Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Αλγοριθμική Εκτίμηση Επιπτώσεων Στο Πλαίσιο Του GDPR: Μελέτη Περίπτωσης Σε Δημόσιο Φορέα

Νικόλαος Γ. Μανωλάκας

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Μάιος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Αλγοριθμική Εκτίμηση Επιπτώσεων Στο Πλαίσιο Του GDPR: Μελέτη Περίπτωσης Σε Δημόσιο Φορέα

Νικόλαος Γ. Μανωλάκας

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2023

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η παρούσα διπλωματική διατριβή διερευνά εάν η αλγοριθμική εκτίμηση επιπτώσεων μπορεί να αποτελέσει ένα επιπλέον εργαλείο, στην προστασία των πολιτών των οποίων τα προσωπικά και ευαίσθητα προσωπικά τους δεδομένα υφίστανται επεξεργασία με την χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων και/ή δημιουργίας προφίλ, και εάν μπορεί να υπάρξει ένα ενιαίο μεθοδολογικό πλαίσιο ελέγχου μεταξύ αυτής και του GDPR, σε τέτοιου είδους επεξεργασίες για έναν καλύτερο έλεγχο.

Για τα παραπάνω υπάρχει μελέτη περίπτωσης σε δημόσιο φορέα που σχεδιάζει να χρησιμοποιήσει αυτοματοποιημένο εργαλείο λήψης αποφάσεων (Υποθετικό Σενάριο) και εκπονούνται 3 εκτιμήσεις επιπτώσεων και συγκεκριμένα:

- Εκπόνηση διαχείρισης κινδύνων ασφαλείας με βάση τον οδηγό του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας ENISA
- Εκτίμηση επιπτώσεων με την χρήση της AIA, κάνοντας χρήση εργαλείο της Καναδικής Κυβέρνησης
- Και εκπόνηση DPIA, με την χρήση του του εργαλείου PIA που παρέχεται από την CNIL

Summary

This thesis explores whether algorithmic impact assessment can be an additional tool, in the protection of citizens whose personal and sensitive personal data are processed using automated decision-making and/or profiling tools, and whether there can be a single methodological control framework, in such treatments.

For the above there is a case study in a public body that plans to use an automated decision-making tool (Hypothetical Scenario) and 3 impact assessments are prepared, namely:

- Elaboration of security risk management based on the guide of the European Agency for Cybersecurity ENISA
- Impact assessment using the AIA, using a Canadian Government tool
- And DPIA preparation, using the PIA tool provided by the CNIL

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς όλους όσους βοήθησαν στην εκπόνηση αυτής της μεταπτυχιακής διατριβής και ειδικά:

Τον επιβλέποντα καθηγητή μου κ. Κωνσταντίνο Λιμνιώτη, που με καθοδήγησε άψογα και ήταν δίπλα μου όποτε τον χρειάστηκα.

Τους συναδέλφους μου, που μοιράστηκαν μαζί μου τις γνώσεις και τις απόψεις τους.

Τους φίλους και την οικογένειά μου, που με στήριξαν και με ενθάρρυναν σε αυτήν την προσπάθεια και ειδικά τον συμφοιτητή μου Μιχάλη Τροκκούδη.

Εξαιρετικά αφιερωμένο στην κόρη μου Σοφία!

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Οι έννοιες της τεχνητής νοημοσύνης (Artificial Intelligence – AI) και της μηχανικής μάθησης (Machine Learning – ML), είναι πλέον άρρηκτα συνδεδεμένες με την καθημερινότητά μας, είτε υπάρχει η γνώση το τι είναι είτε όχι.

Συγκεκριμένα, η AI καθιστά της μηχανές ικανές να μαθαίνουν από την εμπειρία, να προσαρμόζονται σε νέα δεδομένα και να εκτελούν ανθρωπομορφικά έργα. Τα περισσότερα παραδείγματα AI που υπάρχουν σήμερα έχουν να κάνουν με υπολογιστές, και συγκεκριμένα από υπολογιστές που παίζουν παιχνίδια μέχρι και σε αυτοκίνητα αυτό-οδηγούμενα.

Με την χρήση της συγκεκριμένης τεχνολογίας, οι υπολογιστές μπορούν να εκπαιδευτούν ώστε να επεξεργάζονται έναν τεράστιο όγκο δεδομένων-πληροφοριών, αλλά και να αναγνωρίζουν μοτίβα στα δεδομένα αυτά.

