Αν τα δεδομένα δεν μπορούν να συνδυαστούν με άλλα δεδομένα και εάν το συγκεκριμένο ιατρικό πλαίσιο στο οποίο χρησιμοποιείται η εφαρμογή δεν είναι ξεκάθαρο, τότε είναι μη ευαίσθητα δεδομένα. Εάν τα δεδομένα μπορούν να συνδυάζεται εύκολα με άλλα σύνολα δεδομένων, τότε μπορεί να γίνουν ευαίσθητα δεδομένα. Εάν, για παράδειγμα, είναι σε συνδυασμό με τον καρδιακό ρυθμό, ή σε σύγκριση με τα δεδομένα από άλλους ανθρώπους, μπορεί να αποκαλύψουν ευαίσθητες πληροφορίες για την ικανότητα ενός ατόμου να εκτελεί αγχωτική δραστηριότητα, και έτσι εκτείνεται στην ευαίσθητη κατηγορία υγείας. Όπως μπορούμε να δούμε, δεν είναι πάντα εύκολο να καθορίσετε τι αποτελεί ευαίσθητο δεδομένο ή όχι και πολλές φορές χρειάζεται να εξετάσουμε τον συνδυασμό δεδομένων για να καταλήξουμε στο συμπέρασμα για τον αν αποτελούν ευαίσθητα δεδομένα.

Κεφάλαιο 3. Υπηρεσίες υγείας

3.1 Υπηρεσίες υγείας μέσω κινητών συσκευών επικοινωνίας

Οι υπηρεσίες υγείας μέσω κινητών συσκευών επικοινωνίας (mHealth) είναι μια πτυχή της ηλεκτρονικής υγείας που επικεντρώνεται στην παροχή υπηρεσιών υγειονομικής περίθαλψης μέσω συσκευών κινητής επικοινωνίας. Δεν υπάρχει ενιαίος ορισμός του mHealth, αλλά θα μπορούσαμε να τον περιγράψουμε ως μια "πρακτική ιατρικής και δημόσιας υγείας που υποστηρίζεται από κινητές συσκευές, όπως κινητά τηλέφωνα, συσκευές παρακολούθησης ασθενών, προσωπικοί ψηφιακοί βοηθοί και άλλες ασύρματες συσκευές". Βασίζεται στη χρήση κινητής τεχνολογίας ή ασύρματων συσκευών και αισθητήρων που προορίζονται να φορεθούν, να μεταφερθούν ή να προσεγγιστούν από το άτομο κατά τις συνήθεις καθημερινές δραστηριότητες.

Οι τεχνολογικές συσκευές που φοριούνται στο σώμα, όπως έξυπνα τηλέφωνα (smartphone), έξυπνα ρολόγια (smartwatches) και βραχιόλια, περιλαμβάνουν επίσης μια ποικιλία αισθητήρων που υποστηρίζουν νέες μεθόδους για τη συνεχή παρακολούθηση βιολογικών, συμπεριφορών ή περιβαλλοντικών δεδομένων, την παροχή παρεμβάσεων και την αξιολόγηση των αποτελεσμάτων τους. [2]Αυτά τα συστήματα αισθητήρων περιλαμβάνουν επιταχυνσιόμετρα, γυροσκόπια, αισθητήρες μέτρησης της καρδιακής συχνότητας και γαλβανικής απόκρισης του δέρματος, κάμερες, καθώς και γεωαισθητήρες (GPS) για την παρακολούθηση της ακριβούς γεωγραφικής θέσης. Μέσω τέτοιων συστημάτων αισθητήρων, η παρακολούθηση πτυχών που σχετίζονται με την υγεία μπορεί να πραγματοποιηθεί με μεγάλη ακρίβεια και συχνότητα δειγματοληψίας και σε μεγαλύτερες χρονικές περιόδους από τις πιο παραδοσιακές μεθόδους. Τέτοια συστήματα είναι επίσης κατάλληλα για την παροχή ψηφιοποιημένων παρεμβάσεων. Μέσω της ανάπτυξης αλγορίθμων που προέρχονται από τα δεδομένα των αισθητήρων και των πρόσθετων αυτοαναφερόμενων δεδομένων, μπορούν να εξαχθούν ακριβείς και επίσης νέες πληροφορίες για τις φυσιολογικές, ψυχολογικές, συναισθηματικές και περιβαλλοντικές καταστάσεις. Η χρήση της κινητής τεχνολογίας προσφέρει επίσης νέες λύσεις για την παροχή υπηρεσιών υγείας,

[2] Murray, C.J.; Vos, T.; Lozano, R.; Naghavi, M.; Flaxman, A.D.; Michaud, C.; Ezzati, M.; Shibuya, K.; Salomon, J.A.; Abdalla, S.; et al. Disability-Adjusted Life Years (DALYs) for 291 Diseases and Injuries in 21 Regions, 1990–2010: A Systematic Analysis for the Global Burden of Disease Study 2010. *Lancet* **2012**, *380*, 2197–2223.

συμπεριλαμβανομένης της χρήσης εξατομικευμένης υποστήριξης σε θέματα υγείας, βασισμένης στην παρακολούθηση της συμπεριφοράς σε οικολογικά έγκυρα περιβάλλοντα.[3]

Η δυναμική που έχει δημιουργηθεί τα τελευταία χρόνια για την ανάπτυξη νέων υπηρεσιών που βασίζονται σε μια τέτοια τεχνολογία είναι τεράστια. Το 2014, πάνω από το 75% των ατόμων ηλικίας άνω των 65 ετών στις ΗΠΑ διέθετε κινητό τηλέφωνο και πάνω από 50% χρησιμοποιούσαν smartphones ή tablet ενώ το Ηνωμένο Βασίλειο το 2012 περίπου το 50% χρησιμοποίησε το διαδίκτυο, το οποίο αναμένεται να αυξηθεί στο 90% έως το 2020. Ο αριθμός των ανθρώπων που κατέχουν ένα smartphone παγκοσμίως ανήλθε στα 2,1 δισ. Το 2016 και οι αριθμοί αναμένεται να αυξηθούν σε 2,5 δισ. έως το 2020. Το mHealth ανοίγει τη δυνατότητα παρακολούθησης της υγείας σε επίπεδο ατόμων και πληθυσμού και μπορεί να ενθαρρύνει υγιείς συμπεριφορές για την πρόληψη ή τη μείωση των προβλημάτων υγείας. Με την αυξανόμενη παγκόσμια πρόσβαση στην κινητή τεχνολογία, υπάρχει τεράστιο δυναμικό για την ανάπτυξη εφαρμογών για τη δημόσια υγεία στην ιδιωτική αγορά. Αυτό αντικατοπτρίζεται επίσης από τον ταχύτατα αυξανόμενο αριθμό εφαρμογών που αναπτύσσονται από μεγάλους παράγοντες στην αγορά[4].

3.1.1 Υπηρεσίες υγείας για την διαχείριση ασθενειών

Οι εφαρμογές της υγείας μπορούν να χωριστούν σε εκείνες που στοχεύουν στη διαχείριση της νόσου και εκείνες που στοχεύουν στην αλλαγή της συμπεριφοράς στην υγεία. Μια πρόσφατη συστηματική ανασκόπηση της αποτελεσματικότητας των παρεμβάσεων που χρησιμοποιούν ποικίλες εφαρμογές έξυπνων τηλεφώνων και πλατφόρμες άσκησης για τη βελτίωση της διατροφής, της σωματικής δραστηριότητας και της καθιστικής συμπεριφοράς ολοκληρώθηκαν με μέτρια στοιχεία για παρεμβάσεις με βάση την εφαρμογή. Διαπιστώθηκε επίσης ότι οι παρεμβάσεις πολλών συστατικών ήταν πιο αποτελεσματικές από τις αυτόνομες παρεμβάσεις εφαρμογής. Μια άλλη ανασκόπηση από το 2016 των εφαρμογών smartphone που στοχεύει στην προώθηση της φυσικής δραστηριότητας έδειξε ότι τέτοιες εφαρμογές μπορούν να είναι αποτελεσματικές στην προώθηση της σωματικής δραστηριότητας, ωστόσο, το φαινόμενο όπως καταδεικνύεται μέχρι τώρα φαίνεται να είναι μέτριο. Ένα σημαντικό συμπέρασμα ήταν ότι οι συμμετέχοντες διαφόρων ηλικιών και των δύο φύλων ανταποκρίθηκαν θετικά στις εφαρμογές, ιδιαίτερα εκείνες που παρακολουθούσαν αυτόματα τη δραστηριότητα και την πρόοδο της δραστηριότητας και που ήταν φιλικές προς το χρήστη και ευέλικτες σε σχέση με το είδος της δραστηριότητας που παρακολούθησαν.

[3] Kumar, S.; Nilsen, W.J.; Abernethy, A.; Atienza, A.; Patrick, K.; Pavel, M.; Riley, W.T.; Shar, A.; Spring, B.; Spruijt-Metz, D.; et al. Mobile Health Technology Evaluation: The mHealth Evidence Workshop. Am. J. Prev. Med. 2013, 45, 228–236

[4] Eurostat People in the EU—Statistics on an Ageing Society. Available online: http://ec.europa.eu/eurostat/statistics-explained/index.php/People_in_the_EU_%E2%80%93_statistics_on_an_ageing_society

Οι εφαρμογές για την υγεία που αποσκοπούν στην αύξηση της σωματικής δραστηριότητας και στη διευκόλυνση της αλλαγής της συμπεριφοράς έχουν επίσης αναπτυχθεί, ιδίως για τους ηλικιωμένους. Σχετικά νέες μελέτες κατέδειξαν την επίδραση της ισορροπημένης εκπαίδευσης στο σπίτι (μέση ηλικία 75 ετών) που παρουσιάστηκε στις εφαρμογές tablet και τη φυσική δραστηριότητα που παρέχεται από smartphone με κοινωνικό στοιχείο (μέση ηλικία 60 ετών). Δεδομένης της αύξησης του ηλικιωμένου πληθυσμού τις επόμενες δεκαετίες, οι παρεμβάσεις στον τομέα της υγείας πρέπει να αναπτυχθούν με τις ανάγκες και τις προτιμήσεις αυτών των ομάδων ανθρώπων.

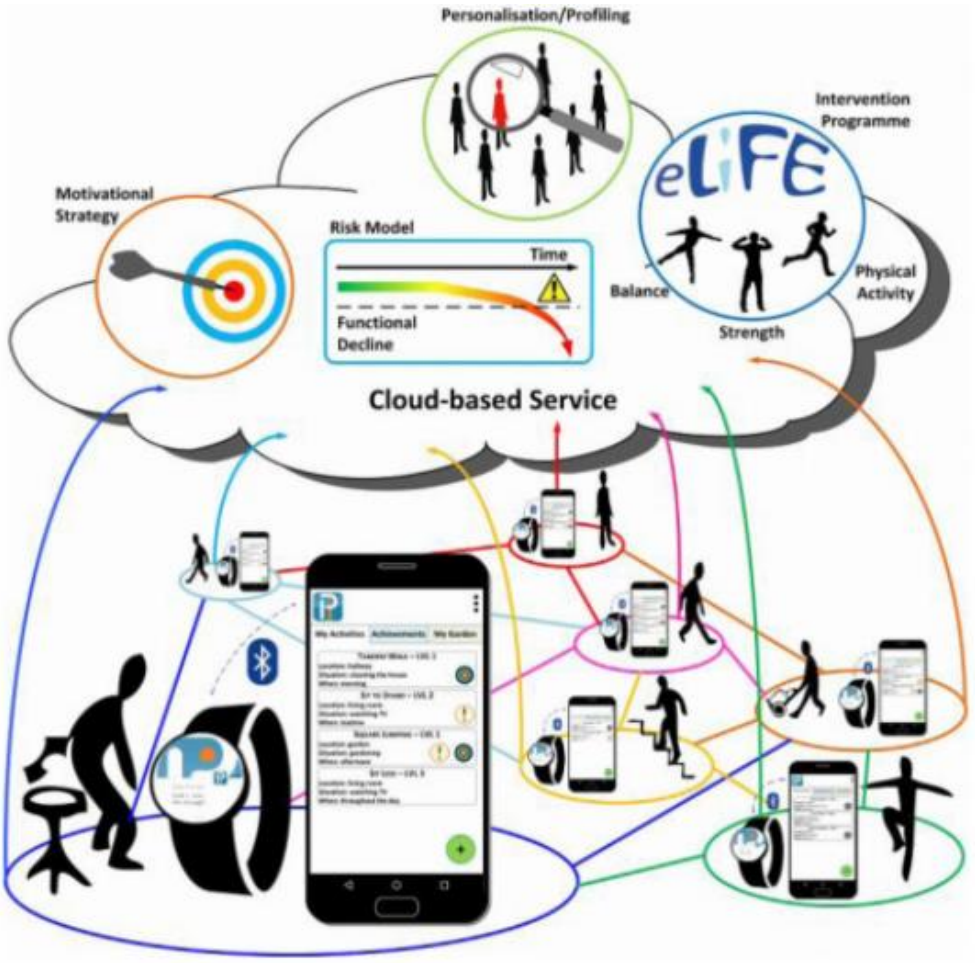
3.2 Ανάπτυξη τεχνολογιών υγείας για ηλικιωμένους

Τα περισσότερα smartphones δεν έχουν αναπτυχθεί με βάση τις δυνατότητες για ηλικιωμένους. Οι μελέτες που συγκρίνουν τη χρήση smartphones από τους νέους και τους μεγαλύτερους σε ηλικία, καταλήγουν στο συμπέρασμα ότι υπάρχουν πέντε διαφορετικοί ανθρώπινοι παράγοντες στους οποίους οι ηλικιωμένοι είναι διαφορετικοί από τους νεότερους ομολόγους τους: χρόνος εκμάθησης, ταχύτητα απόδοσης, ποσοστό σφάλματος, διατήρηση με την πάροδο του χρόνου και υποκειμενική ικανοποίηση . Μια πρόσφατη συστηματική βιβλιογραφική ανασκόπηση σχετικά με την αντίληψη των ηλικιωμένων σχετικά με την τεχνολογία που χρησιμοποιείται για την πρόληψη πτώσης διαπίστωσε ότι ο έλεγχος, η ανεξαρτησία και η αντιληπτή ανάγκη για ασφάλεια είναι σημαντικές για την παρακίνηση για τη χρήση των τεχνολογιών. Σημαντικοί εξωτερικοί παράγοντες ήταν η χρηστικότητα, η δυνατότητα ανάγνωσης από το σύστημα και το κόστος. Μια άλλη συστηματική βιβλιογραφική ανασκόπηση σχετικά με την αποδοχή τεχνολογίας σε ηλικιωμένους ενήλικες βρήκε ανησυχίες σχετικά με την τεχνολογία, τα αναμενόμενα οφέλη της τεχνολογίας, καθώς οι εναλλακτικές λύσεις στην τεχνολογία και η κοινωνική επιρροή είναι σημαντικές Επιπλέον, οι συγγραφείς διαπίστωσαν ότι οι περισσότερες μελέτες είχαν αξιολογήσει την τεχνολογία μόνο σε πρώιμο στάδιο της ανάπτυξης και ότι σχετικά λίγα είναι ακόμη γνωστά για προϊόντα που έχουν ήδη εφαρμοστεί.

Προκειμένου να προωθηθεί η πρόληψη σε θέματα υγείας για τους ηλικιωμένους αλλά και για τους χρόνια πάσχοντες από συγκεκριμένες νόσους, υπάρχει ανάγκη να αναπτυχθούν εφαρμογές υγείας που επικεντρώνονται στον εντοπισμό των κινδύνων που σχετίζονται με τη λειτουργική αστάθεια του ατόμου και στις επεμβάσεις που προάγουν την υγεία και αποτρέπουν επιπλοκές υγείας σε αυτές τις κατηγορίες πληθυσμού.

Παράδειγμα αρχιτεκτονικής πολυλειτουργικού συστήματος mHealth, συμπεριλαμβανομένης της ανίχνευσης του κινδύνου για τη λειτουργική αστάθεια του ατόμου, του προφίλ για την εξατομίκευση της παρέμβασης, της παρέμβασης με την ισορροπία, της δύναμης και της σωματικής

δραστηριότητας που ενσωματώνονται στην καθημερινή ζωή και της ατομικής ανατροφοδότησης σχετικά με τη συμπεριφορά που στοχεύει στην αύξηση των κινήτρων για αλλαγή συμπεριφοράς . Ένα smartphone και ένα smartwatch χρησιμοποιούνται για την παρακολούθηση της συμπεριφοράς, την παρέμβαση και την παροχή εξατομικευμένης ανατροφοδότησης σχετικά με τη συμπεριφορά.



Εικόνα 2

Οι τεχνολογίες της υγείας mHealth δημιουργούν ευκαιρίες για τη συλλογή, τον υπολογισμό και την αποθήκευση μεγάλου όγκου δεδομένων σχετικά με την υγεία και τη συμπεριφορά, συμπεριλαμβανομένων των δεδομένων σχετικά με τις ευαίσθητες συνθήκες υγείας, την τοποθεσία, τα συναισθήματα και τις κοινωνικές αλληλεπιδράσεις και οι δυνατότητες χρήσης και ανταλλαγής πληροφοριών είναι τεράστιες. Η συλλογή και χρήση δεδομένων για την παροχή εξατομικευμένων παρεμβάσεων καθώς και η συλλογή, χρήση πληροφοριών σε επίπεδο πληθυσμού εγείρει ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής, την ασφάλεια και την εμπιστευτικότητα. Η ανάπτυξη των τεχνολογιών και των υπηρεσιών υγείας, καθώς και οι δυνατότητές χρήσης τους, έχουν προχωρήσει τόσο γρήγορα ώστε δεν υπάρχει ρύθμιση σχετικά με τον τρόπο αντιμετώπισης

της κατάστασης. Στην Ευρώπη, αυτό θα αλλάξει στις 25 Μαΐου 2018 με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), ο οποίος αποσκοπεί στην ενίσχυση και ενοποίηση της προστασίας των δεδομένων για τους πολίτες της Ευρωπαϊκής Ένωσης (ΕΕ). Ο βασικός στόχος του GDPR είναι να δώσει στους πολίτες τον έλεγχο των προσωπικών τους δεδομένων, να εναρμονίσει τους κανονισμούς προστασίας δεδομένων σε όλες τις ευρωπαϊκές χώρες και να απλοποιήσει τους κανονισμούς για τις διεθνείς επιχειρήσεις. Αυτό προκαλεί την έρευνα στον τομέα της υγείας για την ανάπτυξη μεθόδων που διασφαλίζουν την ιδιωτική ζωή των χρηστών, ενώ παράλληλα να λαμβάνονται υπόψη οι ερευνητικές ανάγκες.

Ο αριθμός των διαθέσιμων εφαρμογών στα κινητής τηλέφωνα αυξάνεται με ταχύ ρυθμό. Σημαντικές ερωτήσεις είναι πώς θα μπορούν οι καταναλωτές και οι τελικοί χρήστες να βρουν τις σωστές εφαρμογές, πώς θα μπορούν να αξιολογήσουν ποιες από αυτές είναι οι πλέον κατάλληλες για τις ανάγκες τους και πώς θα μπορούν να ανακαλύψουν εάν έχουν υποβληθεί σε αυστηρή επιστημονική ανάπτυξη και δοκιμή. Μια τέτοια αξιολόγηση των σημερινών εφαρμογών μπορεί επίσης να είναι σημαντική για τους ίδιους τους ανθρώπους και για τους φορείς παροχής υγειονομικής περίθαλψης κατά τη λήψη αποφάσεων σχετικά με την προθυμία πληρωμής για κινητές εφαρμογές υγείας, η οποία παραμένει σήμερα ανοικτή ερώτηση.

Κεφάλαιο 4. Συμμόρφωση

4.1 Καταγραφή – ροή Δεδομένων (Data Inventory - Flows)

4.1.1 Υποχρέωση καταγραφής δεδομένων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) φέρνει το ζήτημα της Προστασίας των προσωπικών δεδομένων στο επίκεντρο όπως ήδη έχει διατυπωθεί. Το GDPR απαιτεί από τις εταιρείες που δρουν είτε ως υπεύθυνοι επεξεργασίας είτε ως εκτελούντες την επεξεργασία να διασφαλίζουν την ασφάλεια των προσωπικών δεδομένων που έχουν συλλέξει ή τους έχουν παραχωρηθεί προς επεξεργασία. Απαιτείται από τον κανονισμό πως οι εταιρείες που επεξεργάζονται προσωπικά δεδομένα θα πρέπει να τεκμηριώνουν και να υποδεικνύουν, από που προέρχονται τα δεδομένα καθώς και το πως διαφυλάσσονται κατά την επεξεργασία και την μεταφορά τους καθ' όλη τη διάρκεια του κύκλου ζωής τους. Στο πλαίσιο του κανονισμού, δίνεται έμφαση στο γεγονός ότι όλα τα προσωπικά δεδομένα πρέπει να καταγράφονται και κάθε εταιρεία πρέπει να διαθέτει ένα σύστημα που να παρακολουθεί σε μόνιμη βάση τοις διάφορες πράξεις που διεξάγονται στα δεδομένα προσωπικού χαρακτήρα. Για να γίνει αυτό, απαιτείται από τις εταιρείες να διατηρούν ένα μητρώο δεδομένων (Data Inventory) το οποία θα περιγράφει την δραστηριότητα των δεδομένων, έτσι ώστε να γίνεται η διακυβέρνηση αυτών καθώς και να μπορούν να εφαρμόζονται οι σωστές διαδικασίας για την ορθή διαφύλαξη τους.

Το GDPR απαιτεί όχι μόνο να είναι σε θέση μια εταιρεία, να προσδιορίσει και να προστατεύσει τα δεδομένα όπου και αν βρίσκονται αλλά και να είναι υπεύθυνη, για την ακρίβεια των δεδομένων που κατέχει. Για την εφαρμογή των κανονιστικών απαιτήσεων πρέπει πρώτα να εντοπιστούν αυτά τα δεδομένα στα συστήματά που φιλοξενούνται εφόσον πρόκειται για ηλεκτρονικά δεδομένα και περιγράφει ποια σε ποια επεξεργασία υπόκεινται. Αυτή η διαδικασία ονομάζεται χαρτογράφηση δεδομένων (data mapping) ή καταγραφή δεδομένων (data inventorying) και είναι απαραίτητη ώστε να τεκμηριώνεται αυτές οι πληροφορίες. Το άρθρο 30 του GDPR (Καταγραφή των δραστηριοτήτων επεξεργασίας) είναι η χαρτογράφηση δεδομένων. Χωρίς χαρτογράφηση δεδομένων και την ακριβή απογραφή των δεδομένων, την επεξεργασία τους, τις ροές τους, τα μέσα με τα οποία μεταδίδονται, τα άτομα που επεξεργάζονται τα δεδομένα, είναι αδύνατο για μια εταιρεία ή οργανισμό να εκπληρώσει τις απαιτήσεις της σύμφωνα με το GDPR.