Άλλα παραδείγματα AI, η Siri**[30]**, Alexa**[31]** και Cortana**[32]** και βέβαια άξιο αναφοράς το ChatGPT**[33]**.

Από την άλλη πλευρά, η ML είναι ένα παρακλάδι της τεχνητής νοημοσύνης, που έχει να κάνει με το ότι οι υπολογιστές/μηχανές μπορούν να μαθαίνουν από τα δεδομένα που συλλέγουν με σκοπό να αναγνωρίζουν μοτίβα και να παίρνουν δικές τους αποφάσεις, και όλα αυτά με ελάχιστη ή και μηδενική ανθρώπινη παρέμβαση.

Με λίγα λόγια, οι μηχανικοί αλγόριθμοι εκπαιδεύονται μέσω καταστάσεων και παραδειγμάτων, όπου μαθαίνουν και αναλύουν δεδομένα με σκοπό να κάνουν προβλέψεις για το μέλλον.

Ως αποτέλεσμα των δύο τεχνολογιών στις οποίες έγινε αναφορά, έχουμε τα λεγόμενα εργαλεία Automated Individual Decision-Making And Profiling (Αυτοματοποιημένα Εργαλεία Λήψης Αποφάσεων και Δημιουργίας Προφίλ) **[1]**. Τα παραπάνω εργαλεία έχουν την δυνατότητα να εκτελούν εργασίες και να παίρνουν αποφάσεις χωρίς την ανθρώπινη παρέμβαση. Οι αποφάσεις μπορούν να βασίζονται είτε σε πραγματικά δεδομένα, καθώς και σε ψηφιακά τα οποία έχουν δημιουργηθεί προηγουμένως, από μια άλλη επεξεργασία.

Παραδείγματα εφαρμογών των παραπάνω εργαλείων είναι η απόφαση για το εάν κάποιος μπορεί να λάβει δάνειο από μία τράπεζα, εάν κάποιος υποψήφιος για μια θέση εργασίας είναι ο κατάλληλος να προσληφθεί και πολλά άλλα.

Τα παραπάνω συστήματα χρησιμοποιούνται σε πολλούς τομείς, όπως της υγείας, της εκπαίδευσης, της οικονομίας και έχει σαν αποτέλεσμα οι αποφάσεις να λαμβάνονται πολύ πιο γρήγορα, να είναι πιο «συνεπείς», ειδικά σήμερα που υπάρχει ένας τόσο μεγάλος όγκος δεδομένων και πληροφορίας.

Βέβαια επειδή σε όλες τις περιπτώσεις απαιτείται μία στάθμιση με τα θετικά και τα αρνητικά χαρακτηριστικά, έτσι και εδώ έχουμε και τα αρνητικά εάν γίνεται χρήση των προαναφερόμενων τεχνολογιών, και συγκεκριμένα:

1. Οι πολίτες δεν έχουν ιδέα για το πως τα προσωπικά τους δεδομένα χρησιμοποιούνται και πως γίνεται η επεξεργασία αυτών,

2. Ακόμα και αν οι πολίτες έχουν σχετική πληροφόρηση, δεν καταλαβαίνουν ή δεν ξέρουν ακριβώς την διαδικασία της επεξεργασίας των προσωπικών τους δεδομένων από τα εργαλεία αυτά,

3. Μπορεί οι αποφάσεις που λαμβάνουν τα εργαλεία αυτά, να είναι λανθασμένες και να έχουν τελείως αρνητικές επιπτώσεις στους πολίτες των οποίων τα προσωπικά δεδομένα υφίστανται αυτού του είδους την επεξεργασία.

Όλα τα ανωτέρω συνιστούν παραβιάσεις θεμελιωδών ατομικών δικαιωμάτων για την Ευρωπαϊκή Ένωση και όχι μόνο – ιδίως παραβίαση απαιτήσεων προστασίας προσωπικών δεδομένων. Στο σημείο αυτό, πρέπει να γίνει αναφορά στη σχέση των εργαλείων αυτών και της προστασίας των προσωπικών δεδομένων, και αυτό γιατί ενώ υπάρχει ως νομικό πλαίσιο ο GDPR (General Data Protection Regulation - Γενικός Κανονισμός για την Προστασία Δεδομένων), ένα νομοθέτημα για την προστασία των προσωπικών δεδομένων και των ατομικών ελευθεριών, στην πράξη φαίνεται ότι υπάρχουν κενά στην υλοποίηση των σχετικών νομικών προβλέψεων και συγκεκριμένα οι πολίτες δεν προστατεύονται πλήρως απέναντι στα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, που χρησιμοποιούν AI **[2]**.

Ειδικότερα, παρόλο που αναφέρεται εντός του GDPR ότι κατά την διαδικασία ανάπτυξης των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, υπάρχουν στοιχεία που μπορούν να οδηγήσουν σε πιθανές αρνητικές επιπτώσεις και την πρόληψη αυτών, καθώς

επίσης και παρόλο που περιγράφονται ένα σύνολο αυστηρών προϋποθέσεων για τη νόμιμη χρήση τους, εν τούτοις υπάρχει μια μεγάλη ασάφεια ως προς διάφορα στοιχεία, όπως ως προς το πώς καθορίζονται οι επιπτώσεις και από ποιον/ους, πώς γίνεται η αξιολόγησή τους και πώς διασφαλίζεται η λογοδοσία **[3]**.

Στο σημείο αυτό αναφορά θα πρέπει να γίνει για την AIA (AIA - Algorithmic Impact Assessments - Αλγοριθμική Εκτίμηση Επιπτώσεων), ένα εργαλείο που σαν σκοπό έχει την δημιουργία ενός Framework για τον έλεγχο και την διασφάλιση ότι τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, λειτουργούν κατά τέτοιο τρόπο, έτσι ώστε να μην υπάρχει παραβίαση του τρόπου επεξεργασίας των προσωπικών δεδομένων των πολιτών και των ατομικών ελευθεριών αυτού, αλλά και το ότι οι αποφάσεις που παίρνουν λαμβάνονται σωστά **[20]**. Η AIA έχει προταθεί ως εργαλείο που καλείται να αντιμετωπίσει τέτοιους κινδύνους από αυτοματοποιημένα εργαλεία λήψης αποφάσεων. Λόγω του ότι αποτελεί μία σχετικά νέα προσέγγιση και είναι εστιασμένη αποκλειστικά σε τέτοιου τύπου επεξεργασίες, στις προβλέψεις του GDPR (που άλλωστε είναι γενικό νομοθέτημα και καλύπτει κάθε είδους επεξεργασία προσωπικών δεδομένων) δεν υπάρχει αναφορά σε ανάγκη εκπόνησης AIA.

1.1 Αναγκαιότητα και Σπουδαιότητα Έρευνας

Δεν αμφισβητείται ότι η χρησιμοποίηση νέων τεχνολογιών και εργαλείων, δημιουργεί μια νέα δυναμική, για οργανισμούς, δημόσιους φορείς και εταιρείες, ως προς την επεξεργασία ενός τεράστιου όγκου πληροφορίας, που καθημερινά αυξάνει ολοένα με εκθετικούς ρυθμούς, και πλέον ο ανθρώπινος παράγοντας δεν μπορεί να διαχειριστεί, χωρίς την βοήθεια νέων τεχνολογιών και εργαλείων.

Επίσης, σε καμία περίπτωση δεν υπάρχει αρνητική οπτική σε νέες τεχνολογίες και εργαλεία που θα βοηθήσουν την καθημερινότητα των πολιτών, σε μια κοινωνία που καθημερινά εξελίσσεται με ραγδαίους ρυθμούς, και αναπόφευκτα η χρήση νέων τεχνολογιών και εργαλείων θα έρθουν να λύσουν προβλήματα, που πριν μερικά χρόνια φάνταζαν σαν ταινία επιστημονικής φαντασίας.

Παρόλα αυτά, όλες αυτές οι τεχνολογίες και τα εργαλεία δεν μπορούν να χρησιμοποιηθούν απλά επειδή θα βελτιώσουν την καθημερινότητα των πολιτών, θα πρέπει να τηρούν κάποιες προδιαγραφές, να υπάρχουν έλεγχοι ως προς το εάν λειτουργούν σωστά και σύννομα με νόμους, οδηγίες, πολιτικές, έτσι ώστε να μην λέγεται απλά ότι γίνεται χρήση του τάδε εργαλείου ή τεχνολογίας που βοηθάει στη επίλυση του τάδε προβλήματος, αλλά να λέγεται ότι γίνονται όλα τα

παραπάνω αλλά με ένα τρόπο νόμιμο, χωρίς να αποκρύπτονται πληροφορίες θελημένα ή άθελα από τους πολίτες που έχουν δικαίωμα να ξέρουν αυτές τις πληροφορίες.