4.1.2 Ροές δεδομένων (Data Flows)

Η δμιουργία ροών δεδομένων είναι ένα βασικό βήμα που θα πρέπει να πραγματοποιήθει από την επιχείρηση-οργανισμό με βάση το GDPR. Με αυτή την ανάλυση η εταιρεία μπορεί να ανακαλύψει πού είναι τα βασικά κενά της, και να κάνει τα βήματα που πρέπει για να ετοπίσει τα δεδομένα που διαθέτει και τους τόπους που αυτό διακινούνται. Μια ροή δεδομένων είναι μια μεταφορά πληροφοριών από από μια τοποθεσία στην άλλη. Για παράδειγμα, από τους προμηθευτές και τους δευτερεύοντες προμηθευτές μέσω των πελατών εντός ή εκτός της ΕΕ. Είναι δεδομένο πως η καταγραφή μαζί με την ροή δεδομένων αποτελούν πρωταρχικό βήμα για την συμμόρφωση με τον κανονισμό. Ένας οργανισμός πρέπει να γνωρίζει τα προσωπικά δεδομένα που επεξεργάζεται και ότι το τα δεδομένα υποβάλλονται σε επεξεργασία σύμφωνα με το νομικό πλαίσιο. Κατά την χαρτογράφηση της ροής πληροφοριών, θα πρέπει να εντοπίστουν τα σημεία αλληλεπίδρασης μεταξύ των ενδιαφερόμενων μέρων. Είναι σημαντικό να κινούμαστε μέσω του κύκλου ζωής των πληροφοριών για τον εντοπισμό απρόβλεπτων ή ακούσιων χρήσεων δεδομένων. Μια εταιρεία θα πρέπει να εξετάσει επίσης τις πιθανές μελλοντικές χρήσεις των πληροφοριών που συλλέγει ακομή και αν δεν είναι άμεσα αναγκαίο. Ο πρώτος στόχος μιας ροής δεδομένων είναι να προσδιοριστεί ο τρόπος με τον οποίο χρησιμοποιούνται τα δεδομένα και για να βεβαιωθούμε, όταν είναι απαραίτητο, πως τα άτομα για τα οποία γίνεται συλλογή δεδομένων είναι ενήμερα για την χρήση των δεδομένων που έχουν συλλεχθεί. Εάν ένας οργανισμός συλλέγει δεδομένα για το λόγο ότι μια μέρα μπορεί να τα χρησιμοποιήσει, το GDPR απαγορεύει αυτή τη συλλογή. Υπάρχουν διάφοροι τρόποι με τους οποίους τα δεδομένα μπορούν να συλλεχθούν, και είναι σημαντικό να ξέρει η εταιρεία τι συμβαίνει πραγματικά με καθένα από αυτούς τους τρόπους καθώς και με τις τεχνικές συλλογής που ακολουθούνται. Τα δεδομένα για την δημιουργία της ροής δεδομένων μπορούν να συλλεχθούν κατά την επιθεώρηση των υπαρχόντων εγγράφων του οργανισμού, μέσω στοχευμένων συναντήσεων με το προσωπικού που διαχειρίζεται προσωπικά δεδομένα, μέσω συμπλήρωσης ερωτηματολογίων ή ακομή και από εσωτερική παρατήρηση διεργασιών. Εάν η αποτύπωση της ροής ενός οργανισμού σχετικά με τον τρόπο με τον οποίο ρέουν τα δεδομένα της είναι διαφορετική από την πραγματικότητα, τότε υπάρχει παραβίαση με βάση τον κανονισμό και θα μπορούσε να επιβληθεί πρόστιμο. Ο οργανισμός θα πρέπει να διοργανώνει συναντήσει με όλα τα μέλη των ομάδων που διαχειρίζονται δεδομένα και να συζητούν τι συμβαίνει σε κάθε στάδιο της διαδικασίας συλλογής δεδομένων, καθώς και για το που πηγαίνουν τα δεδομένα όπως και ποιος έχει πρόσβαση σε αυτά. Η ροή είναι κάτι που έχει δεδομένα τα οποία έρχονται στο ένα άκρο και τα δεδομένα εξέρχονται στο άλλο. Τυπικά, η έξοδος μιας διαδικασίας ή μιας ροή εργασίας είναι μια είσοδος σε

μια άλλη επεξεργασία ή διαδικασία. Όπως και με τα βασικά στοιχεία ενός δεδομένου στην καταγραφή, ο οργανισμός πρέπει να εξετάσει τα προσωπικά δεδομένα που συλλέγονται και σε τι μορφή έχουν συλλεχθεί. Χρειάζεται επίσης να δούμε πώς συλλέχθηκαν τα δεδομένα, ποιος είναι υπεύθυνος γι 'αυτά, πού βρίσκονται και ποιος έχει πρόσβαση σε αυτά. Η εταιρεία θα πρέπει να είναι σε θέση να γνωρίζει αν τα δεδομένα έχουν αποκαλυφθεί ή μοιραστεί με οποιονδήποτε άλλο και εάν το σύστημα αλληλεπιδρά ή μεταφέρει πληροφορίες σε οποιοδήποτε άλλο σύστημα.

4.1.3 Αρχεία δραστηριοτήτων επεξεργασίας

Κάθε υπεύθυνος επεξεργασίας θα πρέπει να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας στο πλαίσιο της ευθύνης τους για τα δεδομένα που επεξεργάζεται, συμπεριλαμβανομένων:

- Όνομα και στοιχεία επικοινωνίας του controller και, κατά περίπτωση, του joint controller, τον εκπρόσωπο του controller και τον υπεύθυνο προστασίας δεδομένων (DPO).
- Τους σκοπούς της επεξεργασίας.
- Περιγραφή των κατηγοριών των υποκειμένων των δεδομένων.
- Περιγραφή των κατηγοριών προσωπικών δεδομένων.
- Κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να αποκαλυφθούν τα προσωπικά δεδομένα συμπεριλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς.
- Κατά περίπτωση, διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα, συμπεριλαμβανομένης την γνωστοποίηση της εν λόγω τρίτης χώρας και τον μηχανισμό μεταβίβασης που επικαλείται.
- Όπου είναι δυνατόν, τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων.
- Όπου είναι δυνατόν, γενική περιγραφή της τεχνικής και οργανωτικής ασφάλειας – μέτρα.

4.1.4 Μεθοδολογία Καταγραφής Δεδομένων

Η μεθοδολογία καταγραφής δεδομένων (data inventorying) είναι ακρογωνιαίος λίθος της συμμόρφωσης με το GDPR και θα πρέπει να εκτελείται σε συγκεκριμένα βήματα, καθώς και να διατηρεί ακριβές το αποτέλεσμα ώστε να αποτυπώνεται ορθά. Για αυτό τον λόγω θα πρέπει ο εκτελών την μεθοδολογία να καταρτίζει ένα ακριβές πλάνο εκτέλεσης, το οποίο θα συλλέγει από όλες τις πήγες ενός οργανισμού ή μιας εταιρείας τις κατάλληλες πληροφορίες που θα κάνουν την καταγραφή των δεδομένων ακριβής.

Οι βασικές μέθοδοι που χρησιμοποιούνται για την εκτέλεση της μεθοδολογίας καταγραφής δεδομένων είναι κυρίως οι :

1. Διαδικασία συνεντεύξεων
2. Αυτόματος εντοπισμός των δεδομένων με χρήση υλισμικού
3. Ανατροφοδότηση από άλλα συστήματα

Φυσικά μπορεί να χρησιμοποιηθεί και συνδυασμός ώστε να γίνει διασταύρωση ή εμπλουτισμός του data inventory από διαφορετικές πηγές.

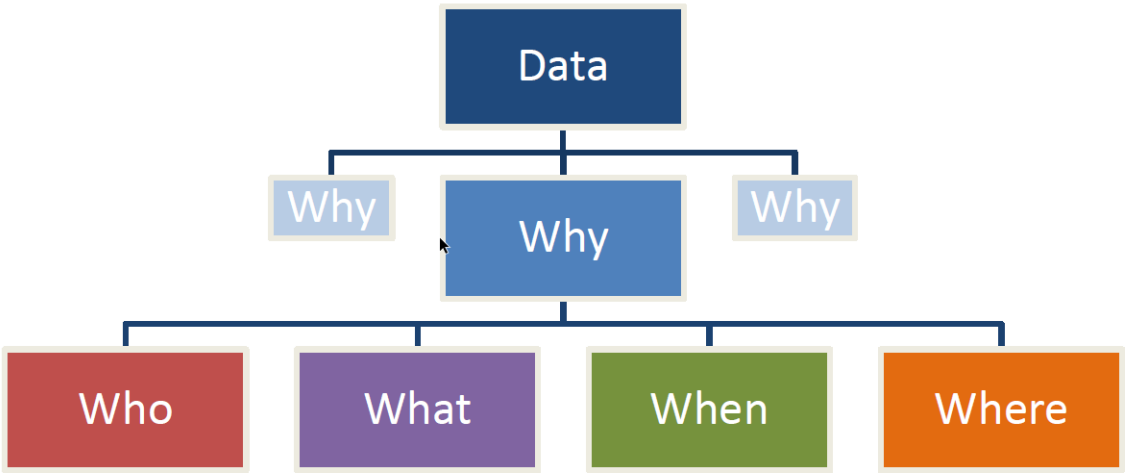
Η διαδικασία των συνεντεύξεων θα πρέπει να είναι οργανωμένη με ερωτήσεις, που να απευθύνονται σε μέρη που επεξεργάζονται ή παίρνουν μέρος στην επεξεργασία και να απαντούν κατά βάση στα Γιατί - Ποιος - Πότε – Που (Why-Who-When-Where).

Με βάση την μεθοδολογία των 5W's όπως την ονομάζουμε δημιουργούμε σετ ερωτήσεων οι οποίες θα μας δώσουν απαντήσεις ώστε να συμπληρώσουμε το data inventory μας.

4.1.4.1 Αντιστοίχιση με βάση τα 5 W's

Αυτή η ενότητα παρέχει βασικά βήματα στους controllers - processors για τη δημιουργία ενός data inventory - mapping των δραστηριοτήτων επεξεργασίας δεδομένων. Σε πολλές περιπτώσεις, οι φόρμες αίτησης / επικοινωνίας (έντυπη ή ηλεκτρονική) παρέχουν συχνά ένα καλό σημείο από το οποίο μπορούμε να ακολουθήσουμε την διαδρομή των δεδομένων. Ο τύπος, η πολυπλοκότητα, ο όγκος, η ευαισθησία ή ο κίνδυνος της επεξεργασίας μπορεί να απαιτούν μια πιο «σε βάθος» ή εξελιγμένη προσέγγιση.

Οι πληροφορίες που συγκεντρώνονται θα βοηθήσουν να ενημερωθούν τα επόμενα βήματα - συμμόρφωση με τις αρχές και τα δικαιώματα και δημιουργία των "αρχείων των δραστηριοτήτων επεξεργασίας" που απαιτούνται από το άρθρο 30 του GDPR.



Εικόνα 3

4.1.4.2 Γιατί επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ; (Why)

Τα προσωπικά δεδομένα καθορίζονται ευρέως στο GDPR και σημαίνει κάθε πληροφορία σχετικά με ένα φυσικό πρόσωπο που μπορεί να εντοπιστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αναγνωριστικό όπως όνομα, αναγνωριστικό αριθμό, δεδομένα θέσης, ηλεκτρονικό αναγνωριστικό ή σε ένα ή περισσότερους παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του προσώπου.

Εξετάζοντας όλους τους τομείς της επιχείρησης ή της υπηρεσίας θα πρέπει να είμαστε σε θέση και απαριθμήσουμε όλους τους λόγους για τους οποίους χρησιμοποιούνται προσωπικά δεδομένα.

Παραδείγματα για τα οποία χρησιμοποιούνται προσωπικά δεδομένα περιλαμβάνουν:

- Διαχείριση Προσωπικού
- Διαχείριση Πελατών
    - Παραδείγματα :
        - Κάτοχος λογαριασμού
        - Πελάτης
        - Μαθητής
        - Ασθενής
- Νομικές υποχρεώσεις
    - Παραδείγματα :
        - Άδεια εργασίας
        - Φόροι

- Παροχή αγαθών ή υπηρεσιών – τρόπος παροχής
    - Online
    - Face to Face
- Δραστηριότητες Marketing
- Profiling
- Παροχή υπηρεσιών επεξεργασίας σε τρίτους - χωρίς όμως να λαμβάνονται αποφάσεις που να επηρεάζουν τα άτομα
- Παροχή υπηρεσιών επεξεργασίας σε τρίτους - αλλά λήψη αποφάσεων (μόνο ή από κοινού) που επηρεάζουν τα άτομα

4.1.4.3 Ποιου τα προσωπικά δεδομένα επεξεργάζονται; (Who)

Θα πρέπει να είμαστε σε θέση να απαντήσουμε στην ερώτηση αυτή ώστε να προσδιορίσουμε το υποκείμενο των δεδομένων και να το καταγράψουμε. Για καθέναν από τους λόγους που αναφέρονται, απαριθμούνται όλες οι διάφορες κατηγορίες προσώπων για τα οποία γίνεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Παραδείγματα κατηγοριών:

- Προσωπικό
- Πελάτες
- Συγγενείς/κηδεμόνες
- Επιχειρηματικές επαφές
- Προμηθευτές
- Μέλη
- Άλλο

4.1.4.4 Τι είδους προσωπικά δεδομένα επεξεργάζονται ; (What)

Θα πρέπει να είμαστε σε θέση να απαντήσουμε και να περιγράψουμε τις διαφορετικές υποκατηγορίες προσωπικών δεδομένων που επεξεργάζονται από το σύστημα ή την επιχείρηση, να προσδιορίσουμε την πηγή καθώς και την νομική υπόσταση των δεδομένων.

Παραδείγματα :

- Προσωπικά στοιχεία - (όνομα, διεύθυνση, ηλεκτρονικό ταχυδρομείο, τηλέφωνο, ημερομηνία γέννησης, επαφή έκτακτης ανάγκης, σεξουαλικό προσανατολισμό, εθνικότητα κ.λπ.)

- Οικονομικές λεπτομέρειες - (τραπεζικό λογαριασμό, τα στοιχεία της πιστωτικής κάρτας, τον αριθμό φορολογικού μητρώου, τη φορολογική αναφορά κ.λπ.)
- Πληροφορίες για την υγεία
- Εικόνες / Εγγραφές φωνής
- Στοιχεία διαβατηρίου / άδειας οδήγησης / εθνικής ταυτότητας
- Διεύθυνση IP
- Ποινικές καταδίκες / αδικήματα
- Βιομετρία - Εκτύπωση δακτύλου / σάρωση αμφιβληστροειδούς / DNA κ.λπ.
- Εκπαίδευση & κατάρτιση
- Στοιχεία απασχόλησης (βιογραφικό σημείωμα, αναφορές, ετήσιες εκτιμήσεις, καθεστώς απασχόλησης, άδεια εργασίας, άδεια, ασθένεια κ.λπ.)

Πηγή των δεδομένων :

- Οι ίδιοι
- Τρίτο άτομο
- Άλλες πηγές

  Για παράδειγμα:

  - Πιστωτική υπηρεσία
  - Έλεγχος ποινικού μητρώου
  - Διαδίκτυο / Κοινωνικά ΜΜΕ
  - Κυβερνητικές υπηρεσίες
  - Ιδιώτες ερευνητές
  - εταιρείες ελέγχου Due Diligence / CDD

Η νομική βάση θα μπορούσε να είναι :

- Νομική υποχρέωση
- Νομική λειτουργία του δημόσιου οργανισμού
- Προστασία ζωτικών συμφερόντων αυτού του προσώπου
- Εκτέλεση σύμβασης
- Δικαιολογημένα συμφέροντα του υπεύθυνου επεξεργασίας δεδομένων
- Συναίνεση

4.1.4.5 Πότε γίνεται η επεξεργασίας δεδομένων προσωπικού χαρακτήρα; (When)

Δεν πρέπει να ξεχνούμε πως με την έννοια επεξεργασία ο κανονισμός περιλαμβάνει τις ενέργειες απόκτησης, αποκάλυψης και διαγραφής προσωπικών δεδομένων. Είναι σημαντικό λοιπόν και θα πρέπει να ορίσουμε το πότε συμβαίνουν όλες οι παραπάνω ενέργειες.

Παραδείγματα :

- Περίοδος διατήρησης δεδομένων
- Επαγγελματική πρακτική
- Προσδιορισμός κανονισμού ή νόμου που καθορίζει την περίοδο διατήρησης

4.1.4.6 Που γίνεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα; (Where)

Εξίσου σημαντικό με τα προηγούμενα τέσσερα είναι και το σημείο, στο οποίο γίνεται η επεξεργασία και σε πολλές περιπτώσεις, η επεξεργασία μπορεί να λαμβάνει μέρος σε παραπάνω από ένα σημεία.

Παραδείγματα:

- Μη αυτόματες εγγραφές - χειρόγραφα
- Ηλεκτρονικές εγγραφές
- Εσωτερικά συστήματα διαχείρισης
- Bring your own device (BYOD)
- Εξωτερική φιλοξενούμενη υπηρεσία
- Υπηρεσίες στο νέφος (Cloud Services)

4.1.4.7 Σύνοψη 5W's – Ερωτηματολόγιο

Για να μπορέσουμε να συνοψίσουμε και να αποτυπώσουμε τα 5W's με την μορφή ερωτήσεων που θα γίνουν με την μέθοδο της συνέντευξης, έχουμε δημιουργήσει τα παρακάτω τρία σετ ερωτήσεων, με βάση τα οποία μπορεί να συμπληρωθεί σωστά το data inventory . Οι ερωτήσεις καλύπτουν τις απαιτήσεις των 5W's και σκοπό έχουν να οδηγήσουν στην σωστή συλλογή πληροφοριών από τον συνεντευξιαζόμενο . Είναι ενδεικτικές και δεν δεσμευουν σε καμία περίπτωση αυτόν που εκτελεί την συνέντευξη.

1ο Σετ ερωτήσεων
1. **Ποιο είναι το όνομα του συστήματος, όπου τα στοιχεία δεδομένων συλλέγονται, αποθηκεύονται και διαμοιράζονται;** 2. **Ποιος είναι ο ιδιοκτήτης του συστήματος;** 3. **Ποιο είναι το όνομα της επιχειρηματικής λειτουργίας που χρησιμοποιεί το σύστημα;** 4. **Είναι αυτό το σύστημα κρίσιμο για την επιχείρηση;** 5. **Ποιος είναι ο κύριος σκοπός του συστήματος;** 6. **Ποιος είναι ο τύπος / λειτουργικότητα του συστήματος; (π.χ. συσκευή, διακομιστή, κατάλογος, εφαρμογή, ιστότοπος, εφαρμογή για κινητά)**

7. **Οι άδειες πρόσβασης έχουν οριστεί στο σύστημα για να διασφαλιστεί ότι οι χρήστες έχουν πρόσβαση μόνο ώσπου πρέπει ;**
8. **Ποιος ορίζεται ως διαχειριστής του συστήματος που είναι υπεύθυνος για τη χορήγηση πρόσβασης;**
9. **Ποιος είναι ο υπεύθυνος πληροφορικής για το σύστημα (IT Contact);**
10. **Ποια είναι η φυσική θέση του διακομιστή του συστήματος;**
11. **Το σύστημα φιλοξενείται από την εταιρεία ή από τρίτο μέρος; (Εάν ο τρίτος, ποιος)**

Πίνακας 1

2ο Σετ ερωτήσεων
1. **Το σύστημα επεξεργάζεται δεδομένα προσωπικού χαρακτήρα;** *(Προσωπικά Δεδομένα: Οποιεσδήποτε πληροφορίες σχετικά με αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο)(Αναγνωρίσιμο πρόσωπο: Κάποιος που μπορεί να αναγνωριστεί άμεσα ή έμμεσα, συμπεριλαμβανομένων με αναφορά σε ένα όνομα, έναν αριθμό αναγνώρισης, δεδομένα θέσης, ηλεκτρονικό αναγνωριστικό ή σε έναν ή περισσότερους παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστικού ή κοινωνικού προσδιορισμού αυτού του προσώπου.)* **2. Περιλαμβάνουν τα δεδομένα οποιουδήποτε από τους ακόλουθους τύπους πληροφοριών;** *(Φυλή, εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συνδικαλιστική οργάνωση, γενετικά δεδομένα, τα μοναδικά βιομετρικά δεδομένα, τα δεδομένα για την υγεία, τη σεξουαλική διαβίβαση δεδομένων προσανατολισμός και σεξουαλική δραστηριότητα*. **3. Ανασκοπείται η πρόσβαση στο σύστημα και ποια είναι η συχνότητα της αναθεώρησης;** **4. Έχει ακολουθηθεί μια πολιτική διατήρησης δεδομένων για αυτό το σύστημα και ποια είναι η πολιτική διατήρησης που ακολουθήθηκε;** **5. Ποια είναι η περίοδος διατήρησης των δεδομένων;**

Πίνακας 2

3ο Σετ ερωτήσεων
1. **Το σύστημα αυτό λαμβάνει δεδομένα από ή αποστέλλει δεδομένα σε εξωτερικό τρίτο μέρος;** 2. **Τα δεδομένα χρησιμοποιούνται από τρίτα μέρη που καλύπτονται από γραπτή σύμβαση;** 3. **Ποια εσωτερικά συστήματα τροφοδοτούν πληροφορίες σε αυτό το σύστημα;** 4. **Ποια εσωτερικά συστήματα λαμβάνουν πληροφορίες από αυτό το σύστημα;** 5. **Υπάρχει κάποια καταρτισμένο πλάνο για την προστασία προσωπικών δεδομένων;** 6. **Εάν το σύστημα παραβιαστεί, ποιες θα ήταν οι αναμενόμενες συνέπειες;** 7. **Υπάρχει πολιτική διαχείρισης παραβιάσεων δεδομένων ή συμβάντος;**

Πίνακας 3

4.2 Εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων (DPIA)

4.2.1 Εκτέλεση της DPIA

Με σκοπό να εφαρμοστεί η DPIA σε ένα νέο πληροφοριακό σύστημα επεξεργασίας δεδομένων, διατυπώνεται στη συνέχεια μια γενική προσέγγιση μεθοδολογίας, η οποία θα αποτελείται από τις κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων σχετικά με τη προστασία των δεδομένων να εκτελείται με όσον το δυνατόν περισσότερη σαφήνεια και μεθοδικότητα. Η διαδικασία αυτή αποτελείται από τα εξής βήματα:

- 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.

Κάθε επεξεργασία δεδομένων εντός της εταιρείας πρέπει να συμμορφώνεται με τις απαιτήσεις προστασίας δεδομένων και κάθε εταιρεία πρέπει να είναι σε θέση να αποδείξει την συμμόρφωση της. Το θέμα της εκτίμησης των επιπτώσεων στην αξιολόγηση κινδύνου / προστασία δεδομένων ("DPIA"), αποτελεί στοιχείο της γενικής έννοιας του GDPR για την προστασία δεδομένων. Το άρθρο 32 του GDPR διευκρινίζει την "ασφάλεια στην επεξεργασία" και στο άρθρο 35 του GDPR, την αξιολόγηση των επιπτώσεων στην προστασία δεδομένων. Και τα δύο άρθρα περιγράφουν τις ευθύνες του υπεύθυνου επεξεργασίας, σύμφωνα με το οποίο το άρθρο 32 του GDPR ισχύει και για τους εκτελούντες της επεξεργασία. Σύμφωνα με το άρθρο 32 του GDPR, η αξιολόγηση βασίζεται στην πιθανότητα εμφάνισης και τη σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Σε πολλές εταιρείες, τα μέτρα που πρέπει να εφαρμοστούν έχουν ήδη αξιολογηθεί όσον αφορά τις πτυχές που σχετίζονται με τον κίνδυνο - συχνά σε συμφωνία με την ασφάλεια των πληροφοριών σύστημα διαχείρισης ("ISMS"). Όσον αφορά το άρθρο 32 του GDPR, η μεθοδολογία που χρησιμοποιείται σήμερα είναι αυτή που ήδη εφαρμόζεται και είναι διαδεδομένη από την κλασσική ανάλυση και εκτίμηση κινδύνου. Όπως έχει ήδη καθιερωθεί σε πολλές εταιρείες, μπορεί να γίνει διάκριση μεταξύ βασικής ασφάλειας πληροφοριών, η οποία βασικά ισχύει για όλες τις διαδικασίες και εισαγωγή ειδικών μέτρων για την διαδικασία επεξεργασίας πληροφοριών.

Η αξιολόγηση αντίκτυπου για την προστασία των δεδομένων (άρθρο 35 του GDPR) είναι το αντίστοιχο του προηγούμενου (άρθρο 20 της οδηγίας 95/46 / ΕΚ).

Μια σημαντική καινοτομία που επιφέρει ο ΓΚΠΔ, συνίσταται στην καταρχήν κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την αρχή ελέγχου (εκάστοτε αρμόδια ΑΠΔΠΧ) της

επεξεργασίας, που προέβλεπε η Οδηγία 95/46/ΕΚ5 και η οποία βάρυνε τους υπευθύνους επεξεργασίας, και στην αντικατάστασή της:

> α. αφενός, από την υποχρέωση για τους υπευθύνους επεξεργασίας να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας, για τις οποίες είναι υπεύθυνοι, καθώς και την υποχρέωση για τους εκτελούντες την επεξεργασία να τηρούν αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, που διεξάγονται για λογαριασμό υπευθύνου επεξεργασίας,
>
> β. αφετέρου, από την υποχρέωση για τους υπευθύνους επεξεργασίας να διενεργούν εκτίμηση αντικτύπου (Data protection impact assessment - DPIA) σχετικά με την προστασία δεδομένων σε συγκεκριμένες κατηγορίες επεξεργασιών.

Η κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προς τις ΑΠΔΠΧ δικαιολογήθηκε από τη διαπίστωση ότι η υποχρέωση αυτή -παρά το ότι επιφέρει στις αρχές ελέγχου και, ιδίως, στους υπευθύνους επεξεργασίας διοικητικό και οικονομικό φόρτο- δεν συνέβαλε σε όλες τις περιπτώσεις στη βελτίωση της προστασίας των δεδομένων προσωπικού χαρακτήρα. Προκρίθηκε, συνεπώς, η αντικατάσταση αυτής της γενικής υποχρέωσης γνωστοποίησης από «αποτελεσματικές διαδικασίες και μηχανισμούς που επικεντρώνονται σε εκείνους τους τύπους πράξεων επεξεργασίας που ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους». Ως «τύποι πράξεων» επεξεργασίας, από τους οποίους ενδέχεται να προκύψουν κίνδυνοι για τα υποκείμενα των δεδομένων, χαρακτηρίζονται, ιδίως, εκείνοι που περιλαμβάνουν τη χρήση νέων τεχνολογιών ή είναι νέου τύπου και δεν έχει διενεργηθεί προηγούμενη εκτίμηση αντικτύπου ως προς την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας ή παρίσταται αναγκαία η αξιολόγησή τους, λόγω του χρόνου που έχει παρέλθει από την αρχική επεξεργασία. Στο πλαίσιο αυτό, η ρητή θέσπιση υποχρέωσης διενέργειας DPIA παρίσταται, καταρχάς, ως ένα αντιστάθμισμα στην κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας, με σκοπό την αντιμετώπιση των υψηλών κινδύνων, που ενδέχεται να προκύψουν για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους. Ωστόσο, η υποχρέωση διενέργειας DPIA θεσπίζεται -κατά τρόπο γενικότερο και σαφώς ουσιαστικότερο- στο ΓΚΠΔ κυρίως ως ένα μέτρο ενίσχυσης της συμμόρφωσης προς τις διατάξεις του, λαμβανομένης πάντοτε υπόψη της ανάγκης αντιμετώπισης των υψηλών κινδύνων, που ενδέχεται να προκύψουν για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους. Υπό την έννοια αυτή η υποχρέωση διενέργειας DPIA σημαίνει ότι ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να αξιολογήσει όλες τις παραμέτρους των κρίσιμων πράξεων επεξεργασίας

πριν από την έναρξή τους, προκειμένου να διασφαλίσει την αποτελεσματική προστασία των υποκειμένων. Επιπλέον, εάν απαιτείται από τις περιστάσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να πραγματοποιεί σχετικά διαβούλευση με την αρμόδια ΑΠΔΠΧ, πριν από την έναρξη της επεξεργασίας. Συνακόλουθα, η υποχρέωση διενέργειας DPIA σημαίνει, επίσης, ότι πρόκειται για ένα μέτρο, το οποίο είναι πλήρως ενταγμένο στην ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξορισμού (Privacy by design / Privacy by default), σύμφωνα με τα οριζόμενα στις διατάξεις του άρθρου 25 του ΓΚΔΠ.

4.2.2 Έννοια και περιεχόμενο της υποχρέωσης διενέργειας DPIA

Ο υπεύθυνος επεξεργασίας υποχρεούται ρητά σε διενέργεια DPIA, πριν από την κρίσιμη επεξεργασία, κάθε φορά που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών, και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας αυτής, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Είναι δυνατό η διενέργεια DPIA να μην αφορά μεμονωμένη επεξεργασία, αλλά ένα σύνολο πράξεων επεξεργασίας, εφόσον αυτές είναι παρόμοιες και ενέχουν παρόμοιους υψηλούς κινδύνους για τα ενδιαφερόμενα υποκείμενα. Ο ΓΚΠΔ, εξειδικεύοντας την έννοια των επεξεργασιών δυνάμενων να επιφέρουν ως άνω υψηλούς κινδύνους καθιστά –κατά τρόπο ενδεικτικό («ιδίως») και όχι περιοριστικό- τη διενέργεια DPIA υποχρεωτική σε τρεις τουλάχιστον τύπους επεξεργασιών:

α. 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,

β. 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) και

γ. της συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Πέρα από τους ως άνω τύπους επεξεργασιών που προσδιορίζονται ρητά, θεσπίζεται υποχρέωση για κάθε ΑΠΔΠΧ να καταρτίζει και να δημοσιοποιεί κατάλογο με τους τύπους επεξεργασίας, που υπόκεινται -κατά την κρίση της- στην υποχρέωση για διενέργεια DPIA. Θεσπίζεται, επίσης, ευχέρεια για κάθε ΑΠΔΠΧ να καταρτίζει και να δημοσιοποιεί κατάλογο με τους τύπους

επεξεργασίας, που –πάντοτε κατά την κρίση της- εξαιρούνται από την υποχρέωση για διενέργεια 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 ΑΠΔΠΧ στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Το ελάχιστο περιεχόμενο της DPIA, που διενεργείται υποχρεωτικά κατά τα προαναφερόμενα, σύμφωνα με το ΓΚΠΔ συνίσταται σε:

α. συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών αυτών, καθώς και του εννόμου συμφέροντος που επιδιώκει, κατά περίπτωση, ο υπεύθυνος επεξεργασίας, (β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς τους,

β. εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων

γ. 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.

Προσθέτουμε ότι, εφόσον υπάρχει εκτελών την επεξεργασία, αυτός θα πρέπει να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας, όταν χρειάζεται και αφού του ζητηθεί, ώστε να διασφαλίζει τη συμμόρφωση προς τις υποχρεώσεις, που απορρέουν από τη διενέργεια DPIA, σχετικά με την προστασία των δεδομένων, και από την προηγούμενη διαβούλευση με την αρμόδια ΑΠΔΠΧ.

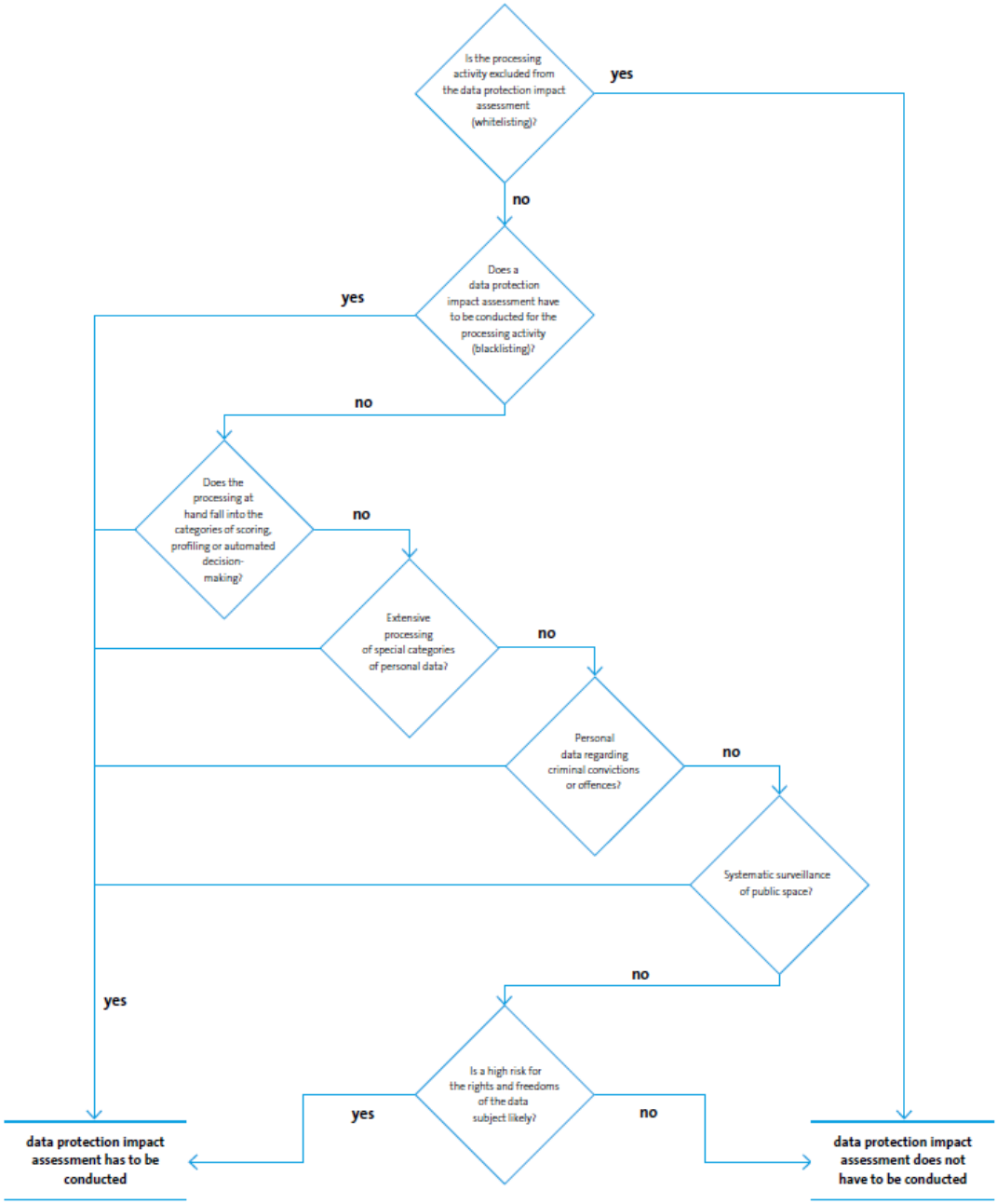
4.2.3 Απόφαση για διενέργεια DPIA

Οι αρχές προστασίας δεδομένων μπορούν να καταρτίσουν κατάλογο των δραστηριοτήτων επεξεργασίας για τις οποίες, γενικά, δεν απαιτείται εκτίμηση επιπτώσεων για την προστασία των δεδομένων (whitelist) και των ειδών επεξεργασίας δραστηριότητες που υπόκεινται πάντοτε στην απαίτηση για αξιολόγηση των επιπτώσεων στην προστασία των δεδομένων (blacklist). Σε ορισμένες περιπτώσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να διεξάγει αξιολόγηση των επιπτώσεων στην προστασία δεδομένων. Η σοβαρότητα της παρέμβασης στα θεμελιώδη δικαιώματα χρησιμεύει ως προσανατολισμός για την ταξινόμηση υψηλών κινδύνων για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Το GDPR απαιτεί από τον ελεγκτή να αξιολογεί τον κίνδυνο προστασίας δεδομένων βάσει αντικειμενικών κριτηρίων. Η άποψη του ευρωπαϊκού νομοθέτη είναι ότι ιδίως οι νέες τεχνολογίες αποτελούν έναυσμα για την υποχρέωση

διενέργειας αξιολόγησης αντικτύπου για την προστασία των δεδομένων. Ανεξαρτήτως της υποχρέωσης διεξαγωγής αξιολόγησης των επιπτώσεων στην προστασία των δεδομένων, αυτό μπορεί πάντα να γίνει εθελοντικά ως προσθήκη στην αξιολόγηση κινδύνου σύμφωνα με το άρθρο 32 του GDPR. Ως απλοποίηση της διαδικασίας, πολλές δραστηριότητες επεξεργασίας δεδομένων με παρόμοιο υψηλό κίνδυνο μπορούν να εξεταστούν σε μία μόνο αξιολόγηση. Σχηματικά παρουσιάζεται ακολούθως το δένδρο απόφασης.[5]

[5] Risk Assessment & Data Protection Impact Assessment bitKom

Δένδρο απόφασης για διενέργεια DPIA



Εικόνα 4

4.2.4 Οφέλη από την εκτέλεση της DPIA

Από την εκτέλεση και την ολοκλήρωση της εκτίμησης των επιπτώσεων σχετικά με την προστασία των προσωπικών δεδομένων προκύπτουν σημαντικά πλεονεκτήματα ουσιαστικής σημασίας για τον οργανισμό. Αυτά τα πλεονεκτήματα αφορούν το εσωτερικό και εξωτερικό περιβάλλον του οργανισμού και θα μπορούσαν να καταγραφούν ως εξής (European Commission – Directorate General Justice, 2012; Smart Grid Task Force, 2014; Information Commissioner's Office, 2014):

Εσωτερικά:

1. διαχείριση του κινδύνου (αναγνώριση και περιορισμός),
2. αποφυγή κοστοβόρων επαναπροσδιορισμών της διαδικασίας επεξεργασίας αλλά και της ίδιας της εφαρμογής εάν από την αρχή έχουν προσδιοριστεί οι ενδεχόμενοι κίνδυνοι και απειλές,
3. 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,
4. βελτίωση της προστασίας των προσωπικών δεδομένων και της αποδοτικότητας της συγκεκριμένης υπηρεσίας,
5. βελτίωση του τρόπου διαχείρισης των δεδομένων γνωρίζοντας τις πιθανές απειλές και αστοχίες,
6. αύξηση της ασφάλειας του συστήματος όσον αφορά την προστασία των δεδομένων και των γενικότερων λειτουργιών του οργανισμού που βασίζονται σε αυτό,
7. βελτίωση της τεχνογνωσίας σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριακών συστημάτων.

Εξωτερικά:

1. ενίσχυση της αξιοπιστίας του οργανισμού από την πλευρά των εμπλεκόμενων μερών και προώθηση του ehealth και των υπηρεσιών υγείας μέσω κινητών συσκευών,
2. υπόδειξη συμμόρφωσης με την νομοθεσία περί προστασίας προσωπικών δεδομένων και επιβεβαίωση ότι η ασφάλεια λαμβάνεται σοβαρά υπόψη.

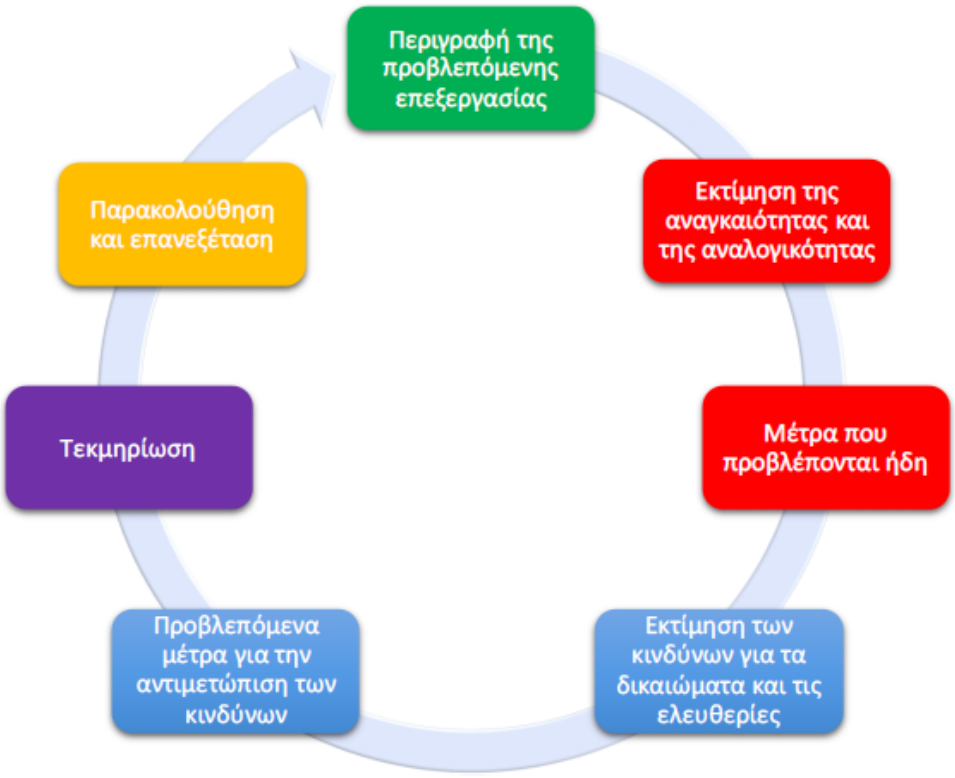
4.2.5 Μεθοδολογία διενέργειας DPIA

Ο κανονισμός δεν υποδεικνύει συγκεκριμένη μεθοδολογία για την διενέργεια μιας DPIA, σαφώς και υπάρχουν δοκιμασμένες βέλτιστες πρακτικές της οποίες μπορούμε να ακολουθήσουμε, ώστε να πετύχουμε τον σκοπό της DPIA. Αυτό φυσικά δίνει τη δυνατότητα σε αυτόν που διενεργεί την DPIA να επιλέξει μεταξύ πληθώρας και δοκιμασμένων τεχνικών που θα του δώσουν την δυνατότητα να επιτύχει ένα σωστό αποτέλεσμα. Μπορεί ο κανονισμός να μην προτείνει συγκεκριμένη μεθοδολογία όπως προαναφέρθηκε όμως είναι σαφής ως προς τα κριτήρια και τα χαρακτηριστικά τα οποία θα πρέπει να περιλαμβάνονται σε μία σωστή DPIA.

Ο κανονισμός ορίζει το ελάχιστο περιεχόμενο της DPIA (άρθρο 35 παράγραφος 7 και αιτιολογικές σκέψεις 84 και 90):

1. «περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας»·
2. «εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας»·
3. «εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων»·
4. «τα προβλεπόμενα μέτρα:
    - «αντιμετώπισης των κινδύνων»·
    - «απόδειξης της συμμόρφωσης με τον παρόντα κανονισμό».

Το ακόλουθο γράφημα απεικονίζει τη γενική επαναλαμβανόμενη διαδικασία που πρέπει να ακολουθείται για τη διενέργεια DPIA.



Εικόνα 5

Κατά την εκτίμηση του αντικτύπου μιας πράξης επεξεργασίας δεδομένων πρέπει να λαμβάνεται υπόψη (άρθρο 35 παράγραφος 8) η συμμόρφωση με έναν κώδικα δεοντολογίας (άρθρο 40). Τούτο μπορεί επίσης να χρησιμεύσει στην απόδειξη ότι έχουν επιλεγεί ή ληφθεί τα κατάλληλα μέτρα, με τον όρο ότι ο κώδικας δεοντολογίας ενδείκνυται για την πράξη επεξεργασίας. Θα πρέπει επίσης να λαμβάνονται υπόψη οι πιστοποιήσεις, οι σφραγίδες και τα σήματα [προστασίας των δεδομένων] για τον σκοπό της απόδειξης της συμμόρφωσης των πράξεων επεξεργασίας των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία (άρθρο 42) με τον κανονισμό, καθώς και οι δεσμευτικοί εταιρικοί κανόνες . Όλες οι συναφείς απαιτήσεις που περιέχει ο κανονισμός παρέχουν ένα ευρύ, γενικό πλαίσιο για τον σχεδιασμό και την υλοποίηση DPIA. Η πρακτική υλοποίηση μιας DPIA θα εξαρτηθεί από την πλήρωση των απαιτήσεων του κανονισμού, οι οποίες μπορεί να συμπληρωθούν με πιο αναλυτικές πρακτικές οδηγίες. Ως εκ τούτου, η υλοποίηση DPIA είναι κλιμακώσιμη. Τούτο σημαίνει ότι ακόμη και ένας μικρής εμβέλειας υπεύθυνος επεξεργασίας μπορεί να σχεδιάσει και να διενεργήσει DPIA πρόσφορη για τις πράξεις επεξεργασίας του.

Η αιτιολογική σκέψη 90 του κανονισμού παραθέτει μια σειρά στοιχείων της DPIA που αλληλεπικαλύπτονται με τα πλήρως καθορισμένα στοιχεία της διαχείρισης κινδύνων. Με όρους

διαχείρισης κινδύνου, μια DPIA αποσκοπεί στη «διαχείριση των κινδύνων» για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, με χρήση των ακόλουθων διαδικασιών, μέσω:

- του καθορισμού του πλαισίου: «λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας και τις πηγές του κινδύνου»·
- της εκτίμησης των κινδύνων: «ώστε να εκτιμήσει την ιδιαίτερη πιθανότητα και τη σοβαρότητα του υψηλού κινδύνου»·
- της αντιμετώπισης των κινδύνων: «που μετριάζουν αυτόν τον κίνδυνο» και «διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα» και «αποδεικνύουν τη συμμόρφωση προς τον παρόντα κανονισμό».

Η DPIA κατά τον κανονισμό αποτελεί εργαλείο διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, υιοθετεί τη δική τους οπτική, όπως ισχύει σε ορισμένους τομείς (π.χ. κοινωνική ασφάλεια). Αντιθέτως, σε άλλους τομείς η διαχείριση των κινδύνων (π.χ. ασφάλεια πληροφοριών) επικεντρώνεται στην οργανωτική διάρθρωση.

Ο κανονισμός παρέχει ευελιξία στους υπεύθυνους επεξεργασίας για τον καθορισμό της ακριβούς δομής και της μορφής της DPIA, προκειμένου αυτή να εξυπηρετεί τις υφιστάμενες πρακτικές εργασίας. Υπάρχουν πολυάριθμες καθιερωμένες διαδικασίες, εντός της ΕΕ και παγκοσμίως, που λαμβάνουν υπόψη τα στοιχεία που περιγράφονται στην αιτιολογική σκέψη 90. Ωστόσο, ανεξαρτήτως της μορφής που θα λάβει, η DPIA θα πρέπει να αποτελεί μια πραγματική αξιολόγηση των κινδύνων, που θα παρέχει στους υπεύθυνους επεξεργασίας τη δυνατότητα να λάβουν μέτρα για την αντιμετώπισή τους.

Διαφορετικές μεθοδολογίες θα μπορούσαν να χρησιμοποιηθούν για να συνδράμουν στην υλοποίηση των βασικών απαιτήσεων που θέτει ο κανονισμός. Έχουν προσδιοριστεί ορισμένα κοινά κριτήρια ώστε να επιτρέπεται στους υπεύθυνους επεξεργασίας να υιοθετούν διαφορετικές προσεγγίσεις, συμμορφούμενοι παράλληλα με τον κανονισμός. Τα εν λόγω κριτήρια αποσαφηνίζουν τις βασικές απαιτήσεις του κανονισμού και παρέχουν επαρκές έδαφος για τη χρήση διαφορετικών μορφών υλοποίησης. Τα εν λόγω κριτήρια μπορούν να χρησιμοποιηθούν για την απόδειξη ότι μια συγκεκριμένη μεθοδολογία DPIA πληροί τα απαιτούμενα πρότυπα που θέτει ο κανονισμός.[6]

[6] Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679 http://ec.europa.eu/justice/data-protection/index_en.htm

4.2.5.1 Βήματα εκτέλεσης DPIA

4.2.5.1.1 Βήμα 1 - Προκαταρκτική αξιολόγηση και κριτήρια που καθορίζουν την ανάγκη διεξαγωγής μιας DPIA

Ο στόχος του πρώτου βήματος είναι να παρέχει καθοδήγηση στον ιδιοκτήτη του συστήματος ή της υπηρεσίας να διαπιστώσει εάν είναι απαραίτητη μια DPIA και ποιος θα πρέπει να διεξάγει αυτή την DPIA. Προτείνεται συνεπώς στον ιδιοκτήτη του συστήματος να πραγματοποιήσει μια αρχική ανάλυση της υπό εξέταση αίτησης και να αποφασίσει εάν θα προχωρήσει στα επόμενα βήματα της DPIA ή θα σταματήσει τη διαδικασία. Κατά τη διάρκεια αυτού του βήματος θα πρέπει να απαντηθούν βασικά ερωτήματα :

1) Γίνεται επεξεργασία προσωπικών δεδομένων;
2) Λειτουργεί ως εκτελών την επεξεργασία ή ως υπεύθυνος επεξεργασίας;
3) Υπάρχει αντίκτυπο στα δικαιώματα και τις ελευθέριες του ατόμου;
4) Σε ποιο στάδιο της ανάπτυξης θα πρέπει να διενεργηθεί η DPIA;
5) Ποιος είναι ο σκοπός της υπηρεσίας ή του συστήματος που επεξεργάζεται προσωπικά δεδομένα;

Οι θετικές απαντήσεις υποστηρίζουν την ανάγκη διεξαγωγής μιας DPIA. Δεν πρόκειται για ποσοτική άσκηση. Αυτό σημαίνει ότι μία μόνο θετική απάντηση θα μπορούσε να καταστήσει αναγκαία τη διεξαγωγή μιας DPIA.

4.2.5.1.2 Βήμα 2 - Αρχικοποίηση

Κατά την εκκίνηση μιας DPIA πρέπει να λαμβάνονται υπόψη διαφορετικά στοιχεία και να αποτυπώνονται :

1) Καταγραφή ομάδας έργου
2) Καταγραφή ρόλου ομάδας ή ατόμου
3) Καταγραφή αρμοδιοτήτων ομάδας έργου
4) Καταγραφή συνεντευξιαζόμενων και εγγράφων που παρέχονται

4.2.5.1.3 Βήμα 3 - Προσδιορισμός, χαρακτηρισμός και περιγραφή των συστημάτων / εφαρμογών που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα

Σε αυτό το βήμα, ο ιδιοκτήτης του συστήματος πρέπει να δώσει μια ολοκληρωμένη και πλήρη εικόνα της εφαρμογής, του περιβάλλοντος, των επεξεργασμένων δεδομένων και των ορίων του συστήματος. Πρέπει να περιγραφεί ο σχεδιασμός της εφαρμογής, οι γειτονικές διεπαφές με άλλα συστήματα και οι ροές πληροφοριών. Τα διαγράμματα ροής δεδομένων που δείχνουν επεξεργασία

πρωτογενών και δευτερευόντων δεδομένων συνιστώνται για την απεικόνιση της προέλευσης, της θέσης και του προορισμού των δεδομένων. Οι δομές δεδομένων πρέπει επίσης να τεκμηριώνονται, έτσι ώστε να μπορούν να αναλυθούν πιθανοί σύνδεσμοι. Για να επιτευχθεί αυτό, ο ιδιοκτήτης του συστήματος θα κληθεί να συμπληρώσει ένα σύνολο πινάκων. Κάθε πίνακας συνοδεύεται από μια σειρά οδηγιών σχετικά με τον τρόπο με τον οποίο θα πρέπει να συμπληρωθεί προκειμένου να παρέχεται καθοδήγηση μέσω αυτού του μέρους της διαδικασίας, όπως έχει περιγραφεί αναλυτικά σε προηγούμενα κεφάλαια.