Με βάση όλα τα προαναφερόμενα έτσι και τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ (με την βοήθεια του AI και του ML), τα οποία βοηθούν τις εταιρείες να επεξεργαστούν έναν τεράστιο όγκο δεδομένων και πληροφορίας, γρήγορα και σε πολλές περιπτώσεις χωρίς την παρέμβαση ανθρώπινου παράγοντα για την λήψη αποφάσεων και την δημιουργία προφίλ, εισάγουν το ερώτημα το κατά πόσο είναι ευθυγραμμισμένα με νόμους, πολιτικές, οδηγίες σε ότι έχουν να κάνουν με την επεξεργασία προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών.

Απόρροια όλων αυτών είναι τελικά η διακινδύνευση της προστασίας των προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών αλλά και των ελευθεριών του, ενώ επίσης ειδικότερα είναι αμφίβολο αν ικανοποιείται το δικαίωμα να γνωρίζουν τι επεξεργασία υφίστανται οι προσωπικές πληροφορίες τους, όταν χρησιμοποιούνται οι συγκεκριμένες τεχνολογίες αλλά και εργαλεία που προαναφέρθηκαν.

Σε καμία περίπτωση δεν θα πρέπει να αποκρύπτονται θελημένα η άθελα πληροφορίες που ζητάει να μάθει κάποιος πολίτης, όσον αφορά τον τρόπο λειτουργίας των προαναφερόμενων εργαλείων και επεξεργασίας των δεδομένων.

Η συγκεκριμένη διατριβή προσπαθεί κατ' αρχάς να να ρίξει φως εάν οι σχετικές προβλέψεις του GDPR μπορούν πρακτικά να παρέχουν επαρκείς διασφαλίσεις για τα δικαιώματα και τις ελευθερίες των προσώπων εν όψει των κινδύνων από αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, υπό το φως ιδίως της διερεύνησης τη λεγόμενης αλγοριθμικής εκτίμησης αντικτύπου για συστήματα τεχνητής νοημοσύνης – ένας όρος ο οποίος, όπως προαναφέρθηκε, δεν εμφανίζεται εντός του GPDR.

Στο πλαίσιο αυτό, θα διερευνηθεί η συσχέτιση στην πράξη της εκτίμησης αντικτύπου ως προς τα προσωπικά δεδομένα, όπως προβλέπεται στο άρθρο 35 του GDPR, και της αλγοριθμικής εκτίμησης αντικτύπου για περιπτώσεις λήψης αυτοματοποιημένων αποφάσεων, με απώτερο στόχο στην ανάπτυξη ενός μεθοδολογικού πλαισίου που τα ενοποιεί κατάλληλα.

Επίσης, θα γίνει μια προσπάθεια στο να βρεθούν εάν υπάρχουν κανονισμοί, κατευθυντήριες γραμμές ακόμα και εργαλεία στην δημιουργία του γενικού πλαισίου προστασίας αλλά και σωστής λειτουργίας των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ αλλά και διαφάνειας. Ακολούθως, μέσω μελέτης περίπτωσης, θα αναπτυχθεί μεθοδολογία η οποία

θα συνδυάζει υπάρχοντα εργαλεία προκειμένου να προκύψει μία ενιαία προσέγγιση, η οποία ιδανικά θα πρέπει να ακολουθείται από οργανισμούς που καλούνται να πραγματοποιήσουν επεξεργασίες δεδομένων μέσω αυτοματοποιημένων εργαλείων λήψης αποφάσεων.

1.2 Σκοπός και Στόχος Διατριβής

Λαμβάνοντας υπόψιν τα όσα έχουν γραφτεί μέχρι τώρα, γίνεται ξεκάθαρο ότι είναι πολύ σημαντικό να διασφαλίζεται η προστασία προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών, σε μια κοινωνία που πλέον η λέξη αυτοματοποίηση διάφορων διαδικασιών, από την απόφαση εάν ένας πολίτης θα λάβει δάνειο μέχρι το εάν θα προσληφθεί σε μια θέση, και πόσο μάλλον εάν όλα αυτά γίνονται με την βοήθεια τεχνολογιών όπως έχουν προαναφερθεί όπως για παράδειγμα ML και AI, και πολλές φορές χωρίς καν την μεσολάβηση του ανθρώπινου παράγοντα.