4.2.5.1.4 Βήμα 4 - Προσδιορισμός των πιθανών κινδύνων

Ο στόχος αυτού του βήματος είναι να προσδιοριστούν οι συνθήκες και οι δυνητικοί κίνδυνοι που ενδέχεται να απειλήσουν ή να διακυβεύσουν τα προσωπικά δεδομένα του υποκειμένου των δεδομένων και να επηρεάσουν την ιδιωτική του ζωή με βάση κανονισμό. Μια διαδικασία εκτίμησης κινδύνου θα πρέπει συνήθως να εξετάζει τους κινδύνους από την άποψη της πιθανότητας εμφάνισης (likelihood) και τον αντίκτυπο των συνεπειών τους (impact). Αυτοί οι κίνδυνοι απορρήτου αποτελούνται κυρίως από ένα ακραίο γεγονός και τις απειλές που θα μπορούσαν να πυροδοτήσουν αυτό το γεγονός (πολλές απειλές μπορούν να προκαλέσουν το ίδιο γεγονός). Ο υπεύθυνος προστασίας θα πρέπει να συμμετέχει στην ανάλυση αυτή, όπως έχει ήδη προταθεί.

Τα ακραία γεγονότα αντιπροσωπεύουν τις ακόλουθες καταστάσεις που πρέπει να αποφευχθούν:

- Μη διαθεσιμότητα των νομικών διαδικασιών: δεν υπάρχουν ή δεν υπάρχουν πλέον ή δεν λειτουργούν
- Αλλαγή της επεξεργασίας: αποκλίνει από αυτό που είχε αρχικά προγραμματιστεί (εκτροπή του σκοπού, υπερβολική ή αθέμιτη συλλογή ...).
- Αθέμιτη πρόσβαση σε προσωπικά δεδομένα: αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- Ανεπιθύμητη αλλαγή στα προσωπικά δεδομένα: τροποποιούνται ή αλλάζουν.
- Εξαφάνιση προσωπικών δεδομένων: καταστρέφονται ή δεν είναι πλέον διαθέσιμα.
- Γνωστοποίηση των προσωπικών δεδομένων σε άλλους: διανέμονται σε άτομα που δεν χρειάζονται.

Κάθε φορά που ένα τέτοιο γεγονός μπορεί να συμβεί, επιφέρει επιπτώσεις στην ιδιωτική ζωή των υποκειμένων των δεδομένων και οι εν λόγω επιπτώσεις θα πρέπει να αξιολογούνται δεόντως και συστηματικά και τελικά να μετριάζονται.

Ατυχώς ή εσκεμμένα, αυτά τα γεγονότα μπορούν να δημιουργηθούν από μία ή περισσότερες πηγές κινδύνου :

- Εσωτερική πηγή: πρόσωπα που ανήκουν στον οργανισμό, χρήστης, διαχειριστής συστήματος, διαχειριστής δικτύου, υπηρεσία χειριστής τηλεφωνικού κέντρου, υπάλληλο εμπορικής υπηρεσίας
- Εξωτερικοί συνεργάτες: άτομα εκτός του οργανισμού: αποδέκτης, πάροχος, ανταγωνιστής, εξουσιοδοτημένο τρίτο μέρος, κυβερνητική οργάνωση, ανθρώπινη δραστηριότητα που περιβάλλει, εξωτερική / υπεργολαβία
- Μη ανθρώπινες πηγές: προβληματικοί αισθητήρες, ιός υπολογιστών, φυσική καταστροφή όπως κεραυνός, ενεργειακή ανισορροπία, διακοπή ρεύματος, διακοπή λειτουργίας.

4.2.5.1.5 Βήμα 5 - Αξιολόγηση κινδύνου προστασίας δεδομένων

Σε αυτό το βήμα, τα προσδιορισμένα ακραία γεγονότα και οι σχετικές απειλές θα αξιολογούνται και θα μετρούνται με βάση τη σοβαρότητα των επιπτώσεων στα άτομα και την πιθανότητα εμφάνισης. Για να ταξινομηθούν οι επιπτώσεις και η πιθανότητα, μπορούν να χρησιμοποιηθούν αρκετά ευρέως διαθέσιμα μοντέλα. Είναι αποδεκτή η χρήση εναλλακτικών μεθοδολογιών. είτε βιομηχανικών είτε εσωτερικών, εφόσον οι κίνδυνοι για την προστασία της ιδιωτικής ζωής που μπορούν να επηρεάσουν το υποκείμενο των δεδομένων προσδιορίζονται και ποσοτικοποιούνται κατάλληλα.

4.2.5.1.6 Βήμα 6 – Προσδιορισμός, σύσταση ελέγχων και υπολειπόμενοι κίνδυνοι

Στο στάδιο αυτό, ο στόχος είναι να εξεταστούν οι κίνδυνοι που εντοπίστηκαν και αξιολογήθηκαν στο προηγούμενο στάδιο και να παρουσιαστούν οι έλεγχοι που έχουν εφαρμοστεί ή πρόκειται να εφαρμοστούν προκειμένου να μειωθεί ο κίνδυνος σε κατάλληλα επίπεδα. Κάθε προσδιορισμένος κίνδυνου πρέπει να μετριαστεί κατάλληλα με έναν ή περισσότερους ελέγχους, λαμβάνοντας υπόψη την πιθανότητα και τον αντίκτυπό τους. Οι έλεγχοι που έχουν εγκριθεί ή έχουν ήδη σχεδιαστεί από τον ιδιοκτήτη του συστήματος πρέπει να καλύπτουν τις ακόλουθες διαστάσεις:

- Η υποδομή (δίκτυο επικοινωνιών, προστασία εξοπλισμού, κλπ.).
- Οι υπάλληλοι / προσωπικό που εμπλέκονται στη διαδικασία (μηχανισμοί πρόσβασης, ελέγχου κ.λπ.).
- Η οργάνωση και οι διαδικασίες.
- Οι τεχνολογίες (μέτρα προστασίας του συστήματος, συμπεριλαμβανομένου του ελέγχου ασφάλειας και της μεθοδολογίας ασφάλειας με βάση την τεχνολογία, κ.λπ.).

Η έκθεση DPIA πρέπει να εξηγεί λεπτομερώς τον τρόπο με τον οποίο οι επιλεγόμενοι (εφαρμοζόμενοι ή προγραμματισμένοι) έλεγχοι σχετίζονται με συγκεκριμένους κινδύνους και πρέπει να αποδεικνύουν ότι οδηγούν σε αποδεκτά επίπεδα κινδύνου. Όταν ο κίνδυνος μοιράζεται με τρίτους, ο κάτοχος του συστήματος θα πρέπει επίσης να διευκρινίσει ποιος έλεγχος έχει εφαρμόσει ή σκοπεύει να εφαρμόσει αυτό το τρίτο μέρος προκειμένου να αντιμετωπίσει αυτόν τον κίνδυνο με αποδεκτό τρόπο. Συνιστάται επίσης να σχεδιαστεί και να εφαρμοστεί μια εσωτερική διαδικασία, με σκοπό την τακτική επαλήθευση της ύπαρξης συγκεκριμένων ελέγχων (π.χ. διενέργεια ελέγχων σε τακτική βάση, ο οποίος αποτελεί τον τελικό έλεγχο.

4.2.5.1.7 Βήμα 7 - Τεκμηρίωση και σύνταξη της έκθεσης DPIA

Οι επιδόσεις της DPIA μετά τις φάσεις που προσδιορίστηκαν παραπάνω πρέπει να τεκμηριώνονται δεόντως και τα αποτελέσματά της να παρουσιάζονται στην τελική έκθεση DPIA. Η έκθεση DPIA μπορεί να δομηθεί γύρω από τις φάσεις της εργασίας που περιγράφονται σε αυτό το έγγραφο, παρουσιάζοντας τα αποτελέσματα κάθε φάσης στον αναγνώστη, επισυνάπτοντας οποιαδήποτε δικαιολογητικά ή υλικό που χρησιμοποιήθηκε στην αξιολόγηση. Ο στόχος της τεκμηρίωσης είναι διττός: α) να διευκολυνθεί η εφαρμογή της διαδικασίας και β) να εκπονηθεί τελική έκθεση η οποία θα μπορούσε να υποβληθεί στην ΑΠΔΠΧ εάν ζητηθεί. Η DPIA περιλαμβάνει εσωτερικές διαδικασίες και μπορεί να χειρίζονται ιδιόκτητες διαβαθμισμένων πληροφορίων του οργανισμού που σχετίζονται με προϊόντα και διαδικασίες, με ειδικές απαιτήσεις εμπιστευτικότητας. Ως εκ τούτου, η ανάλυση που πραγματοποιήθηκε και η τεκμηρίωσή της ίσως χρειαστεί να εξασφαλιστούν κατάλληλα, σύμφωνα με το σύστημα ταξινόμησης πληροφοριών του οργανισμού. Η υπογεγραμμένη έκθεση DPIA, η οποία περιέχει εγκεκριμένη απόφαση, θα πρέπει να δίδεται στον υπεύθυνο προστασίας δεδομένων του εκάστοτε οργανισμού (εάν υπάρχει) σύμφωνα με τις εσωτερικές διαδικασίες του ιδιοκτήτη του συστήματος.

4.2.5.1.8 Βήμα 8 - Αναθεώρηση και συντήρηση

Σκοπός αυτής της φάσης είναι να διασφαλιστεί ότι η ανάληψη υποχρέωσης που απορρέει από την διεξαχθείσα DPIA διεξάγεται στο υπάρχον σύστημα ή στο έργο που υλοποιείται. Προτείνονται οι ακόλουθες εργασίες:

- Επανεξέταση της εφαρμογής των ελέγχων μετριασμού και αποφυγής κινδύνου που εντοπίστηκαν στην DPIA.
- Προετοιμασία έκθεσης ανασκόπησης.
- Παρουσίαση της έκθεσης ανασκόπησης απορρήτου στα ανώτερα διευθυντικά στελέχη και τον DPO εφόσον υπάρχει.
- Δημοσιοποίηση της έκθεσης απορρήτου.

- Αξιολόγηση της ανάγκης για αναθεώρηση της DPIA μετά από ορισμένο χρονικό διάστημα ή μετά την ολοκλήρωση ενός νέου σταδίου στο έργο ή το πρόγραμμα. Η ανασκόπηση μπορεί να ενσωματωθεί στις τυπικές, περιοδικές ή περιστασιακές εσωτερικές διαδικασίες του οργανισμού.

4.2.6 Κριτήρια για μια αποδεκτή DPIA

Η ομάδα εργασίας του άρθρου 29 προτείνει τα ακόλουθα κριτήρια, τα οποία οι υπεύθυνοι επεξεργασίας μπορούν να χρησιμοποιούν για να αξιολογούν κατά πόσο μια ΕΑΠΔ ή μια μεθοδολογία διενέργειας DPIA είναι επαρκώς περιεκτική προκειμένου να συμμορφώνεται με τον κανονισμό:

1. παρέχεται συστηματική περιγραφή των πράξεων επεξεργασίας [άρθρο 35 παράγραφος 7 στοιχείο α)]:
   α. λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)·
   β. καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα·
   γ. παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας·
   δ. προσδιορίζονται τα στοιχεία του ενεργητικού στα οποία εναποτίθενται τα δεδομένα (υλισμικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)·
   ε. λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας (άρθρο 35 παράγραφος 8)·
2. εκτιμώνται η αναγκαιότητα και η αναλογικότητα [άρθρο 35 παράγραφος 7 στοιχείο β)]·
   α. καθορίζονται τα προβλεπόμενα μέτρα συμμόρφωσης με τον κανονισμό [άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90], λαμβάνοντας υπόψη:
      i. τα μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει:
         - καθορισμένων, ρητών και νόμιμων σκοπών [άρθρο 5 παράγραφος 1 στοιχείο β)]·
         - της νομιμότητας της επεξεργασίας (άρθρο 6)·
         - κατάλληλων, συναφών και περιορισμένων στα αναγκαία δεδομένων [άρθρο 5 παράγραφος 1 στοιχείο γ)]·
         - της περιορισμένης διάρκειας αποθήκευσης [άρθρο 5 παράγραφος 1 στοιχείο ε)]·
      ii. μέτρα που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων:
         - πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14):

- δικαίωμα πρόσβασης και δικαίωμα στη φορητότητα των δεδομένων (άρθρα 15 και 20)·
- δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19)·
- δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21)·
- σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28)·
- διασφαλίζονται οι περιστάσεις που περιβάλλουν τη διεθνή διαβίβαση ή τις διεθνείς διαβιβάσεις (Κεφάλαιο V)·
- προηγούμενη διαβούλευση (άρθρο 36).

3. τελούν υπό διαχείριση οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων [άρθρο 35 παράγραφος 7 στοιχείο γ)]:
   α. έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (πρβλ. αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων·
      i. έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90)·
      ii. εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων· [7]

4.2.7 Κόστος εφαρμογής της DPIA

Η υποχρέωση των εκτελούντων της επεξεργασίας προσωπικών δεδομένων να διενεργούν εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων (DPIA), όπου η επεξεργασία φαίνεται να παρουσιάζει κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, επιφέρει ένα επιπλέον κόστος για τον εκάστοτε οργανισμό, με την έννοια ότι χρειάζεται πόρους για να εκτελέσει την εν λόγω εκτίμηση. Η εκτίμηση του πιθανού κόστους της DPIA εξαρτάται από έναν σημαντικό αριθμό παραγόντων. Το μέγεθος και η αυστηρότητα της DPIA θα εξαρτηθούν κυρίως από το πώς ο οργανισμός αντιλαμβάνεται τους κινδύνους αλλά και τη σοβαρότητα με την οποία τους αντιμετωπίζει. Η εκτίμηση του πιθανού κόστους της DPIA εξαρτάται από τους ενδεικτικά κάτωθι συναφείς παράγοντες:

- μέγεθος της εκτίμησης,

[7] Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679 http://ec.europa.eu/justice/data-protection/index_en.htm

- αυστηρότητα της νομοθεσίας,
- συμμετοχή των εμπλεκόμενων μερών,
- πρόσληψη ειδικού στελέχους για την εκτέλεση της εκτίμησης.

Προσθέτοντας όλες τις παραπάνω πιθανές δαπάνες γίνεται κατανοητό πως η DPIA αποτελεί μια διαδικασία που κοστίζει αρκετά. Το ζήτημα που εγείρεται είναι αν το όφελος από την DPIA όντως καλύπτει το κόστος της, κάτι που μπορεί να εξακριβωθεί από μια ανάλυση κόστους-οφέλους, λαμβάνοντας όμως υπόψη και επιπλέον ποιοτικούς παράγοντες .

4.3 Ανάλυση αποκλίσεων (GAP Analysis)

Σκοπός της ανάλυσης αποκλίσεων (GAP analysis) είναι, να βοηθήσει την εταιρεία ή τον οργανισμό να καταλάβει που βρίσκεται σχετικά με την συμμόρφωση του ως προς το GDPR.Εκτός από βασική διεργασία που θα πρέπει να εκτελεστεί, ώστε να βοηθήσει στην αναγνώριση των κενών που προκύπτουν ως προς την συμμόρφωση, μπορεί να βοηθήσει και στην εξέλιξή της συμμόρφωσης ως μέτρο σύγκρισης και μέτρησης της προόδου που έχει γίνει. Επίσης η ανάλυση αποκλίσεων μπορεί να :

- Βοηθήσει την εταιρεία ώστε να επικεντρωθεί στις βασικές αρχές του GDPR
- Βοηθήσει την εταιρεία να δώσει την σωστή βαρύτητα στα δικαιώματα του ατόμου
- Βοηθήσει στην κατανόηση του βασικού σκοπού της εταιρείας
- Αναδείξει κενά ως προς νομικές υποχρεώσεις εκτός GDPR
- Δώσει μια γενική εικόνα των ελέγχων ιδιωτικότητας που εφαρμόζονται
- Δώσει μια γενική εικόνα των πολιτικών και των διαδικασιών που μπορούν να έχουν αντίκτυπο στην ιδιωτικότητα
- Αναδείξει κινδύνους για την προστασία δεδομένων

Η ανάλυση αποκλίσεων θα πρέπει να εκτελείται μέσω ερωτήσεων οι οποίες να καλύπτουν ξεκάθαρα τις ανάγκες των παρακάτω τομέων:

1. Ενημέρωση για θέματα προστασίας δεδομένων
2. Πληροφορίες και δεδομένα που διατηρούνται
3. Επικοινωνία σχετικά με θέματα προστασίας δεδομένων
4. Ατομικά δικαιώματα
5. Θέματα αιτήσεων πρόσβασης
6. Νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα
7. Παιδία
8. Συγκατάθεση

9. Παραβιάσεις δεδομένων
10. Προστασία δεδομένων κατά τον σχεδιασμό - Εκτιμήσεις επιπτώσεων προστασίας
11. Υπεύθυνοι προστασίας δεδομένων
12. Διεθνές περιβάλλον

4.3.1 Μεθοδολογία εκτέλεσης ανάλυσης αποκλίσεων

Η μεθοδολογία εκτέλεσης της ανάλυσης αποκλίσεων θα πρέπει να περιλαμβάνει ένα σετ ερωτήσεων, με βάση το οποίο θα μπορεί να αποτυπώνεται η πραγματική εικόνα ως προς τη προστασία των δεδομένων αλλά και σε σχέση με της ανάγκες τους GDPR. Για αυτό το σκοπό είναι απαραίτητο το πλαίσιο να είναι οριοθετημένο με βάση τους τομείς που αναφέρθηκαν στην προηγούμενη ενότητα.

- *Ενημέρωση για θέματα προστασίας δεδομένων*: Πρέπει να βεβαιωθείτε ότι οι υπεύθυνοι λήψης αποφάσεων και οι εργαζόμενοι στον οργανισμό γνωρίζουν και είναι ενημερωμένοι για το GDPR καθώς και να μπορούν να κατανοήσουν το αντίκτυπο.
- *Πληροφορίες και δεδομένα που διατηρούνται*: Θα πρέπει να τεκμηριωθεί ποια προσωπικά δεδομένα διατηρούνται, από πού προήλθαν και με ποιον μοιράζονται.
- *Επικοινωνία σχετικά με θέματα προστασίας δεδομένων*: Θα πρέπει να ελεγχθούν οι τρέχουσες ειδοποιήσεις απορρήτου και δημιουργηθεί ένα σχέδιο δράσης.
- *Ατομικά δικαιώματα*: Θα πρέπει να γίνει έλεγχος στις διαδικασίες σας για να βεβαιωθεί ότι καλύπτουν όλα τα δικαιώματα που πρέπει να έχουν τα άτομα.
- *Θέματα αιτήσεων πρόσβασης*: Θα πρέπει να ενημερωθούν οι διαδικασίες και να σχεδιαστεί τρόπος χειρισμού αιτημάτων εντός των νέων χρονοδιαγραμμάτων για την παροχή πληροφοριών προς τα υποκείμενα επεξεργασίας.
- *Νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα*: Θα πρέπει να προσδιοριστεί η νόμιμη βάση για την επεξεργασία
- *Παιδία*: Θα πρέπει να εξεταστεί αν μπορούν να τεθούν σε εφαρμογή συστήματα για την επαλήθευση της ηλικίας και να λάβουν τη συγκατάθεση των γονέων ή των κηδεμόνων οποιαδήποτε δραστηριότητα επεξεργασίας δεδομένων για παιδία
- *Συγκατάθεση*: Θα πρέπει να ελεγχθεί ο τρόπος που αναζήτησης, καταγραφής και διαχείρισης τη συγκατάθεσης
- *Παραβιάσεις δεδομένων*: Πρέπει να εξεταστεί ότι υπάρχουν οι σωστές διαδικασίες για την ανιχνεύσει παραβίασης δεδομένων.

- *Προστασία δεδομένων κατά τον σχεδιασμό - Εκτιμήσεις επιπτώσεων προστασίας:* Θα πρέπει να υπάρχει εξοικείωση με τον κώδικα πρακτικής για την αξιολόγηση επιπτώσεων στην ιδιωτική ζωή καθώς και εναρμόνιση με τις τελευταίες κατευθυντήριες γραμμές του Άρθρου 29 της Ομάδας εργασίας .
- *Υπεύθυνοι προστασίας δεδομένων* : Θα πρέπει να ορίστεί κάποιος που θα αναλάβει την ευθύνη για τη συμμόρφωση με την προστασία των δεδομένων και να εκτιμήσει.
- *Διεθνές περιβάλλον*: Εάν ο οργανισμός λειτουργεί σε περισσότερες από μία χώρες της ΕΕ (δηλαδή διεξάγονται διασυνοριακές συναλλαγές επεξεργασίας), θα πρέπει να καθοριστούν τα δεδομένα του οδηγού και να γνωστοποιηθούν στην εποπτικής αρχής προστασίας.

Για την εφαρμογή της μεθοδολογίας προτείνεται η δημιουργία ερωτηματολογίου, με σετ ερωτήσεων που αποσκοπούν στην καταγραφή της υφιστάμενης κατάστασης υλοποίησης ως προς την συμμόρφωση. Το ερωτηματολόγιο θα πρέπει να απευθύνεται σε άτομα της εταιρείας που έχουν συναφή σχέση με την συμμόρφωση και την προστασία δεδομένων.

Η οργάνωση και δομή των ερωτήσεων θα πρέπει να καλύπτουν όλο το εύρος που αφορά την προστασία προσωπικών δεδομένων, για αυτό το σκοπό ο κορμός των ερωτήσεων θα πρέπει να καλύπτουν του κάτωθι βασικούς πυλώνες :

- **Προσδιορισμός δεδομένων**: όπως ήδη έχει αναφερθεί το πρώτο βήμα προς τη συμμόρφωση με το GDPR είναι να αξιολογηθεί εάν το GDPR ισχύει για τον οργανισμό και, εάν ναι, σε ποιο βαθμό. Αυτή η ανάλυση αρχίζει με την κατανόηση των δεδομένων που διατηρεί και επεξεργάζεται ο οργανισμός καθώς και με το που αυτά βρίσκονται.
- **Διαχείριση δεδομένων**: Το GDPR παρέχει στα υποκείμενα των δεδομένων - τα άτομα στα οποία αναφέρονται τα δεδομένα - τον έλεγχο του τρόπου συλλογής και χρήσης των προσωπικών τους δεδομένων. Τα υποκείμενα δεδομένων μπορούν για παράδειγμα να ζητήσουν από τον οργανισμό να παράσχει πληροφορίες σχετικά με την επεξεργασία των δεδομένων που σχετίζονται με αυτούς, να μεταφέρει τα δεδομένα τους σε άλλες υπηρεσίες, να διορθώσει λάθη στα δεδομένα τους ή να περιορίσει ορισμένα δεδομένα από περαιτέρω επεξεργασία σε ορισμένες περιπτώσεις. Σε ορισμένες περιπτώσεις, οι αιτήσεις αυτές πρέπει να απευθύνονται εντός καθορισμένων χρονικών περιόδων
- **Προστασία δεδομένων**: Οι οργανισμοί κατανοούν όλο και περισσότερο τη σημασία της ασφάλειας των πληροφοριών - αλλά το GDPR αυξάνει τη πίεση προς αυτή την κατεύθυνση. Απαιτεί οι οργανισμοί να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων από απώλεια ή μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη.

- **Αναφορές δεδομένων**: Το GDPR θέτει νέα πρότυπα στη διαφάνεια, τη λογοδοσία και την τήρηση αρχείων. Θα πρέπει να υπάρχει διαφάνεια όχι μόνο για το πώς χειρίζεται ένας οργανισμός τα προσωπικά δεδομένα, αλλά και για το πώς διατηρεί την τεκμηρίωση που καθορίζει, τις διαδικασίες για τη χρήση των προσωπικών δεδομένων.