Σκοπός της παρούσας Διατριβής είναι να διερευνήσει τις ειδικές προκλήσεις που απορρέουν από την ανάπτυξη και χρήση αυτοματοποιημένων εργαλείων για την επεξεργασία προσωπικών δεδομένων και, ειδικότερα, να εξετάσει εάν ο GDPR παρέχει, από την αμιγώς νομική σκοπιά, επαρκείς δικλείδες ασφαλείας απέναντι στην επεξεργασία των προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών με την χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, καθώς επίσης και να μελετήσει τη συσχέτιση μεταξύ της AIA και των συναφών νομικών απαιτήσεων του GDPR. Ειδικότερα, θα διερευνηθεί εάν μπορεί να υπάρξει πρακτικά ένα κοινό πλαίσιο μεταξύ του GDPR και της AIA, για τον καλύτερο συνεχή έλεγχο της λειτουργίας των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

1.3 Ερευνητικά Ερωτήματα

Τα ερευνητικά ερωτήματα, στα οποία θα γίνει προσπάθεια να απαντηθούν μέσα από την συγκεκριμένη Διατριβή είναι τα εξής:

- Ο GDPR, μπορεί από μόνος του να παρέχει αποτελεσματικά ένα γενικό πλαίσιο προστασίας ως προς αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ;

- Μπορεί να υπάρξουν εργαλεία, κανονισμοί και κατευθυντήριες γραμμές, στην δημιουργία ενός γενικού πλαισίου στο πως ελέγχονται τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ;

- Μπορεί να ελεγχθεί ένα αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ, κατά την φάση της ανάπτυξής του, έτσι ώστε να προβλεφθούν εγκαίρως παραβιάσεις στον τρόπο επεξεργασίας, μεταβίβασης δεδομένων κτλ.;

- Ποια η συσχέτιση μεταξύ της εκτίμησης αντικτύπου ως προς την προστασία δεδομένων και της αλγοριθμικής εκτίμησης αντικτύπου για τεχνικές τεχνητής νοημοσύνης; Μπορούν να συνδυαστούν κατάλληλα σε περιπτώσεις όπου η επεξεργασία δεδομένων γίνεται μέσω τέτοιων τεχνικών;

- Δεδομένου των διαφορετικών τομέων (υγείας, κοινωνικών παροχών κτλ) που υπάρχουν, μπορεί να χρησιμοποιηθούν αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ μέσα πάντα σε ένα ορθό σύστημα ελέγχου αυτών, και υπάρχει ή μπορεί να υπάρξει ένα γενικό πλαίσιο προστασίας των ατομικών δικαιωμάτων και ελευθεριών του/ων υποκειμένου/ων ανεξαρτήτου τομέα;

1.4 Μεθοδολογία

Η μεθοδολογική μας προσέγγιση έγκειται, πέραν της μελέτης των σχετικών εννοιών και της σχετικής βιβλιογραφίας προκειμένου να αποτυπωθούν τα διάφορα ανοιχτά ζητήματα αλλά και τα διάφορα διαθέσιμα ήδη σχετικά εργαλεία, στην εκπόνηση μίας συνολικής εκτίμησης αντικτύπου για ένα τέτοιο σύστημα στο πλαίσιο μίας ρεαλιστικής μελέτης περίπτωσης (Υποθετικό Σενάριο) στο Δημόσιο Τομέα, και συγκεκριμένα ενός αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, που θα μπορούσε να χρησιμοποιηθεί από φορείς του Υπουργείου Μετανάστευσης και Ασύλου.

Στην μελέτη περίπτωσης που προαναφέρθηκε θα γίνει σε πρώτη φάση μια ανάλυση κινδύνων ασφαλείας σύμφωνα με τον οδηγό του Ευρωπαικού Οργανισμού Κυβερνοασφάλειας «ENISA» **[21]**, αλλά επίσης και τον αντίκτυπο που έχει αυτήν η επεξεργασία στα προσωπικά και ευαίσθητα προσωπικά δεδομένα των αιτούντων άσυλο ως προς την Εμπιστευτικότητα, την Ακεραιότητα και την Διαθεσιμότητα.