Η δημιουργία ερωτήσεων που μπορούν να απαντηθούν από την συνεντευξιαζόμενο απλώς με ΝΑΙ/ΟΧΙ θα μπορούσε να είναι της μορφής των πινάκων που ακολουθούν :

1. Προσδιορισμός δεδομένων	
Υποκατηγορία	**Ερώτηση**
1. Αναζήτηση και αναγνώριση προσωπικών δεδομένων	1. Μπορεί ο οργανισμός να αναγνωρίσει γενικά όλες τις τοποθεσίες όπου αποθηκεύονται προσωπικά δεδομένα στην επιχείρηση; 2. Έχει ο οργανισμός την δυνατότητα εντοπισμού όλων των περιπτώσεων προσωπικών δεδομένων που αφορούν συγκεκριμένο υποκείμενο δεδομένων; 3. Έχει ο οργανισμός μια τυπική διαδικασία για την αναζήτηση δεδομένων προσωπικού χαρακτήρα με συνεπή και έγκαιρο τρόπο; 4. Υπάρχει τεχνολογία για να μπορεί το προσωπικό να χρησιμοποιεί μια ενιαία αναζήτηση που επιστρέψει όλες τις περιπτώσεις δεδομένων προσωπικού χαρακτήρα για ένα συγκεκριμένο υποκείμενο δεδομένων;
2. Χρήση ταξινόμησης δεδομένων	5. Μπορεί ο οργανισμός να κατηγοριοποιήσει τα είδη των προσωπικών δεδομένων που χρησιμοποιεί; 6. Χρησιμοποιείται κατηγοριοποίηση δεδομένων σε διαφορετικούς βαθμούς ευαισθησίας, όπως "ευαίσθητα", "εμπιστευτικά" ή "δημόσια"; 7. Χρησιμοποιούνται στοιχεία ετικετών με τους γεωγραφικούς περιορισμούς που ενδέχεται να ισχύουν; 8. Χρησιμοποιείται ετικέτα της προέλευσης των δεδομένων, δηλαδή εάν τα δεδομένα παρασχέθηκαν από το υποκείμενο των δεδομένων ή αποκτήθηκαν με άλλα μέσα; 9. Εκτελούνται δραστηριότητες ταξινόμησης δεδομένων με συνεπή και έγκαιρο τρόπο;
3. Διατήρηση καταλόγου των δεδομένων προσωπικού χαρακτήρα	10. Διαθέτει ο οργανισμός ένα εργαλείο για να καταγράψει πώς και πού χρησιμοποιούνται τα προσωπικά δεδομένα; 11. Έχει γίνει πλήρης απογραφή του πώς και πού χρησιμοποιούνται τα προσωπικά δεδομένα; 12. Υπάρχει τεχνολογία για την αυτοματοποίηση ή μερική αυτοματοποίηση ενημερώσεων του καταλόγου;

13. Υπάρχει διαδικασία που χρησιμοποιείται τακτικά για την ενημέρωση του καταλόγου;
14. Υπάρχουν τεκμηριωμένα στοιχεία για κάθε δραστηριότητα επεξεργασίας, συμπεριλαμβανομένου του πεδίου εφαρμογής, του σκοπού και των κριτηρίων για το πότε απαιτείται η κοινοποίηση και η συναίνεση;

Πίνακας 4

2. Διαχείριση δεδομένων	
Υποκατηγορία	**Ερώτηση**
1. Διαδικασίες διακυβέρνησης δεδομένων	15. Διαθέτει ο οργανισμός πρόγραμμα διαχείρισης δεδομένων; 16. Υπάρχει οργανωτική δομή και ένας επίσημος χάρτης για τη συνεχή εκτέλεση του προγράμματος; 17. Υπάρχει συμφωνία σε όλα τα τμήματα για να διασφαλιστεί ότι η διακυβέρνηση δεδομένων είναι συνεπής και αποτελεσματική σε ολόκληρο τον οργανισμό; 18. Υπάρχουν ειδικές προστασίες για τα προσωπικά δεδομένα των παιδιών; 19. Υπάρχουν πολιτικές απορρήτου και προστασίας δεδομένων; 20. Υπάρχει νομική αιτιολόγηση τεκμηριωμένη για τη χρήση ειδικών κατηγοριών προσωπικών δεδομένων;
2. Αναφορά στις δραστηριότητες επεξεργασίας των υποκείμενων των δεδομένων	21. Παρέχει η εταιρεία στα υποκείμενα των δεδομένων ειδοποιήσεις σχετικά με το απόρρητο (privacy notice); 22. Είναι γραμμένα με σαφή και κατανοητό τρόπο ; 23. Μοιράζεται με τα υποκείμενα δεδομένων όλα τα σημεία όπου συλλέγονται τα προσωπικά δεδομένα; 24. Κοινοποιείται στα υποκείμενα των δεδομένων κάθε νέα μορφή επεξεργασίας πρώτού αυτή ξεκινήσει;
3. Διακοπή επεξεργασίας κατόπιν αιτήματος	25. Όταν ζητείται από ένα υποκείμενο δεδομένων, μπορεί ο οργανισμός να διακόψει την επεξεργασία ορισμένων μορφών προσωπικών δεδομένων; 26. Μπορεί ο οργανισμός να διατηρήσει αποδεικτικά στοιχεία για τη διακοπή χρήσης προσωπικών δεδομένων; 27. Χρησιμοποιείται μια καθιερωμένη διαδικασία για να απαντάτε με συνέπεια και γρήγορα στα αιτήματα των υποκειμένων των δεδομένων να σταματήσουν να χρησιμοποιούν τα δεδομένα τους;
4. Συλλογή με συγκατάθεση	28. Λαμβάνει ο οργανισμός τη συγκατάθεση των υποκειμένων των δεδομένων για να επεξεργαστεί τα προσωπικά τους δεδομένα; 29. Ακολουθείται συνεχής και έγκαιρη απόκτηση συγκατάθεσης του υποκειμένου δεδομένων για όλες τις δραστηριότητες επεξεργασίας που απαιτούν συγκατάθεση; 30. Εξασφαλίζεται ρητά η συγκατάθεση για την χρήση ευαίσθητων δεδομένων;

	31. Εκπληρώνονται οι απαιτήσεις συγκατάθεσης για τα δεδομένα των παιδιών που επεξεργάζεται ο οργανισμός; 32. Επιβεβαιώνεται η ηλικία ενός παιδιού και η ταυτότητα γονέως κηδεμόνα, όπως απαιτείται από τις αρμόδιες ρυθμιστικές αρχές;
5. Μηχανισμός επικοινωνίας με το υποκείμενο δεδομένων	33. Έχει ο οργανισμός έναν δημοσιευμένο και εύκολα προσπελάσιμο τρόπο για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα να επικοινωνούν με τον οργανισμό σχετικά με θέματα ιδιωτικότητας; 34. Υπάρχει ηλεκτρονική φόρμα ή μια πύλη που επιτρέπει στα άτομα να επικοινωνούν με συγκεκριμένα αιτήματα απορρήτου, όπως διαγραφή και αντιρρήσεις; 35. Υπάρχει η δυνατότητα επικύρωσης της ηλικίας και της ταυτότητας των προσώπων στα οποία αναφέρονται τα δεδομένα ή άλλων που κάνουν ερωτήσεις σχετικά με τα δεδομένα προσωπικού χαρακτήρα των υποκειμένων δεδομένων; 36. Υπάρχει το κατάλληλο ενημερωμένο προσωπικό που να μπορεί να ανταποκριθεί σε αιτήματα ; 37. Έχουν οριστεί καθορισμένοι χρόνοι απόκρισης στους αιτούντες; 38. Υπάρχει η δυνατότητα αυτόματης απάντησης και εξυπηρέτησης αιτημάτων για υποκείμενα και τους τοπικούς ρυθμιστές;
6. Διαγραφή προσωπικών δεδομένων	39. Έχει δημιουργηθεί μηχανισμός για τον εντοπισμό και τη διαγραφή δεδομένων προσωπικού χαρακτήρα, κατόπιν αιτήματος; 40. Υπάρχει προσωπικό που είναι εκπαιδευμένο για τον εντοπισμό και τη διαγραφή των προσωπικών δεδομένων; 41. Υπάρχει διαδικασία που έχει καθιερωθεί για την πλήρη διαγραφή δεδομένων; 42. Υπάρχει η δυνατότητα απόδειξης της οριστικής διαγραφής; 43. Υπάρχει η δυνατότητα εντοπισμού και επαφής πρόσθετων ελεγκτών ή παραληπτών προσωπικών δεδομένων για την ικανοποίηση αιτημάτων διαγραφής;
7. Παροχή στο υποκείμενο των δεδομένων του σε δομημένη μορφή	44. Έχει θεσπιστεί μηχανισμός που παρέχει στα πρόσωπα στα οποία αναφέρονται τα δεδομένα αντίγραφο των προσωπικών τους δεδομένων, μεταξύ άλλων σε ηλεκτρονική μορφή; 45. Είναι σε μια κοινή, μηχανικά αναγνώσιμη μορφή; 46. Είναι σε μορφή που μπορεί να αποσταλεί σε άλλο ελεγκτή, όταν ζητηθεί από το υποκείμενο των δεδομένων;

8. Περιορισμός επεξεργασίας	47. Έχει θεσπιστεί διαδικασία και πολιτική για τον περιορισμό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όταν απαιτείται; 48. Υπάρχει η δυνατότητα να αναστέλλουν ή να περιοριστούν οι δραστηριότητες επεξεργασίας κατόπιν αιτήματος; 49. Υπάρχει η δυνατότητα να ενημερώνονται αυτόματα τα υποκείμενα των δεδομένων όταν οι δραστηριότητες επεξεργασίας επαναλαμβάνονται μετά από περιορισμό;
9. Εξέταση αυτόματης επεξεργασίας δεδομένων	50. Μπορεί ο οργανισμός να προσδιορίσει αποφάσεις (π.χ. ελέγχους πιστοληπτικής ικανότητας, ελέγχους ιστορικού) για τα υποκείμενα δεδομένων που εκτελούνται εν όλων ή εν μέρει με αυτοματοποιημένα μέσα; 51. Αξιολογούνται οι πράξεις αυτές από το νομικό προσωπικό και το προσωπικό συμμόρφωσης; 52. Υπάρχει καθορισμένη διαδικασία για την ανθρώπινη παρέμβαση για αυτοματοποιημένες αποφάσεις που είναι επιρρεπείς σε ασυνέπεια;
10. Υπεύθυνος προστασίας δεδομένων (DPO)	53. Υπάρχει κάποιος διορισμένος ως υπεύθυνος προστασίας δεδομένων (DPO); 54. Διεξάγεται εκπαίδευση σε θέματα προστασίας της ιδιωτικής ζωής σε τακτά καθορισμένα χρονικά διαστήματα για όλο το προσωπικό; 55. Πραγματοποιείτε ανεξάρτητη εξέταση και εποπτεία των δραστηριοτήτων προστασίας προσωπικών δεδομένων; 56. Είναι ενήμερος για τις κανονιστικές απαιτήσεις και διατηρεί γνώσεις περί ζητημάτων ιδιωτικότητας;
11. Διαχείριση επιχειρηματικών κινδύνων	57. Διατηρεί ο οργανισμός πρόγραμμα διαχείρισης κινδύνου που περιλαμβάνει εκτιμήσεις για το απόρρητο δεδομένων; 58. Διατηρείτε αρχές και κατευθυντήριες γραμμές για την αντιμετώπιση του κινδύνου σε ολόκληρο τον οργανισμό; 59. Υπάρχει ένα καθορισμένο πλαίσιο για την αξιολόγηση και τη διαχείριση απειλών σε ολόκληρο τον οργανισμό; 60. Γίνονται εκτιμήσεις (οικονομικές, φήμες ή με άλλο τρόπο) για τους κινδύνους κακοδιαχείρισης προσωπικών δεδομένων;

Πίνακας 5

2. Προστασία δεδομένων

Υποκατηγορία	**Ερώτηση**
1. Προστασία δεδομένων και προστασία της ιδιωτικής ζωής από τον σχεδιασμό και την αρχή (by design and by default)	61. Σχεδιάζει ο οργανισμός πώς να αναπτύξει την τεχνολογία, τα προϊόντα, τις διαδικασίες και την οργανωτική δομή του με την προστασία δεδομένων και την ιδιωτική ζωή ως βασικά συστατικά στοιχεία και γνωρίζει τα κενά για να το πράξει; 62. Υπάρχει η δυνατότητα ψευδονυμοποίησης προσωπικών δεδομένων; 63. Υπάρχει διαδικασία για να καθορίσετε πόσα προσωπικά δεδομένα είναι απαραίτητα για την εκτέλεση των λειτουργιών του οργανισμού ή των παρεχόμενων υπηρεσιών, προϊόντων; 64. Υπάρχουν ολοκληρωμένες αρχές προστασίας δεδομένων και προστασίας της ιδιωτικής ζωής στο πλαίσιο του τρέχοντος κύκλου ζωής του λογισμικού και της τεχνολογίας;
2. Κρυπτογράφηση προσωπικών δεδομένων	65. Είναι ο οργανισμός ενήμερος για τις τεχνολογίες κρυπτογράφησης προσωπικών δεδομένων και έχει κρυπτογραφήσει ορισμένα προσωπικά δεδομένα, όπως κυβερνητικούς αριθμούς αναγνώρισης, ημερομηνίες γέννησης ή τραπεζικούς αριθμούς; 66. Έχει διατηρηθεί ένα πρότυπο προστασίας δεδομένων που να τεκμηριώνει τα κριτήρια κρυπτογράφησης; 67. Υπάρχουν οι κατάλληλες τεχνολογίες για την κρυπτογράφηση; 68. Γίνεται ανασκόπηση των τεχνολογιών κρυπτογράφησης καθώς και των ισχυρών αλγορίθμων που χρησιμοποιούνται;
3. Εξασφάλιση προσωπικών δεδομένων με βάση ελέγχους ασφαλείας που διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα	69. Υπάρχει διαρκείς προσπάθεια του οργανισμού για να εντοπίσει τους απαραίτητους ανθρώπους, διαδικασίες και τεχνολογικούς ελέγχους για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (CIA) προσωπικών δεδομένων; 70. Υπάρχουν επίσημα καθορισμένες απαιτήσεις προστασίας της CIA για τα προσωπικά δεδομένα που ελέγχει; 71. Υπάρχει πρόγραμμα ή επίσημη διαδικασία βελτίωσης των συνολικών μέτρων προστασιών της CIA μέσω τακτικών επενδύσεων σε εμπειρογνώμονες, τεχνολογία και βέλτιστες πρακτικές ασφαλείας;

	72. Έχει εφαρμοστεί εσωτερικός έλεγχος της τεχνολογίας ή της διαδικασίας για τη χρήση των προσωπικών δεδομένων μόνο στους εξουσιοδοτημένος; 73. Υπάρχει σχέδιο εφαρμογής διαδικασιών για την έγκαιρη αποκατάσταση της διαθεσιμότητας προσωπικών δεδομένων σε περίπτωση που δεν είναι διαθέσιμη λόγω περιστατικών όπως επιθέσεις στον κυβερνοχώρο, φυσικές καταστροφές, διακοπή ρεύματος ή τεχνικές προκλήσεις; 74. Έχουν εφαρμοστεί κατάλληλες διασφαλίσεις για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα στα διεθνή σύνορα και σε διεθνείς οργανισμούς, όπως η τήρηση των προτύπων που δημοσιεύονται από κυβερνητικούς οργανισμούς της Ευρωπαϊκής Ένωσης (ή των εθνικών); 75. Έχει γίνει η εφαρμογή κατάλληλων μέτρων για τη διατήρηση της εμπιστευτικότητας των προσωπικών δεδομένων, πέραν της κρυπτογράφησης, όπως οι άδειες αρχείων, οι λίστες ελέγχου πρόσβασης και η φυσική ασφάλιση υπολογιστών και εξοπλισμού δικτύου; 76. Έχουν εφαρμοστεί τα κατάλληλα μέτρα για τη διατήρηση της ακεραιότητας των προσωπικών δεδομένων, όπως ο κατακερματισμός, η δημιουργία αντιγράφων ασφαλείας και η επικύρωση των δεδομένων;
4. Προετοιμασία και ανίχνευση παραβιάσεων δεδομένων	77. Είναι ενήμερος ο οργανισμός για τις πιθανές επιπτώσεις από παραβιάσεις δεδομένων προσωπικού χαρακτήρα και έχει ένα σχέδιο αντιμετώπισης; 78. Ο οργανισμός ενημερώνει τα απαιτούμενα μέρη για παραβιάσεις δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των υποκειμένων των δεδομένων και των εποπτικών αρχών (εντός 72 ωρών για τις εποπτικές αρχές), όταν υπάρχει υψηλός κίνδυνος επίδρασης στα υποκείμενα των δεδομένων; 79. Υπάρχει μια διαδικασία ή τεχνολογία για την ανίχνευση παραβιάσεων δεδομένων; 80. Διατηρείται λεπτομερή αρχεία σχετικά με τις παραβιάσεις δεδομένων, συμπεριλαμβανομένης της προέλευσης, των επιπτώσεων και των διορθωτικών μέτρων; 81. Διατηρείται μετρήσεις για τον εντοπισμό, την αποκατάσταση και την αναφορά περιπτώσεων παραβίασης προσωπικών δεδομένων, όπως η επιχειρησιακή επίπτωση και η αποτελεσματικότητα της αποκατάστασης;

Πίνακας 6

4. Αναφορές δεδομένων	
Υποκατηγορία	**Ερώτηση**
1. Διατήρηση αρχείου για απόδειξη συμμόρφωσης	82. Διατηρεί ο οργανισμός αρχεία δραστηριοτήτων επεξεργασίας με ορισμένες πρόσθετες πληροφορίες σχετικά με το σκοπό ή το πεδίο των δραστηριοτήτων; 83. Διατηρούνται αρχεία με τις απαιτούμενες κατηγορικές πληροφορίες σχετικά με τα προσωπικά δεδομένα, όπως η αιτιολόγηση για τη χρήση, οι βασικές οργανωτικές επαφές και οι τύποι δεδομένων που χρησιμοποιούνται; 84. Έχουν εφαρμοστεί σωστά καθορισμένες διαδικασίες για την καταγραφή των απαιτούμενων πληροφοριών; 85. Διαθέτει ο οργανισμός τεχνολογία για την καταγραφή των απαιτούμενων πληροφοριών;
2. Καταγραφή και ροές δεδομένων	86. Διαθέτει ο οργανισμός τεκμηρίωση των συνεχών μεταφορών δεδομένων προσωπικού χαρακτήρα προς και από την ΕΕ; 87. Διατηρείτε αρχείο όλων των δραστηριοτήτων επεξεργασίας που αφορούν τη μεταφορά προσωπικών δεδομένων εντός και εκτός της ΕΕ, συμπεριλαμβανομένων των μητρώων ad-hoc μεταφορών που δεν αποτελούν μέρος μιας τρέχουσας διαδικασίας; 88. Έχουν οριστεί διαδικασίες για την παρακολούθηση και καταγραφή γεωγραφικών μεταφορών δεδομένων προσωπικού χαρακτήρα;
3. Χρήση αξιολόγησης των επιπτώσεων στην προστασία δεδομένων	89. Μπορεί ο οργανισμός να καθορίσει τους κινδύνους που σχετίζονται με την επεξεργασία προσωπικών δεδομένων; 90. Αξιολογείτε το επίπεδο και τα είδη κινδύνων που σχετίζονται με τις αλλαγές στην επεξεργασία των προσωπικών δεδομένων, καθώς και τον τρόπο μείωσης των κινδύνων; 91. Εκτελείτε αξιολογήσεις αντικτύπου προστασίας δεδομένων (DPIA), όποτε εντοπίζονται δραστηριότητες επεξεργασίας υψηλού κινδύνου; 92. Αναφέρετε τα αποτελέσματα της DPIA στους ρυθμιστές και τους εξωτερικούς φορείς, κατά περίπτωση; 93. Χρησιμοποιείται την DPIA για να ενημερώσετε τις ευρύτερες δραστηριότητες διαχείρισης κινδύνου του οργανισμού;

Πίνακας 7

Το σύνολο των παραπάνω ερωτήσεων, πέραν από τις απαντήσεις που σημειώνονται μπορούν να περιλαμβάνουν και αιτιολογικά σχόλια που εξηγούν την απάντηση του συνεντευξιαζόμενου. Με αυτό τον τρόπο καλύπτεται η ανάλυση αποκλίσεων σε σχέση με την συμμόρφωση στον GDPR. Οι απαντήσεις μπορούν να βαθμολογηθούν και να έχουν βάρος με το οποίο να τροφοδοτείται ένα μοντέλο απεικόνισης του βαθμού ετοιμότητας της επιχείρησης σε σχέση με τις υποχρεώσεις της που απορρέουν από το GDPR. Στην μελέτη περίπτωσης που θα παρουσιαστεί στο επόμενο κεφάλαιο θα γίνει η παρουσίαση του μοντέλου, το οποίο βασίζεται στις ερωτήσεις της μεθοδολογίας.

Κεφάλαιο 5. Μελέτη Περίπτωσης

5.1 Εισαγωγή – Περιγραφή μελέτης περίπτωσης

Οι πάροχοι υγειονομικής περίθαλψης πρέπει να διασφαλίζουν ότι συμμορφώνονται με τις απαιτήσεις των δημόσιων αρχών και είναι σε θέση να αποδείξουν ότι προστατεύουν επαρκώς τις πληροφορίες των ασθενών τους ή των πελατών τους. Οποιοδήποτε νοσοκομείο ή άλλος οργανισμός υγειονομικής περίθαλψης πρέπει επίσης να επαληθεύει την ταυτότητα των ασθενών του και να δημιουργεί ένα ακριβές σύστημα που επιτρέπει τη διαγραφή ή τη διόρθωση των δεδομένων τους. Το ίδιο ισχύει και για τους παρόχους υπηρεσιών υγείας που δραστηριοποιούνται όχι στην πρωτοβάθμια αντιμετώπιση περιστατικών υγείας, αλλά έρχονται επικουρικά να καλύψουν την ανάγκη της πρόληψης, της ενημέρωσης και της παροχής στοχευμένων υπηρεσιών υγείας είτε σε χρόνια πάσχοντες είτε σε ηλικιακές ομάδες ανθρώπων που πραγματικά έχουν ανάγκη, όπως οι ηλικιωμένοι. Οι στενευμένες υπηρεσίες υγείας που δρουν συμπληρωματικά με της βασικές υπηρεσίες υγείας και αντιμετώπισης περιστατικών, όπως για παράδειγμα κλινικές, δημόσια – ιδιωτικά νοσοκομεία, ιατρικά κέντρα, πλέον έχουν δημιουργήσει νέου τύπου προϊόντα και υπηρεσίες οι οποίες παρέχονται μέσω διαδικτυακών πυλών και έξυπνων εφαρμογών, δίνοντας την δυνατότητα στους πελάτες τους να κάνουν χρήση αυτών χωρίς φυσική παρουσία σε κάποιο ιατρικό ή κέντρο νοσηλείας. Οι νέες αυτές υπηρεσίες που παρέχονται πλέον στοχεύουν τόσο στην καλύτερη πρόγνωση περιστατικών υγείας του ασθενή όσο και στη έγκυρη παρακολούθηση της υγείας του, μέσω της συλλογής των ιατρικών δεδομένων του. Οι τρείς συνήθης τύποι δεδομένων που συλλέγονται και επεξεργάζονται από τους παρόχους είναι:

1. Γενετικά δεδομένα: περιλαμβάνονται στο άρθρο 9 του GDPR: "Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα". Η αιτιολόγηση 13 την ορίζει ως "προσωπικά δεδομένα σχετικά με τα κληρονομικά ή αποκτηθέντα γενετικά χαρακτηριστικά ενός φυσικού προσώπου που παρέχουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία αυτού του φυσικού προσώπου και οι οποίες προκύπτουν, ιδίως, από ανάλυση ενός βιολογικού δείγματος εν λόγω φυσικό πρόσωπο ".
2. Βιομετρικά δεδομένα: χρησιμοποιούνται για τη "μοναδική αναγνώριση φυσικού προσώπου", περιλαμβάνονται επίσης στο άρθρο 9 του κανονισμού. Η αιτιολόγηση 14 την ορίζει ως "προσωπικά δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία που σχετίζεται με τα φυσικά, φυσιολογικά ή συμπεριφορικά

χαρακτηριστικά ενός φυσικού προσώπου, τα οποία επιτρέπουν ή επιβεβαιώνουν τη μοναδική αναγνώριση αυτού του φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα".

3. Δεδομένα σχετικά με την υγεία: περιλαμβάνονται επίσης στο άρθρο 9 ορίζονται στην αιτιολόγηση 15 ως "προσωπικά δεδομένα σχετικά με τη φυσική ή ψυχική υγεία ενός φυσικού προσώπου, συμπεριλαμβανομένης της παροχής υπηρεσιών υγειονομικής περίθαλψης, τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του".

Η νεοσύστατη εταιρεία Ahealth Α.Ε. απευθύνεται σε ηλικιωμένους και χρόνιους ασθενείς. Με την επέλαση του Internet of Things σε κάθε έκφανση της ανθρώπινης δραστηριότητας, ο τομέας της Ηλεκτρονικής Υγείας είναι το πιο χρήσιμο κεφάλαιο στο βιβλίο του IoT. Μόνο με μια σύνδεση στο Internet, η εφαρμογή που έχουν αναπτύξει εξοικονομεί χρόνο και χρήμα, παρέχοντάς τη δυνατότητα να διατηρείτε παντού και πάντα επαφή με τους οικείους και με τον θεράποντα ιατρό του ασθενή.

1. **Ανεξάρτητη διαβίωσή**: Στόχος είναι η βελτίωση της ποιότητας ζωής των ηλικιωμένων, συνδυάζοντας τεχνολογίες που διασφαλίζουν την ανεξάρτητη διαβίωσή τους:
    - Καινοτόμες υπηρεσίες επικοινωνίας
    - Παρακολούθηση της τήρησης της φαρμακευτικής αγωγής
    - Εποπτεία και καθημερινή υποστήριξη
    - Διαχείριση καταστάσεων έκτακτης ανάγκης
2. **Ιατρική Παρακολούθηση:** Αξιοποιώντας καινοτόμες τεχνολογίες για την αντιμετώπιση των αναγκών των χρόνιων ασθενών, χρησιμοποιούνται έξυπνες συσκευές κι αισθητήρες μη επεμβατικής φύσεως, ώστε να αναπτυχθούν συστήματα για:
    - Παρακολούθηση της φυσικής και συναισθηματικής τους κατάστασης
    - Ανίχνευση και διαχείριση δυνητικά επικίνδυνων καταστάσεων
    - Κοινωνική δικτύωση και ενθάρρυνση δραστηριοτήτων αυτοφροντίδας
    - Μοντελοποίηση της συμπεριφοράς με στόχο τη βελτίωση της αυτοδιαχείρισης
3. **Ηλεκτρονικό Ιατρικό Ιστορικό** : Η ολοκληρωμένη υπηρεσία Ηλεκτρονικού Ιατρικού Ιστορικού παρέχει στους ιατρούς πλήρη πληροφόρηση για την κατάσταση και το ιστορικό των ασθενών τους, βελτιώνοντας την ικανότητά τους να προβαίνουν σε έγκαιρες εμπεριστατωμένες αποφάσεις για την εξατομικευμένη θεραπεία και φαρμακευτική αγωγή των ασθενών.

Η πλατφόρμα ενσωματώνει καθιερωμένα πρότυπα, προκειμένου να παράσχει αποτελεσματική ενοποίηση των δεδομένων και διαλειτουργικότητα με εξωτερικούς παρόχους υγειονομικής περίθαλψης, υπηρεσίες και συσκευές.

4. **Καταγραφή Φυσικής Δραστηριότητας και Ανίχνευση Πτώσεων** : έχει σχεδιαστεί και υλοποιήθει ένα διακριτικό σύστημα, βασισμένο σε wearable συσκευές. Το σύστημά συλλαμβάνει κι αναλύει δεδομένα κίνησης και συμπεριφοράς για την αναγνώριση δραστηριότητας του κάθε χρήστη. Με αυτό τον τρόπο, η καθημερινή σωματική δραστηριότητα του χρήστη αξιολογείται σύμφωνα με το προσωπικό του προφίλ, με στόχο το σύστημά μας:
    - Να παρέχει στον ιατρό του πολύτιμα δεδομένα
    - Να τον ενθαρρύνει να προβαίνει σε φυσική δραστηριότητα ανάλογα με τις ανάγκες του
    - Να ενισχύει την ευεξία του
    - Να εντοπίζει αυτόματα τυχόν πτώσεις, ώστε να ενεργοποιηθεί άμεσα η υπηρεσία έκτακτης ανάγκης

5.2 Πλάνο συμμόρφωσης

Στην παρούσα μελέτη περίπτωσης ακολουθήθηκαν μεθοδολογικές προσεγγίσεις και βέλτιστες πρακτικές που ακολουθούνται από αντίστοιχες προσεγγίσεις, που αφορούν έργα προστασίας δεδομένων και ασφάλειας πληροφοριακών συστημάτων ώστε τα βήματα που θα ακολουθήσουν για την συμμόρφωση να είναι σε σωστές βάσεις. Το πλάνο δεν περιλαμβάνει την πλήρη συμμόρφωση με τον κανονισμό, αλλά είναι τα βασικά βήματα που θα πρέπει να έχει κάνει η Ahealth A.E ώστε να μπορέσει να τα περιλάβει στο γενικότερο πλαίσιο συμμόρφωσης της με τον κανονισμό. Είναι πολύ σημαντικό να αναφερθεί πως η μελέτη της εν λόγω περίπτωσης έγινε σε διάστημα τριών μηνών και σκοπό πέρα από την ανάπτυξη των μεθοδολογιών, που έχουν καταγραφεί, ήταν και η γενικότερη γνωριμία με την εταιρεία καθώς και η υπόδειξη τεχνικών λύσεων σε οργανωτικά θέματα ασφάλειας πληροφοριών και ορθότερης ανάπτυξης των υπηρεσιών, με γνώμονα τις επερχόμενες αλλαγές του GDPR. Η δημιουργία ενός πλάνου στο οποίο κινήθηκε η εν λόγω μελέτη, ήταν πολύ σημαντική ώστε στο μικρό χρονικό διάστημα να ολοκληρωθούν τα βασικά σημεία :

1. Γνωριμία με την εταιρεία και τα προϊόντα της
2. Εκπόνηση προγράμματος ενημέρωσης για τον GDPR
3. Ανάλυση οργανωτικής δομής
4. Δημιουργία ομάδας έργου

5. Μελέτη υφιστάμενης κατάστασης στον τομέα ανάπτυξης και ασφάλειας πληροφοριών σε υφιστάμενα προϊόντα
6. Ανάλυση τεχνολογιών που χρησιμοποιούνται για την ανάπτυξη εφαρμογών
7. Αξιολόγηση και επανασχεδιασμός υφιστάμενης πολιτικής ασφαλείας
8. Παρουσίαση μοντέλου για την καταγραφή δεδομένων που χρησιμοποιεί η βασική εφαρμογή- προϊόν της Ahealth A.E.
9. Υλοποίηση καταγραφής δεδομένων με βάση την αναπτυχθείσα μεθοδολογία
10. Παρουσίαση μεθοδολογίας για την εκτέλεση DPIA
11. Δημιουργία πλάνου για την αξιολόγηση υφιστάμενων συμβολαίων συνεργασίας και privacy notices
12. Παρουσίαση καλών πρακτικών για την επίτευξη privacy by default και privacy by design
13. Εκπόνηση ανάλυση αποκλίσεων σε σχέση με τον GDPR (GAP analysis) και μοντελοποίηση των αποτελεσμάτων τα οποία παρουσιάζονται με γραφικό κατανοητό τρόπο.

Αυτά είναι τα βασικά σημεία που εκπονήθηκαν κατά την διάρκεια του έργου με την βοήθεια της ομάδας εργασίας, που σχηματίστηκε από εργαζόμενους της Ahealth A.E. Για την παρούσα εργασία θα παρουσιαστούν μόνο τα αποτελέσματα που αφορούν την μεθοδολογική προσέγγιση που έχει γίνει στο Κεφάλαιο 4 και αφορά την :

- Καταγραφή – ροή δεδομένων (Data inventorying-flow)
- Ανάλυση αποκλίσεων (GAP Analysis)

Τα υπόλοιπα βασικά σημεία του έργου που ολοκληρώθηκαν δεν μπορούν να περιέλθουν στον σκοπό της εν λόγω εργασίας, καθώς αποτελούν εμπιστευτικά δεδομένα της επιχείρησης και για τον λόγω αυτό δεν μπορούν να δημοσιευτούν. Όμως, θα πρέπει να τονίσουμε πως αποτελούν βασικά βήματα εκπόνησης του έργου και δίχως αυτά δεν θα μπορούσαμε να δημιουργήσουμε την μεθοδολογική προσέγγιση που έχει ήδη περιγράφει, όπως επίσης και η επιχείρηση δεν θα είναι σε θέση να προχωρήσει το έργο συμμόρφωσης.

5.2.1 Ahealth - Καταγραφή – ροή δεδομένων

Η καταγραφή των δεδομένων που συλλέγει, επεξεργάζεται και μεταδίδει η Ahealth για την δημιουργία προϊόντων και υπηρεσιών, παρουσιάζονται στον ακόλουθο πίνακα. Με βάση την μεθοδολογία των 5Ws όπως έχει ήδη αναπτυχθεί στο Κεφάλαιο 4, τα πεδία και οι πληροφορίες που συμπληρωθήκαν από την ομάδα εργασίας, οργανώθηκαν με τρόπο τέτοιο ώστε να εκπληρώνουν τις απαιτήσεις της μεθοδολογίας.

Who	What					Where				Why		When		
Data Subject	Data Asset	Personal Data Category	PII Classification	Collected by	Legal Basis	Data transfer Mechanism	Source	Storage of Data	Deletion Policy	Collection Purpose	Type of Processing	Collection Method	Updated	Retention Policy

Πίνακας 8

Who	*Data Subject*	Ποιο είναι το υποκείμενο των δεδομένων;
What	*Data Asset*	Ονομασία δεδομένου
	Personal Data Category	Κατηγορία προσωπικού δεδομένου
	PII Classification	Προσδιορισμός κατηγορίας προσωπικών δεδομένων ταυτοποίησης ταυτότητας
	Collected by	Από ποιον συλλέχθηκαν τα δεδομένα;
	Legal Basis	Υπάρχει νομική βάση συλλογής;
Where	*Data transfer Mechanism*	Πως μεταφέρονται τα δεδομένα κατά τη συλλογή;
	Source	Ποια η πηγή των δεδομένων ;
	Storage of Data	Που συγκεντρώνονται τα δεδομένα;
	Deletion Policy	Πότε διαγράφονται;

Why	*Collection Purpose*	Ποιος ο σκοπός της συλλογής;
	Type of Processing	Ποιος ο τύπος της επεξεργασίας;
When	*Collection Method*	Με ποιον τρόπο συλλέγονται;
	Updated	Κάθε πότε γίνονται αλλαγές;
	Retention Policy	Πόσο χρόνο διατηρούνται;

Πίνακας 9

Παρουσίαση ενδεικτικών αποτελεσμάτων :

Who	**What**					**Where**			**Why**			**When**		
Data Subject	Data Asset	Personal Data Category	PII Classification	Collected by	Legal Basis	Data transfer Mechanism	Source	Storage of Data	Deletion Policy	Collection Purpose	Type of Processing	Collection Method	Updated	Retention Policy
Client	**Email**	User Identifiers	Possibly Identifiable	Platform or Mobile Application	Consent of individual	HTTPS Requests	User Generated	Cloud Provider (IaaS)	None	*Used as username for sign in*	Simple search	Manually Input	No	None
	Name	User Identifiers	Identifiable		Consent of individual	HTTPS Requests			None	*Display on platform*	Simple search	Manually Input	As required	None
	Address	Contact Information	Identifiable		Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search	Manually Input	As required	None
	Telephone	Contact Information	Possibly Identifiable		Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search	Manually Input	As required	None
	Mobile Phone	Contact Information	Possibly Identifiable		Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search	Manually Input	As required	None
	VAT Number	User Identifiers	Sensitive		Consent of individual	HTTPS Requests			None	*For invoicing purposes*	Simple search	Manually Input	No	None
	Profile picture	File (Photos, Videos, Music, Notes)	Sensitive		Consent of individual	HTTPS Requests			None	*Display on platfom*	Simple search	Manually Input	As required	None
	Photos	File (Photos, Videos, Music, Notes)	Sensitive		Consent of individual	HTTPS Requests			None	*Social engagement with family/friends*	Simple search	Manually Input	Regularly	None
	Logins	Log Files	Not Identifiable	Mobile Application	Consent of individual	HTTPS Requests	System Generated		None	*Used for system logging and monitoring*	Simple search	System Input	Regularly	None
Contact	**Address**	Contact Information	Identifiable	Platform or Mobile Application	Consent of individual	HTTPS Requests	User Generated	Cloud Provider (IaaS)	None	*Communication with other users*	Simple search	Manually Input	As required	None
	Telephone	Contact Information	Possibly Identifiable		Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search	Manually Input	As required	None
	Mobile	Contact Information	Possibly Identifiable		Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search	Manually Input	As required	None
	Gender	Racial Data	Not Identifiable		Consent of individual	HTTPS Requests			None	*Customized user salutation, title, pronouns, etc.*	Simple search	Manually Input	As required	None
	Date of birth	User Identifiers	Sensitive		Consent of individual	HTTPS Requests			None	*Display age to user's doctor*	Simple search	Manually Input	No	None

	Profile picture	File (Photos, Videos, Music, Notes)	Sensitive		Consent of individual	HTTPS Requests			None	*Display on system*	Simple search	Manually Input	As required	None
	Logins	Log Files	Not Identifiable	Mobile Application	Consent of individual	HTTPS Requests	System Generated		None	*Used for system logging and monitoring*	Simple search	System Input	Regularly	None
Patient	**Email**	User Identifiers	Possibly Identifiable	Platform or Mobile Application	Consent of individual	HTTPS Requests	User Generated	Mobile Application Storage	None	*Used as username for sign in*	Simple search	Manual input	No	None
	Name	User Identifiers	Identifiable		Consent of individual	HTTPS Requests			None	*Display on platform*	Simple search	Manual input	As required	None
	Address	Contact Information	Identifiable		Consent of individual	HTTPS Requests		Cloud Provider (IaaS)	None	*Communication with other users*	Simple search	Manual input	As required	None
	Telephone	Contact Information	Possibly Identifiable		Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search	Manual input	As required	None
	Mobile	Contact Information	Possibly Identifiable		Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search	Manual input	As required	None
	Gender	Racial Data	Not Identifiable		Consent of individual	HTTPS Requests			None	*Customized user salutation, title, pronouns, etc.*	Simple search	Manual input	As required	None
	Date of birth	User Identifiers	Sensitive		Consent of individual	HTTPS Requests			None	*Display age to user's doctor*	Simple search	Manual input	No	None
	Height	Biometric Data	Sensitive		Consent of individual	HTTPS Requests			None	*Display age to user's doctor*	Simple search	Manual input	No	None
	Weight	Biometric Data	Sensitive		Consent of individual	HTTPS Requests			None	*Display age to user's doctor*	Simple search	Manual input	As required	None
	Social Security ID	User Identifiers	Sensitive		Consent of individual	HTTPS Requests			None	*Retrieve patient's lab test results from healthcare provider*	Simple search	Manual input	No	None
	Profile picture	File (Photos, Videos, Music, Notes)	Sensitive		Consent of individual	HTTPS Requests			None	*Display on system*	Simple search	Manual input	As required	None
	Contact list (user, date created, created by, relation type)	Account Information	Identifiable	Platform	Consent of individual	HTTPS Requests			None	*Used for collobaration*	Simple search	Manual input	Regularly	None
	Conditions (date start, date end, comments, doctor, category)	Health Data	Sensitive	Platform	Consent of individual	HTTPS Requests			None	*Store in patient's personal health record for historic overview*	Simple search	Manual input	Regularly	None
	Allergies (date start, date end, doctor, comments, type)	Health Data	Sensitive	Platform	Consent of individual	HTTPS Requests			None	*Store in patient's personal health record for historic overview*	Simple search	Manual input	Regularly	None

	Medications (drug name, type, description, start date, end date, comments, dosage schedule, doctor)	Health Data	Sensitive	Platform or Mobile Application	Consent of individual	HTTPS Requests			None	*Store in patient's personal health record for historic overview*	Simple search	Manual input	Regularly	None
	Lab test results (category, exam name, value, unit, date)	Health Data	Sensitive	Platform	Consent of individual	HTTPS Requests			None	*Store in patient's personal health record for historic overview*	Simple search	Automatic	Regularly	None
	Doctor's notes	Health Data	Sensitive	Platform	Consent of individual	HTTPS Requests			None	*Store in patient's personal health record for historic overview*	Simple search	Manual input	As required	None
	Biosignal measurements (category, value, date)	Biometric Data	Sensitive	Mobile Application	Consent of individual	Bluetooth transfer			None	*Store in patient's personal health record for historic overview*	Analytics	Manual input	Regularly	None
	Logins (start, end, device info)	Log Files	Not Identifiable	Mobile Application	Consent of individual	HTTPS Requests	System Generated		None	*System monitoring*	System logging	Manual input	Regularly	None
	Biosignal measurements (category, value, unit, date sensed, date uploaded, user, device info)	Biometric Data	Sensitive	Mobile Application	Consent of individual	HTTPS Requests			None	*Store in patient's personal health record for historic overview*	Analytics	Sensors	Regularly	None
	Videoconference logs	Log Files	Sensitive	Platform	Consent of individual	HTTPS Requests			None	*System monitoring*	Simple search	Automatic	Regularly	None
	Lab test results (category, exam name, body site, value, unit, date, range)	Health Data	Sensitive	Platform	Consent of individual	HTTPS Requests	3rd Party		None	*Store in patient's personal health record for historic overview*	Simple search	Manual input	Regularly	None
Physician(Doctor,Pharmacist)	**Email**	Contact Information	Possibly Identifiable	Manual input	Consent of individual	HTTPS Requests	User Generated	Cloud Provider (IaaS)	None	*Communication with users*	Simple search	Manual input	No	None
	Name	User Identifiers	Possibly Identifiable	Manual input	Consent of individual	HTTPS Requests			None	*Display on platform*	Simple search		As required	None
	Address (Street, No, City, Zip, State)	Contact Information	Identifiable	Manual input	Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search		As required	None
	Telephone	Contact Information	Possibly Identifiable	Manual input	Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search		As required	None
	Mobile	Contact Information	Possibly Identifiable	Manual input	Consent of individual	HTTPS Requests			None	*Communication with other users*	Simple search		As required	None
	VAT number	User Identifiers	Sensitive	Manual input	Consent of individual	HTTPS Requests			None	*Authentication of profession (for doctors)*	Simple search		No	None
	Profile picture	File (Photos, Videos, Music, Notes)	Sensitive	Manual input	Consent of individual	HTTPS Requests			None	*Display on system*	Simple search		Regularly	None

	Doctor list (user, date started, date ended)	Account Information	Sensitive	Manual input	Consent of individual	HTTPS Requests			None	*Display on system*	Simple search		Regularly	None
	Specialty	User Identifiers	Not Identifiable	Manual input	Consent of individual	HTTPS Requests			None	*Display on system and inform other subjects about the Physician speciality*	Simple search		No	None
	Logins (start, end, device info)	Log Files	Not Identifiable	System logging	Consent of individual	HTTPS Requests	System Generated			*System monitoring*	Simple search		Regularly	None

Πίνακας 10

5.2.2 Ahealth - Ανάλυση αποκλίσεων (GAP Analysis)

Με βάση το ερωτηματολόγιο και την μεθοδολογία που έχει αναπτυχθεί για την ανάλυση αποκλίσεων ακολουθούν οι απαντήσεις της ομάδας εργασίας, για λόγους κατανόησης της ορολογίας το ερωτηματολόγιο είναι γραμμένο στην Αγγλική γλώσσα.

Customer:	Ahealth A.E.	
ID	Question	Answer
Discover		
D.1: Search for and identify personal data		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership Related GDPR Reference(s): Article 15(3)	
D1.0	Can the organization generally identify all locations where personal data is stored across the enterprise, including on internal servers or cloud storage, as well as those hosted by any third-party providers?	Yes
	Does the organization have:	
D1.1	The ability to locate all instances of personal data pertaining to a given data subject?	Yes
D1.2	A formal process in place to search for personal data in a consistent and timely manner?	No
D1.3	Technology in place for personnel to use a single search to return all instances of personal data for a given data subject?	Yes
D.2: Facilitate data classification		

	Recommended Responder: Data Protection Officer (DPO), Processor Related GDPR Reference(s): Article 30(2)(b-d); 32(2)	
D2.0	Can the organization categorize the types of personal data it uses?	Yes
	Does the organization:	
D2.1	Label different categories of data in varying degrees of sensitivity, such as "sensitive," "confidential," or "public"?	Yes
D2.2	Label data with the geographic restrictions that may apply?	No
D2.3	Label the origin of data, i.e. whether data was provided by the data subject or obtained through other means?	No
D2.4	Perform data classification activities in a consistent and timely manner?	No
D2.5	Automatically perform all of the above activities?	No
D.3: Maintain an inventory of personal data holdings		
	Recommended Responder: Data Center Leadership, Data Protection Officer (DPO), Marketing/Digital, Processor Related GDPR Reference(s): Article 30(1-3)	
D3.0	Does the organization have a tool to catalog how and where personal data is used, and is it partially or fully populated?	Yes
	Does the organization have:	
D3.1	A complete inventory of how and where personal data is used with all instances documented?	Yes

D3.2	Technology in place to automate or partially automate updates to the inventory?	No
D3.3	A process that is used regularly to keep the inventory up to date?	No
D3.4	An inventory of all processing activities where personal data is being obtained?	Yes
D3.5	Documented details of each processing activity including scope, purpose, and criteria for when notifications and consent are required?	No
Manage		
M.1: Enable data governance practices and processes		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), HR, Legal Related GDPR Reference(s): Article 5(2); 6(1); 8(2); 9(1); (2)(b-h); 10(1); 12(1); 24(2)	
M1.0	Does the organization have a data governance program?	No
	Does the data governance program include:	
M1.1	An organizational structure and formal charter for carrying out the program in a consistent manner?	No
M1.2	Integration across departments to ensure data governance is consistent and effective organization-wide?	No
M1.3	Data privacy and protection policies?	No
M1.4	Technology to protect against, monitor, and report on privacy and protection policy violations?	No
M1.5	Specific protections for children's personal data?	No
M1.6	Policies that enforce accountability within the organization?	No

M1.7	Legal justification documented for using special categories of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)?	No
M.2: Provide detailed notice of processing activities to data subjects		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), HR, Legal Related GDPR Reference(s): Article 7(2); 12(1); 13(1-3); 14(1-4)	
M2.0	Does the organization provide data subjects with privacy notices that describe how their data is used?	Yes
	Are the privacy notices:	
M2.1	Written in clear and plain language?	No
M2.2	Governed by a formal policy and process to ensure they are shared in a timely, consistent, and appropriate manner?	Yes
M2.3	Inclusive of required information, such as organization contact details and purposes for using personal data?	N/A
M2.4	Shared with data subjects at first point of contact, when informing them they may object to how the organization uses their personal data?	No
M2.5	Generated and shared by automated means?	No
M2.6	Shared with data subjects at all points where personal data is collected?	No
M2.7	Shared with data subjects when personal data is collected from a source other than the data subjects, including online profiles, sites, or other interactions not directly between the data subject and the organization?	No

M2.8	Shared with data subjects, before the organization uses their personal data for new purposes not already communicated to them?	N/A
M.3: Discontinue processing on request		
	Recommended Responder: Data Center Leadership, Data Protection Officer (DPO), Marketing/Digital, Processor Related GDPR Reference(s): Article 7(3); 21(1-4); 30(4)	
M3.0	When requested by a data subject, can the organization discontinue processing some forms of personal data?	No
	Can the organization:	
M3.1	Discontinue processing all forms of a data subject's personal data (particularly direct marketing) when requested by the data subject and deemed appropriate by the organization?	No
M3.2	Provide data subjects with notice and justification for the continued use of their personal data, when a request to discontinue use is rejected?	No
M3.3	Record and maintain evidence of discontinued personal data use?	No
M3.4	Use an established process to consistently and promptly respond to requests from data subjects to stop using their data?	No
M3.5	Automatically perform all of the above activities?	No
M.4: Collect unambiguous, granular consent from data subjects		
	Recommended Responder: Data Protection Officer (DPO), Legal Related GDPR Reference(s): Article 7(1), (4); 8(1); 9(1), (2)(a), (3); 12(6); 16(1); 17(3); 18(2-3)	
M4.0	Can the organization obtain consent from data subjects to process their personal data?	Yes
	Can the organization:	

M4.1	Obtain data subject consent, prior to using the data subject's personal data?	No
M4.2	Consistently and promptly obtain data subject consent for all processing activities that require consent?	No
M4.3	Explicitly obtain consent for use of personal sensitive data, such as racial or religious data?	No
M4.4	Automatically obtain all necessary consent from data subjects?	No
M4.5	Fulfill the requirements of consent for any children's data the organization processes?	N/A
M4.6	Validate the age of a child and the identity of a parental guardian, as required by relevant regulatory authorities?	Yes
M.5: Facilitate communication mechanism between data subject and organization to handle data subject requests		
	Recommended Responder: Data Protection Officer (DPO), IT Leadership Related GDPR Reference(s) Article 12(2-5); 15; 16; 17(1), (3); 18(1); 19; 20(1)	
M5.0	Does the organization have a published and easily accessible way for data subjects to communicate with the organization on privacy matters?	No
	Does the organization have:	
M5.1	An online form or portal that allows individuals to communicate specific privacy requests, such as erasure and objections?	No
M5.2	Backend tools and processes to track requests from data subjects through to resolution?	No
M5.3	The ability to validate the age and identity of data subjects or others making inquiries about data subject personal data?	No
M5.4	The appropriate personnel trained to respond to privacy requests from data subjects and others?	No
M5.5	The ability to communicate with recipients of personal data about changes, erasure, or use restrictions on the data, in a timely manner?	No

M5.6	A tracking system that data subjects and regulators can use to view the status of their privacy requests and inquiries?	No
M5.7	Defined response times made available to requestors?	No
M5.8	The ability to automatically respond to and service inquiries from data subjects and regulators?	No
M.6: Rectify inaccurate or incomplete personal data regarding data subjects		
	Recommended Responder: Data Center Leadership, Data Protection Officer (DPO), Processor Related GDPR Reference(s): Article 16; 30(4)	
M6.0	For some cases, can the organization correct inaccuracies or complete partial instances of data subject personal data when requested?	No
	Can the organization:	
M6.1	Correct inaccuracies or complete partial instances of all data subject personal data, when requested by the data subject?	No
M6.2	Record, maintain, and readily share evidence of correcting or completing personal data?	No
M6.3	Consistently and promptly correct and complete personal data, as well as record and maintain evidence of this action?	No
M6.4	In some cases, automatically correct and complete personal data, as well as record and maintain evidence of the correction or completion?	No
M6.5	In all cases, automatically correct and complete personal data, as well as record and maintain evidence of the correction or completion?	No
M.7: Erase personal data regarding a data subject		

	Recommended Responder: Data Center Leadership, Data Protection Officer (DPO), Marketing/Digital, Processor Related GDPR Reference(s): Article 17(1)(a-f), (2); 30(4)	
M7.0	Is a mechanism established to locate and erase personal data on request?	Yes
	To address an erasure request, is/are there:	
M7.1	Personnel in place who are trained on how to locate and erase personal data?	No
M7.2	Personnel who can determine in what case a data erasure request should be fulfilled?	Yes
M7.3	A process established to erase data completely and accurately?	No
M7.4	The ability to create and retain a record that an erasure request was fulfilled?	No
M7.5	The ability to locate and contact additional controllers or recipients of personal data to fulfill erasure requests?	No
M7.6	A technology which provides the capability to erase data that resides in multiple data stores?	Yes
M7.7	The ability to automatically perform requested data erasure completely and accurately, when deemed appropriate?	No
M.8: Provide data subject with their personal data in a common, structured format		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO) Related GDPR Reference(s): Article 20(1)(a-b); 20(2)	
M8.0	Is a mechanism established to provide data subjects a copy of their personal data, including in an electronic format?	No
	Is this data provided:	
M8.1	In a common, machine readable format, such as an .xls or .xml file?	No
M8.2	Automatically to the data subject in an appropriate format?	No
M8.3	In a format that can be sent to another controller, when requested by the data subject?	No

M.9: Restrict the processing of personal data		
	Recommended Responder: Data Center Leadership, Data Protection Officer (DPO), Marketing/Digital, Processor Related GDPR Reference(s): Article 18(1)(a-d); 30(4)	
M9.0	Have a procedure and policy been established to restrict processing of personal data, when required?	No
	For that personal data, does the organization:	
M9.1	Have the ability to suspend or restrict processing activities on request?	No
M9.2	Have procedures to notify additional recipients or processors to restrict processing?	No
M9.3	Automatically notify recipients of processing activity restrictions?	No
M9.4	Have a process and technology to notify data subjects if a restriction of processing has been lifted?	No
M9.5	Automatically notify applicable data subjects when processing activities have been resumed after restriction?	No
M9.6	Maintain a record of instances when processing activities were restricted?	No
M9.7	Maintain a record of instances where processing activities were restricted and then resumed, including the explanation?	No
M.10: Review data processing conducted by automated means		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership Related GDPR Reference(s): Article 22(1-4)	
M10.0	Can the organization identify decisions (e.g. credit checks, background checks) for data subjects that are performed completely or partially by automated means?	N/A
	For decisions made via automated processing:	

M10.1	Are the automated decisions evaluated by legal and compliance personnel to establish proper business justification and rationale?	N/A
M10.2	Is there a policy in place to identify when human intervention is necessary to review automated decisions?	N/A
M10.3	Is there a defined procedure for human intervention for automated decisions that are prone to inconsistency?	N/A
M10.4	Is there a defined process to allow data subjects to explain, challenge, or express a point of view on a decision?	N/A
M.11: Appoint a Data Protection Officer (DPO)		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), HR, Legal Related GDPR Reference(s): Article 24(1); 26(1-2); 27(1)(3-4); 35(2); 37(1-7); 38(1-6); 39(1)(a-d)	
M11.0	Is there a person appointed as the Data Protection Officer (DPO)?	No
	Does the Data Protection Officer:	
M11.1	Conduct privacy training at regular, defined intervals for all relevant personnel?	No
M11.2	Maintain regular communications with internal counterparts and external peers in his or her professional network responsible for data privacy?	No
M11.3	Perform independent review and oversight of data privacy activities?	No
M11.4	Stay up to date with regulatory requirements and maintain privacy expertise?	No
M11.5	Provide guidance on defining and maintaining roles and responsibilities of data privacy positions within the organization?	No
M11.6	Review all necessary compliance regulations for data privacy requirements, based on GDPR and other relevant regulations?	No

M.12: Define enterprise risk management strategy, inclusive of data privacy risks		
	Recommended Responder: Risk Management Office Related GDPR Reference(s): Article 24(1), 32(4)	
M12.0	Does the organization maintain a risk management program that includes considerations for data privacy?	No
	Does the risk management program:	
M12.1	Maintain principles and guidelines for addressing risk across the organization?	No
M12.2	Include a defined framework to assess and manage threats across the organization?	No
M12.3	Define mitigation or transfer strategies, as necessary?	No
M12.4	Prioritize risk to focus resources on protecting and securing the highest value business assets?	No
M12.5	Include considerations (whether financial, reputational, or otherwise) for risks of mishandling personal data?	No
Protect		
P.1: Data protection and privacy by design and default		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership, Operations Related GDPR Reference(s): Article 25(1-3)	
P1.0	Is the organization planning how to develop its technology, products, processes, and organizational structure with data protection and privacy as key components, and is it aware of the gaps for doing so?	No
	Has the organization:	
P1.1	Established the ability to pseudonymize personal data?	No

P1.2	Established a process to determine how much personal data is needed to perform the organization's operations?	Yes
P1.3	Established process/personnel access controls (such as segregation of duties), where available technology would be insufficient to adequately protect privacy?	No
P1.4	Established a policy/procedure to provide access to personal data using the principle of least privilege?	Yes
P1.5	Integrated data protection and privacy as key components of relevant policies and processes?	Yes
P1.6	Embedded data protection and privacy practices within the culture of the organization through ongoing training efforts and awareness programs?	Yes
P1.7	Integrated data protection and privacy tenets within its ongoing software and technology development lifecycle?	Yes
P.2: Secure personal data through encryption		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership Related GDPR Reference(s): Article 32(1)(a)	
P2.0	Is the organization aware of technologies to encrypt personal data and has it encrypted some personal data, such as government identification numbers, birthdates, or banking numbers?	Yes
	Does the organization:	
P2.1	Have a policy or procedure in place to define what personal data to encrypt, how to encrypt it, and the purpose of encryption?	No
P2.2	Maintain a data protection standard that documents encryption criteria?	No
P2.3	Have appropriate technologies in place to perform encryption?	No
P2.4	Regularly analyze new encryption technology and keep up to date with strong encryption?	No

P.3: Secure personal data by leveraging security controls that ensure the confidentiality, integrity, and availability of personal data		
	Recommended Responder: Chief Information Security Officer (CISO), Compliance, Data Protection Officer (DPO), IT Leadership Related GDPR Reference(s): Article 29; 32(1)(b-c); (2); 46(1), (2)(a-f), 3(a-b)	
P3.0	Does the organization have an ongoing effort to identify needed people, process, and technology controls to protect the confidentiality, integrity, and availability (CIA) of personal data?	No
	Has the organization:	
P3.1	Formally defined CIA protection requirements for the personal data it controls?	No
P3.2	Formally defined measures to meet its requirements for protecting the CIA of personal data?	No
P3.3	Established a program or formal process of enhancing its overall CIA protections via regular investment in expert personnel, technology, and security best practices?	No
P3.4	Implemented internal technology or process controls to use personal data only as authorized?	No
P3.5	Entered into external agreements with partners/service providers to use personal data only as authorized?	No
P3.6	Implemented technology and processes to enable it to restore personal data availability in a timely manner, in the event it becomes unavailable due to incidents such as cyber attack, natural disaster, power outage, or technical challenges?	No
P3.7	Implemented appropriate safeguards for personal data transfers across international boundaries and to international organizations, such as by following standards published by European Union (or national EU) government agencies?	No

P3.8	Implemented appropriate measures to maintain personal data confidentiality, apart from encryption, such as file permissions, access control lists, and physically securing computers and network equipment?	No
P3.9	Implemented appropriate measures to maintain personal data integrity, such as hashing, backups, and input validation?	No
P.4: Prepare for, detect, and respond to data breaches		
	Recommended Responder: Chief Information Security Officer (CISO), Compliance, Data Protection Officer (DPO), IT Leadership, Legal Related GDPR Reference(s): Article 12(1); 33(1-5); 34(1-2)	
P4.0	Is the organization aware of the potential impacts from breaches of personal data and does it have a response plan in place?	No
	Does the organization:	
P4.1	Notify required parties of breaches of personal data, including data subjects and supervisory authorities (within 72 hours for supervisory authorities), when there is a high risk of impact to data subjects?	No
P4.2	Provide required data breach notices using clear and plain language, giving the breach's nature and impact, the appropriate contact person, and the organization's remedy for the breach?	No
P4.3	Have a process or technology to detect data breaches across all data stores in its control, including online, offline, and third party systems?	No
P4.4	Maintain detailed records of data breaches, including their origin, impacts, and remedies?	No
P4.5	Discuss, document, and apply lessons learned from data breaches?	No
P4.6	Regularly update its data breach response procedures and technology?	No

P4.7	Maintain metrics for how breaches of personal data are detected, remedied, and reported, such as operational impact and remediation efficiency?	No
P.5: Facilitate regular testing of security measures		
	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), IT Leadership Related GDPR Reference(s): Article 32(1)(d)	
P5.0	Does the organization perform testing of its security measures, whether through technical means, social engineering, or tabletop exercises?	Yes
	Does the organization:	
P5.1	Have a process in place to regularly test, assess, and evaluate its organizational and technical security measures?	Yes
P5.2	Have external partners or a managed service periodically test, assess, and evaluate its organizational and technical security measures?	Yes
P5.3	Have technology in place to regularly test, assess, and evaluate its organizational and technical security measures?	Yes
P5.4	Have appropriate personnel in place to perform testing?	Yes
Report		
R.1: Keep record to display GDPR compliance		
	Recommended Responder: Compliance, Data Protection Officer (DPO), Legal, Operations Related GDPR Reference(s): Article 9(4); 23(1-2); 24(3); 30(1-2); 35(4-5); 36(5); 40(3); 42(2), (6); 87; 88(1-2); 90(1)	
R1.0	Does the organization maintain records of processing activities with some additional information regarding the purpose or scope of the activities?	No

	Does the organization:	
R1.1	Maintain records with required categorical information about personal data, such as justification for use, key organizational contacts, and types of data used?	No
R1.2	Have appropriate personnel in place to support recording required categorical information about personal data?	No
R1.3	Have technology in place to record required information?	No
R1.4	Have well-defined processes in place to record required information?	No
R1.5	Have a process to stay up to date with relevant codes of conduct, standards, guidelines, data residency guidance, and binding corporate rules?	No
R1.6	Demonstrate its adherence to relevant codes of conduct, standards, guidelines, data residency requirements, and binding corporate rules?"	No
R.2: Track and record flows of personal data into and out of the EU		
	Recommended Responder: Compliance, Data Protection Officer (DPO), IT Leadership, Legal, Operations Related GDPR Reference(s): Article 45(1); 46(1-2)	
R2.0	Does the organization have documentation of ongoing personal data transfers into and out of the EU?	Yes
	Does the organization:	
R2.1	Maintain a record of all processing activities that involve personal data transfer into and out of the EU, including records of ad-hoc transfers that are not part of an ongoing process?	Yes
R2.2	Have a process to stay up to date with changing requirements for international transfers, including which countries or organizations ensure an adequate level of data protection as decided by the EU?	Yes

R2.3	Have appropriate personnel in place to support tracking and recording personal data transfers across international boundaries?	Yes
R2.4	Have technology in place to track and record geographical transfers of personal data, including documenting to which country the data was transferred and what safeguards were used?	Yes
R2.5	Have defined processes in place to track and record geographical transfers of personal data?	Yes
R.3: Track and record flows of personal data to third-party service providers		
	Recommended Responder: Compliance, Data Protection Officer (DPO), IT Leadership, Legal, Third-Party Processors, Related GDPR Reference(s): Article 13(1)(f); 14(1)(f); 28 (1-5), (9); 46(1)	
R3.0	Does the organization maintain an inventory of processes that transmit personal data to third-party service providers?	N/A
	Does the organization:	
R3.1	Assess potential third-party service providers for adherence to personal data requirements?	N/A
R3.2	Document which third-party service providers process personal data, and define personal data protection requirements for all applicable third-parties?	N/A
R3.3	Embed personal data protection requirements within contracts and agreements with third-party service providers?	N/A
R3.4	Establish procedures for auditing third-party providers' compliance with agreements and controls?	N/A
R3.5	Maintain ongoing communication with third-party service providers about personal data processing requirements?	N/A
R.4: Facilitate data protection impact assessment		

	Recommended Responder: Chief Information Security Officer (CISO), Data Protection Officer (DPO), Project Management Related GDPR Reference(s): Article 5(1); 6(4); 25(2); 32(2); 35(1), (3), (7-9), (11); 36(1) (3) ; 39(1)(b-c); 39(2)	
R4.0	Can the organization determine risks associated with personal data processing?	No
	Does the organization:	
R4.1	Assess the level and types of risk associated with changes to personal data processing, as well as how to mitigate the risks?	No
R4.2	Perform Data Protection Impact Assessments (DPIAs), whenever it identifies high-risk processing activities?	No
R4.3	Have a formal process and template in place to consistently perform these activities, including criteria for when DPIAs are required?	No
R4.4	Use technology to facilitate the DPIA and reviewing of assessment results?	No
R4.5	Engage external stakeholders (e.g., data subjects, privacy advocates) as part of the impact assessment process?	No
R4.6	Report DPIA results to regulators and external stakeholders, where appropriate?	No
R4.7	Use DPIAs to inform broader risk management activities?	No

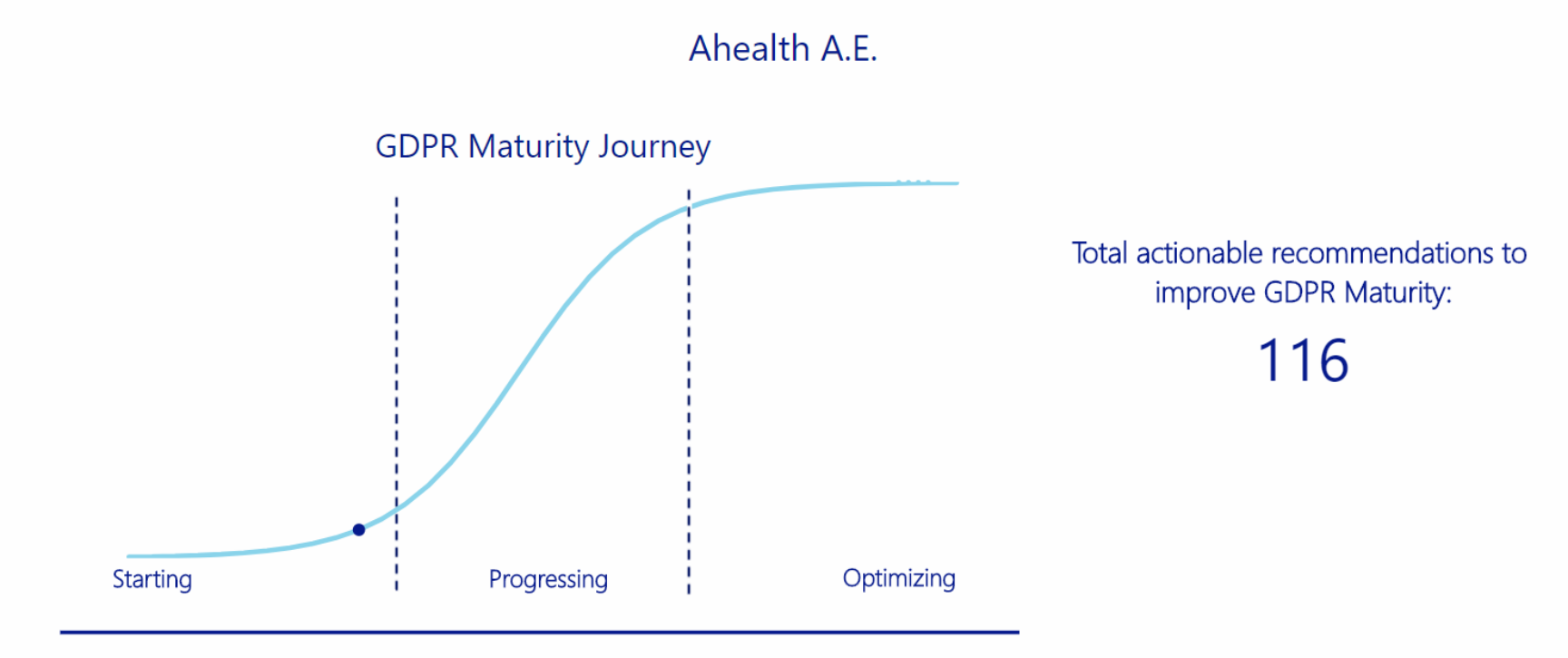
Πίνακας 11

Η βαθμολογία των απαντήσεων για κάθε κατηγορία ερωτήσεων, έχει ένα αριθμητικό βάρος ανάλογα με την απάντηση (Yes/No). Το μέγιστο σύνολο για κάθε κατηγορία είναι 10 το οποίο μετά το την ολοκλήρωση των υπο-ερωτήσεων διαμορφώνεται τελικώς από το πλήθος των απαντήσεων Yes/No, ώστε να δώσει το τελικό βαθμό ετοιμότητας και να αναδείξει τα κενά στο μοντέλο απεικόνισης της ετοιμότητας σε σχέσης με τον GDPR. Για την οργάνωση και συμπλήρωση των ερωτήσεων έχουν χρησιμοποιηθεί τα εργαλεία MS Excel 2016 και για τη απεικόνιση των αποτελεσμάτων το Microsoft Power BI . Η απεικόνιση των αποτελεσμάτων μέσω του εργαλείου Power BI μας έδωσε την δυνατότητα να απεικονίσουμε :

1. Το συνολικό επίπεδο ετοιμότητας – συμμόρφωσης σε σχέση με το GDPR (Maturity Level)
2. Τις ερωτήσεις ανά θεματική κατηγορία και το πλήθος των απαντήσεων “No” ανά κατηγορία ερωτήσεων
3. Τις ερωτήσεις και τα άρθρα του GDPR που αναφέρονται καθώς και να δείξουμε τον βαθμό συμμόρφωσης ανά άρθρο
4. Τις προτάσεις για βελτίωση με βάση τις απαντήσεις και τα υφιστάμενα άρθρα του κανονισμού.

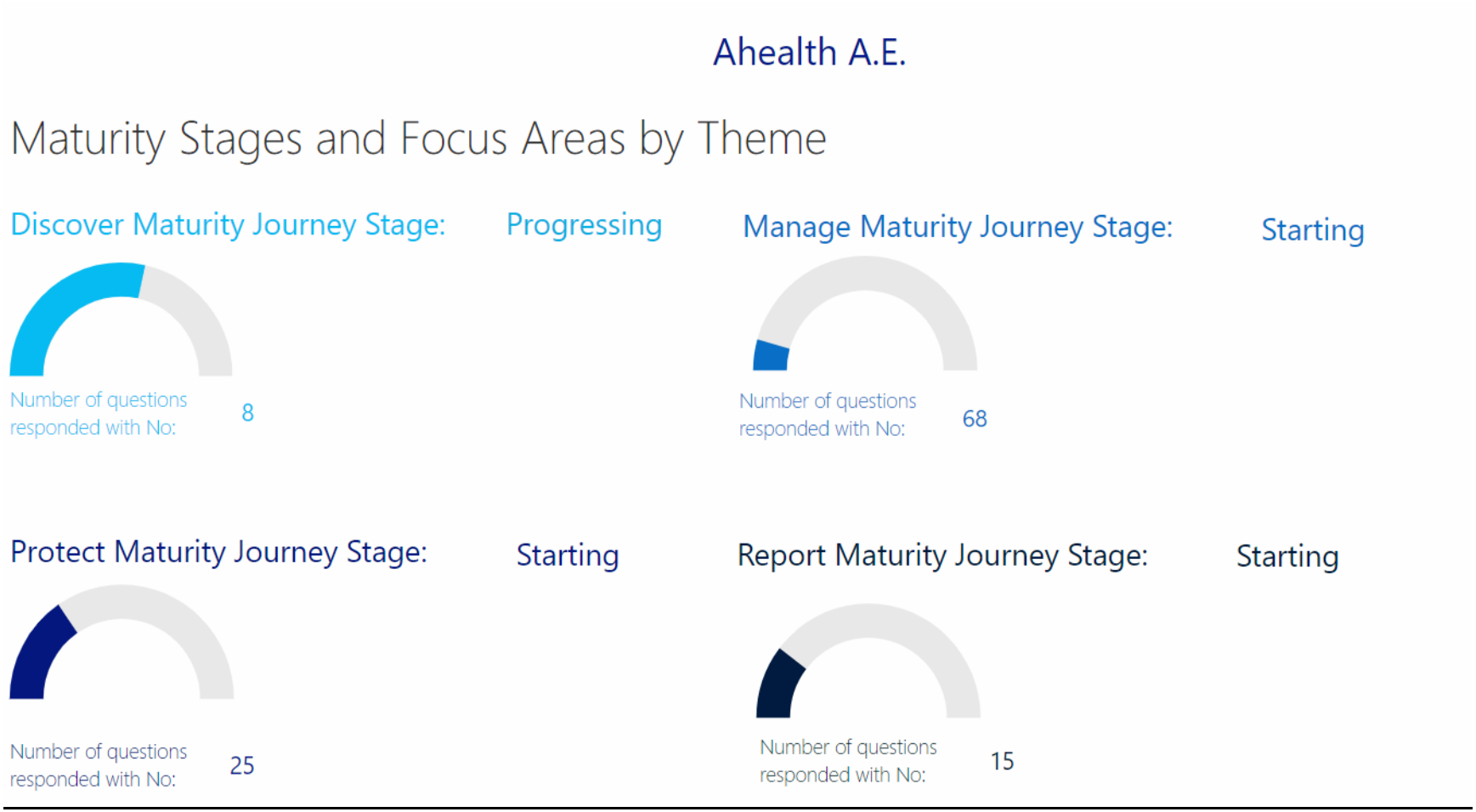
5.2.2.1 Παρουσίαση αποτελεσμάτων GAP Analysis

5.2.2.1.1 Επίπεδο Συμμόρφωσης



Σχήμα 1

5.2.2.1.2 Επίπεδο συμμόρφωσής ανα θεματική κατηγορία ερωτήσεων



Πίνακας 12

5.2.2.1.3 Αποτελέσματα κατηγορίας “Discovery” – Προτάσεις

Ahealth A.E.

Discover: D.1 Search for and identify personal data

Trace and identify personal data to facilitate classification, management, and protection of personal data. Identify personal data of specific data subjects to facilitate data subject rights requests.
Related GDPR Reference(s): Article 38(1-6)

Top Recommendation

Establish a formal process for how to search for and identify data subject personal data, including what tools to use, when to use them, and how to use them.

Πίνακας 13

Ahealth A.E.

Discover: D.2 Facilitate data classification

Classify data to assign and enforce data protection controls, comply with data subject rights requests, and more readily demonstrate compliance with the GDPR.
Related GDPR Reference(s): Article 30(2)(b-d); 32(2)

Maturity Journey Stage: Progressing

Top Recommendation

Establish and maintain a single source of documentation for how all personal data should be classified. Empower one or more organization members to oversee data classification and regularly ensure it is carried out correctly.

Πίνακας 14

Ahealth A.E.

Discover: D.3 Maintain an inventory of Personal data holdings

Identify all personal data holdings and and document each processing activity.
Related GDPR Reference(s): Article 30(1-3)

Maturity Journey Stage: **Progressing**

Top Recommendation

Establish a formalized process and process manager to assign responsibility and capability of maintaining inventory of personal data that is used by the organization.

Πίνακας 15

5.2.2.1.4 Αποτελέσματα κατηγορίας “Manage” – Προτάσεις

Ahealth A.E.

Manage: M.1 Enable data governance practices and processes

Establish policies, roles, and responsibilities for the access, management, and use of personal data.
Related GDPR Reference(s): Article 5(2); 6(1); 9(1), (2)(b-h), 10(1), 24(2)

Maturity Journey Stage: Starting

Top Recommendation

Create policies with specific restrictions and requirements that identify potential employment actions consistent with applicable employment law. Policies should be made available to all employees and acknowledged by employees.

Πίνακας 16

Ahealth A.E.

Manage: M.2 Provide detailed notice of processing activities to data subjects

Provide data subjects with specific and detailed information describing the collection and processing of data subject's personal data.

Related GDPR Reference(s): Article 7(2); 12(1); 13(1-3); 14(1-3)

Maturity Journey Stage: **Progressing**

Top Recommendation

Implement a process to validate data subjects are informed they may object to how the organization uses their personal data, when the organization first contacts them.

Πίνακας 17

Ahealth A.E.

Manage: M.3 Discontinue processing on request

Upon withdrawal of consent for processing by a data subject, discontinue the associated processing activity.
Related GDPR Reference(s): Article 7(3); 21(1-4); 30(4)

Maturity Journey Stage: **Starting**

Top Recommendation

Establish a process for when and how to respond to data subject requests to stop using their personal

Πίνακας 18

Ahealth A.E.

Manage: M.4 Collect unambiguous, granular consent from data subjects

Collect affirmative, granular consent from data subjects prior to engaging in processing activities.
Related GDPR Reference(s): Article 7(1); 8(1); 9(1), (2)(a), (3); 15(4); 16(1); 17(3); 18(2)-(3)

Maturity Journey Stage: **Progressing**

Top Recommendation

Establish a process to ensure data subject personal data is used only after data subjects consent to its use or appropriate legal justifications are in place.

Πίνακας 19

Ahealth A.E.

Manage: M.5 Facilitate requests for rectification, erasure, or transfer of personal data

Receive, track, and respond to data subjects' data subject rights requests (access, erasure, rectification, data portability).
Related GDPR Reference(s) Article 15; 16; 17(1), (3); 18(1); 19; 20(1)

Maturity Journey Stage: Starting

Top Recommendation

Establish a tool to communicate with data subjects on privacy matters, such as a phone number, email helpdesk, or website. This tool should be published and made available to data subjects.

Πίνακας 20

Ahealth A.E.

Manage: M.6 Rectify inaccurate or incomplete personal data regarding data subjects.

Rectify inaccurate or incomplete personal data upon request by data subject.
Related GDPR Reference(s): Article 16; 30(4)

Maturity Journey Stage: **Starting**

Top Recommendation

Develop a process to correct inaccurate personal data or fill in incomplete information. This could include modification to, or addition of, personal data details such as name or address. Implement technology where appropriate to enable this process.

Πίνακας 21

Ahealth A.E.

Manage: M.7 Erase personal data regarding a data subject

Erase personal data upon request by data subject.
Related GDPR Reference(s): Article 17(1)(a-f); 17(2); 30(4)

Maturity Journey Stage: **Progressing**

Top Recommendation

Establish a process to record, log, and maintain records of erasures.

Πίνακας 22

Ahealth A.E.

Manage: M.8 Provide data subject with their personal data in a common, structured format

Identify and export personal data in a commonly-used formats, machine-readable format upon request by data subject.
Related GDPR Reference(s): Article 20(1)(a-b); 20(2)

Maturity Journey Stage: Starting

Top Recommendation

Establish a process to securely transfer personal data to another controller in a machine-readable format, when requested by a data subject.

Πίνακας 23

Ahealth A.E.

Manage: M.9 Restrict the processing of personal data

Restrict processing activities, save for storage, for personal data upon request by data subject.
Related GDPR Reference(s): Article 18(1)(a-d); 30(4)

Maturity Journey Stage: **Starting**

Top Recommendation

Enable logging or maintain a record of when processing activities were restricted and then resumed. Capture an explanation from the individual who makes the decision to resume processing.

Πίνακας 24

Ahealth A.E.

Manage: M.10 Review data processing conducted by automated means

For data that is processed and is made via automated means, implement additional human intervention and considerations.
Related GDPR Reference(s): Article 22(1); 22(2)(a-c); 22(3); 22(4)

Top Recommendation
(Blank)

Πίνακας 25

Ahealth A.E.

Manage: M.11 Appoint a Data Protection Officer (DPO)

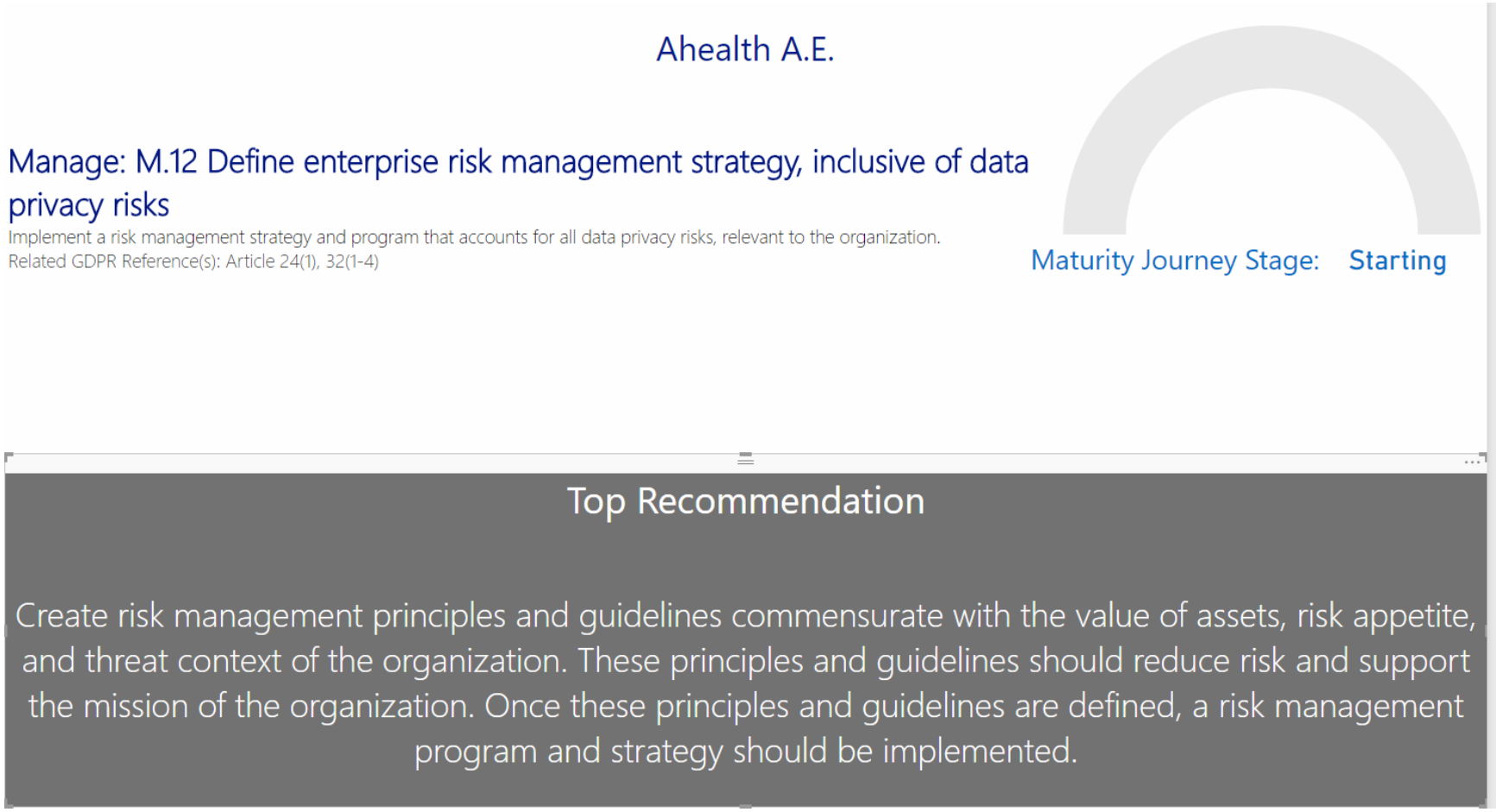
Appoint a Data Protection Officer (DPO), in an independent, oversight role.
Related GDPR Reference(s): Article 38(1-6)

Maturity Journey Stage: **Starting**

Top Recommendation

Determine relevant internal and external parties to communicate with as part of the DPO's role. Maintain a regular cadence of ongoing communications to understand the changing regulatory environment, industry standards, or operational needs related to data protection and privacy, and how industry peers are addressing them.

Πίνακας 26


Ahealth A.E.
Manage: M.12 Define enterprise risk management strategy, inclusive of data privacy risks
Implement a risk management strategy and program that accounts for all data privacy risks, relevant to the organization.
Related GDPR Reference(s): Article 24(1), 32(1-4)
Maturity Journey Stage: Starting
Top Recommendation
Create risk management principles and guidelines commensurate with the value of assets, risk appetite, and threat context of the organization. These principles and guidelines should reduce risk and support the mission of the organization. Once these principles and guidelines are defined, a risk management program and strategy should be implemented.

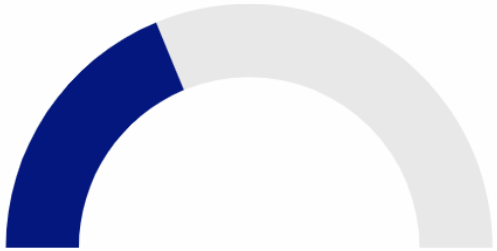
Πίνακας 27

5.2.2.1.5 Αποτελέσματα κατηγορίας “Protect” – Προτάσεις

Ahealth A.E.

Protect: P.1 Data protection by default

Implement technical and organizational measures that incorporate data privacy and protection principles to protect personal data.
Related GDPR Reference(s): Article 25(1-3)



Maturity Journey Stage: Starting

Top Recommendation

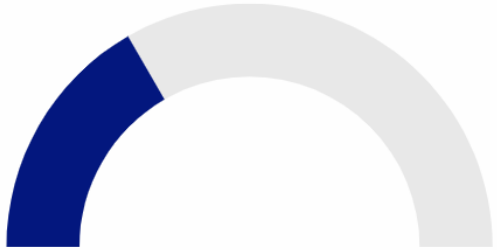
Design personal data access controls (such as segregation of duties) that prevent personnel from mishandling personal data. Continually review and update these access controls, as necessary, for all relevant data stores.

Πίνακας 28

Ahealth A.E.

Protect: P.2 Secure personal data through encryption

Utilize encryption where appropriate to protect personal data.
Related GDPR Reference(s): Article 32(1)(a)



Maturity Journey Stage: **Progressing**

Top Recommendation

Create encryption policies and procedures for relevant technologies, including what personal data to encrypt, how to encrypt it, and why to encrypt it. Regularly update these policies and procedures.

Πίνακας 29

Ahealth A.E.

Protect: P.3 Secure personal data by leveraging security controls that ensure the confidentiality, integrity, and availability of personal data

Implement adequate technical security measures to limit risk of unauthorized access, use, or disclosure of sensitive data.
Related GDPR Reference(s): Article 29; 32(1)(b-c); 32(2); 46(1); 46(2)(a-f); 46(3)(a-b)

Maturity Journey Stage: **Starting**

Top Recommendation

Create a formal program or process to regularly improve CIA protections by 1) hiring or realigning relevant expert personnel, 2) purchasing or developing new or upgrading in-place technology, and 3) researching or enabling personnel to learn current best practices.

Πίνακας 30

Ahealth A.E.

Protect: P.4 Detect and respond to data breaches

Defend against, detect, and respond to data breaches. In the event a breach incident, notify impacted data subjects and appropriate regulatory authorities.
Related GDPR Reference(s): Article 12(1); 33(1-5); 34(1-2)

Maturity Journey Stage: **Starting**

Top Recommendation

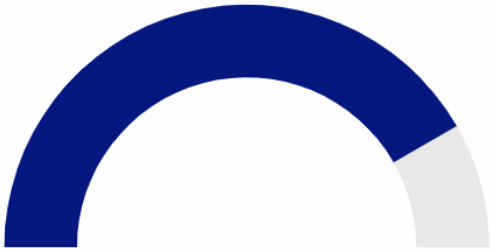
Create templates for data breach notifications and the guidelines for when to use each template. Write notices in clear and plain language and include information, such as breach nature and impact, contacts within the organization, and actions taken to remedy damages from the breach.

Πίνακας 31

Ahealth A.E.

Protect: P.5 Facilitate regular testing of security measures

Regularly test, assess, and evaluate the effectiveness of, technical and organizational measures for ensuring the security of personal data.
Related GDPR Reference(s): Article 32(1)(d)



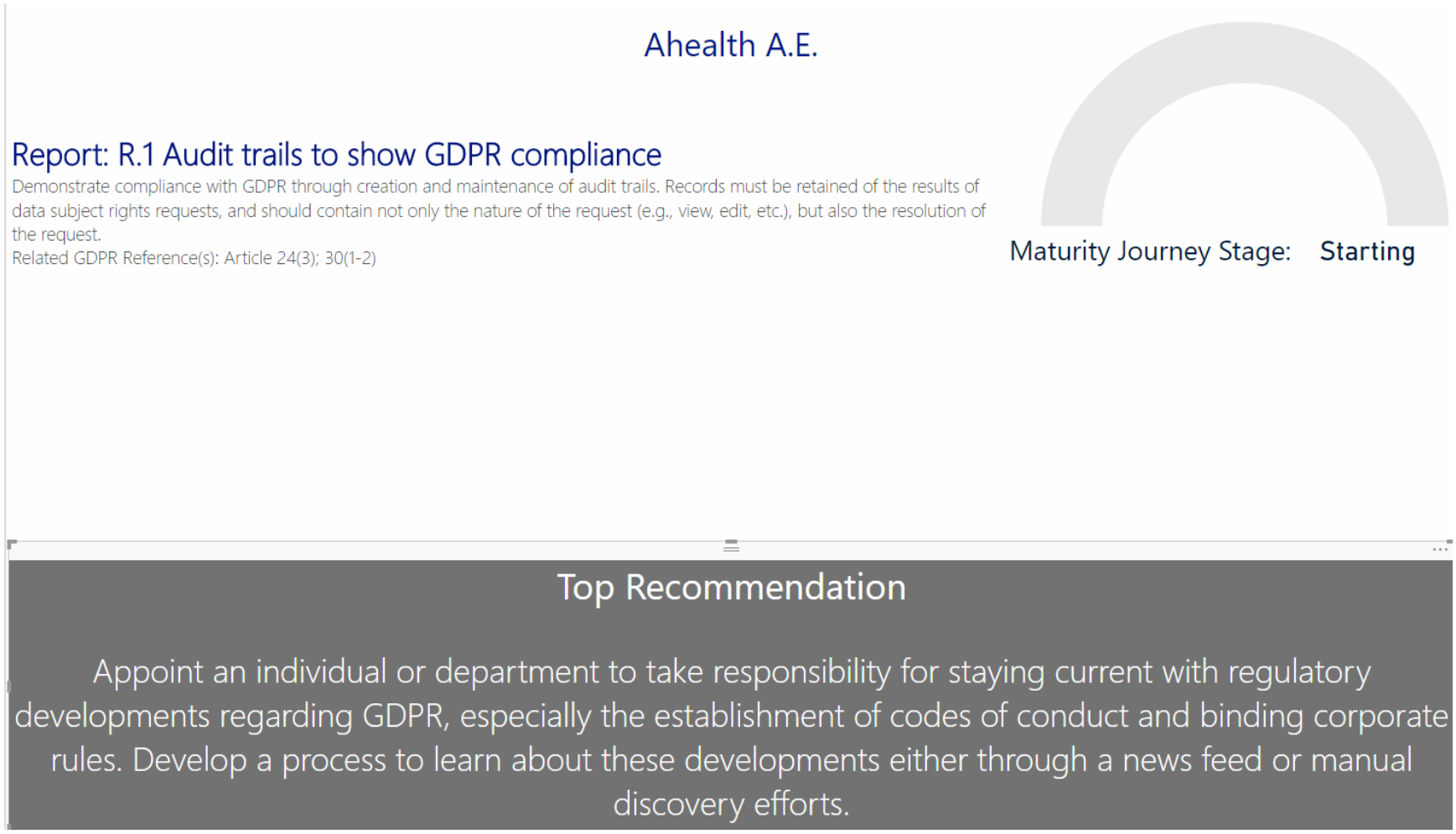
Maturity Journey Stage: **Optimizing**

Top Recommendation

(Blank)

Πίνακας 32

5.2.2.1.6 Αποτελέσματα κατηγορίας “Report” – Προτάσεις



Πίνακας 33

Ahealth A.E.

Report: R.2 Track and record flows of personal data into and out of the EU

Track and record geographic location of personal data.
Related GDPR Reference(s): Article 45(1); 46(1-2)

Maturity Journey Stage: **Optimizing**

Top Recommendation

(Blank)

Πίνακας 34

Ahealth A.E.

Report: R.3 Track and record flows of personal data to third-party service providers

Track and record flows of data to third-party service providers to trace personal data and facilitate data subject rights requests.
Related GDPR Reference(s): Article 13(1)(f); 14(1)(f); 46(1)

Top Recommendation

(Blank)

Πίνακας 35

Ahealth A.E.

Report: R.4 Facilitate data protection impact assessment

Conduct DPIAs for high-risk processing activities.

Related GDPR Reference(s): Article 5(1); 6(4); 24(1); 25(2); 32(2); 35(1); 35(7); 35(9); 35(11); 36(1); 39(1)(b-c); 39(2)

Maturity Journey Stage: **Not Applica...**

Top Recommendation

Define a formal template with frequency of use standards to continually maintain an up-to-date risk assessment and DPIA portfolio. Establish criteria for when a new assessment needs to be performed, such as when using new technologies for processing.

Πίνακας 36

Τα αποτελέσματα της ανάλυσης αποκλίσεων όπως εμφανίζονται από για μελέτη περίπτωσης της Ahealth, μπορούν να χρησιμοποιήθουν από την εταιρεία, ως σημείο αναφοράς για το πλάνο συμμορφωσης που θα εκπονηθεί για το GDPR. Η Ahealth μπορει να εξάγει χρήσιμα συμπεράσματα για το επίπεδο ετοιμότητας της, καθώς και να οργανώσει σωστά τα επόμενα βήματα της που θα την οδηγήσουν στο να παρέχει προιόντα και υπηρεσίες, έχοντας δώσει την σωστή βαρύτητα στην ασφάλεια και την προστασία των προσωπικών δεδομένων των πελατών της.

Κεφάλαιο 6. Επίλογος

6.1 Σύνοψη και συπεράσματα

Μέσω της παρούσας διπλωματικής εργασίας, έγινε προσπάθεια να αποτυπωθούν οι μεθοδολογίες καθώς και οι πρακτικές που ακολουθήθηκαν και εφαρμόσθηκαν στην περίπτωση νεοσύστατης εταιρείας καινοτομίας που δραστηριοποιείται στον κλάδο της ανάπτυξης εφαρμογών και ηλεκτρονικών υπηρεσιών υγείας, ώστε να προετοιμαστεί και να θέσει τις βάσεις που θα την φέρουν πιο κοντά στην συμμόρφωση με τον νέο γενικό κανονισμό για τη προστασία των δεδομένων (GDPR) της ΕΕ. Η ανάπτυξη συγκεκριμένων μεθοδολογιών για την σωστή πορεία της εταιρείας ή του οργανισμού προς την εκπλήρωση συμμόρφωσης με τον κανονισμό, αποτελεί ξεκάθαρο στόχο ο οποίος για να εκπληρωθεί θα πρέπει να βασιστεί σε μεθοδολογίες και πρακτικές που σχεδιάστηκαν, δημιουργηθηκαν και εφαρμόστηκαν με βάση τα άρθρα του Γενικού Κανονισμου για τα Δεδομένα και όπως αυτά ερμηνεύονται στο σύνολο του κανονισμού. Για αυτό το σκοπό η παρούσα εργασία περιέγραψε και παρουσίασε α) Μεθοδολογία καταγραφής και αποτύπωσης δεδομένων (Data Inventorying) η οποία αποτελεί βασικό και πρωτεύον σημείο εκκίνησης για την κατανόηση σχετικά με τον τύπο και την χρησιμότητα των δεδομένων που συλλέγει η εν λόγω εταιρεία και χρησιμοποιεί για την δημιουργία ηλεκτρονικών υπηρεσιών, β) Μεθοδολογία εκτίμησης των επιπτώσεων σχετικά με την προστασία των δεδομένων (DPIA), γ) ανάλυση αποκλίσεων (GAP Analysis) σύμφωνα με την οποία η εταιρεία μπορεί να αξιολογήσει το βαθμό εκπλήρωσης των προ απαιτούμενων όπως αυτά ορίζονται από τον κανονισμό.

Η εταιρεία AHealth A.E. έκανε αποτελεσματική χρήση των μεθοδολογιών και των πρακτικών που περιέγραψε η παρούσα διπλωματική εργασία, και πλεον είναι σε θέση να προχωρήσει στα επόμενα βήματα συμμορφωσης με τον κανονισμό, καθώς και να επαναπροσδιορίσει τις μεθόδους και τις τεχνικές που χρησιμοποει για την προστασία και ασφάλεια προσωπικών δεδομένων που διαχειρίζεται. Η παρούσα εργασία έχει εκπληρώσει τον στόχο της στο μεγαλύτερο ποσοστό και θα μπορούσε να χρησιμοποιηθεί ως βάση για την δημιουργία νέων μοντέλων εκτίμησης επιπτώσεων και γραφικής απεικόνισης τους.

Κεφάλαιο 7. Βιβλιογραφία

1. *"How to build GDPR and HIPAA compliant health apps"*, eBook published October 2017 from www.chino.io
2. *"Health data and data privacy challenges for data proessors under the GDPR"*, webarticle from www.taylorwessin.com
3. *"GDPR TeachPrivacy awareness*", http://www.techprivacy.com
4. "*Προστασία Προσωπικών Δεδομένων Σε Έξυπνα Περιβάλλοντα*" -Λιουδάκης, Γ. (2008). Διδακτορική διατριβή.
5. "*Θεσμικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Ανάκτηση 9 21, 2017*" από Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORTAL
6. "*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46*". Official Journal of the European Union (OJ), 59, σσ. 1-88.
7. Article "*Τεχνικά Μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR): Κρυπτογράφηση και Ψευδωνυμοποίηση*", Νικόλαος Η. Λουκάς – Περιοδικό Συνήγορος
8. "*Guide to the General Data Protection Regulation*" – Bird&Bird eBook January 2017
9. "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*" – NIST Special Publication 800-122, Recommendations of the National Institute of Standards and Technology
10. "*Getting ready for GDPR*" - Isle of Man Information Commissioner – GDPR Toolkit Part 1
11. "*Data Flow Mapping and the EU GDPR*" - www.itgovernance.co.uk
12. "*La sécurité des données personnelles*" - Les guides de la CNIL - édition 2017
13. "*Information and Guidance Notes General Data Protection Regulation (GDPR) Article 30 - Data Inventory/Data Mapping*" – Charities Institute Ireland
14. "*Data Mapping under the GDPR and Beyond*" - Baker & McKenzie LLP
15. "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether*

processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" – Article 29 data protection working party WP 248 rev.01

16. "*PRIVACY IMPACT ASSESSMENT (PIA) Methodology (how to carry out a PIA)"* – CNIL June 2015 Edition
17. "*Risk Assessment & Data Protection Impact Assessment Guide*" - Bitkom e. V. Federal Association for Information Technology
18. Article "*Η υποχρέωση διενέργειας εκτίμησης αντικτύπου (Data protection impact assessment - DPIA) στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)*" - Δημήτρης Γ. Ζωγραφόπουλος - Περιοδικό Συνήγορος
19. "*Part 2: how to do a privacy impact assessment (pia)*"
20. "*Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης*" - Κωνσταντίνος Σιασιάκος, Σοφία Αναστασίου, Κανέλλος Τούντας
21. "*Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems*" - Smart Grid Task Force 2012-14