Στην συνέχεια θα πραγματοποιηθεί η ΑΙΑ, με την βοήθεια του εργαλείου-ερωτηματολογίου του Υπουργείου Οικονομικών του Καναδά **[18]**, που αποτελείται από

48 ερωτήσεις που καθορίζουν το ρίσκο που εισάγει η χρήση του συγκεκριμένου εργαλείου προς αξιολόγηση, και επίσης 33 ερωτήσεις για την βοήθεια του μετριασμού του ρίσκου που εισάγει η χρήση του συγκεκριμένου εργαλείου.

Και τέλος με βάση τις πληροφορίες που θα έχουν εξαχθεί από τις προαναφερόμενες μελέτες, θα πραγματοποιηθεί μια ΕΑΠΔ (Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων) στην βάση του GDPR, κάνοντας χρήση του εργαλείου PIA της Γαλλικής Αρχής Προστασίας Δεδομένων CNIL**[11]**. Σκοπός είναι να καταδείξουμε πώς τα διαφορετικά αυτά εργαλεία μπορούν να συνδυαστούν, έτσι ώστε να «τροφοδοτεί» το ένα το άλλο, καθιστώντας εν τέλει δυνατή μία κατά κάποιο τρόπο ενιαία διαδικασία, η οποία θα μπορούσε να αποτελέσει οδηγό για οποιονδήποτε οργανισμό.

1.5 Διάταξη Μεταπτυχιακής Διατριβής

Η παρούσα Μεταπτυχιακή Διατριβή, θα αποτελείται συνολικά από πέντε κεφάλαια, και συγκεκριμένα:

1) Αρχικό κεφάλαιο η Εισαγωγή, συνοδευόμενο από την αναγκαιότητα της έρευνας, τον σκοπό της έρευνας, τα βασικά ερευνητικά ερωτήματα ενώ ταυτόχρονα θα επεξηγηθεί η επιλογή του είδους της έρευνας και το μοντέλο που θα ακολουθηθεί,

2) Δεύτερο κεφάλαιο, με τίτλο Αυτοματοποιημένα εργαλεία λήψης αποφάσεων, που θα κάνει μια αναφορά τι είναι τα εργαλεία αυτά και τις τεχνολογίες που βρίσκονται πίσω από αυτά,

3) Τρίτο κεφάλαιο, με τίτλο Επεξεργασία προσωπικών δεδομένων – Νομικό πλαίσιο, που θα περιλαμβάνει βασικούς ορισμούς και έννοιες του GDPR (General Data Protection Regulation – Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων), αλλά και μια μελέτη για το εάν αναφέρονται μέσα σε αυτόν τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ,

4) Τέταρτο κεφάλαιο, με τίτλο επισκόπηση βιβλιογραφίας,

5) Πέμπτο Κεφάλαιο, με τίτλο Συσχέτιση της AIA (Algorithm Impact Assessment – Αλγοριθμική Εκτίμηση επιπτώσεων) με τις υποχρεώσεις που απορρέουν από τον GDPR,

6) Έκτο κεφάλαιο, μελέτη περίπτωσης (Υποθετικό Σενάριο) σε φορείς του Υπουργείου Μετανάστευσης και Ασύλου,

7) Και τέλος στο έβδομο κεφάλαιο Συμπεράσματα – Μελλοντική έρευνα.

Κεφάλαιο 2

Αυτοματοποιημένα Εργαλεία Λήψης Αποφάσεων

Το παρόν κεφάλαιο εστιάζει στο να δοθεί μία βασική εικόνα για το τι είναι τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων ή/και δημιουργίας προφίλ, τι τεχνολογίες χρησιμοποιούν και πως λειτουργούν.

Είναι πολύ σημαντικό να γίνει κατανοητό το πόσο έχουν εισβάλει στη καθημερινότητα και το πόσο επηρεάζουν την ζωή των πολιτών.

2.1. Τι είναι τα Αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ

Λόγω του τεράστιου όγκου δεδομένων και πληροφορίας που πλέον υπάρχει, έχει δημιουργηθεί η ανάγκη για γρήγορη επεξεργασία τους, και τα συγκεκριμένα εργαλεία έρχονται να αναλάβουν αυτήν την επεξεργασία πολύ πιο γρήγορα από τον ανθρώπινο παράγοντα – αλλά, με συγκεκριμένες προϋποθέσεις, με βάση το νομικό πλαίσιο που υπάρχει.

Άξιο αναφοράς, ότι τα συγκεκριμένα εργαλεία αυτά χρησιμοποιούνται ευρέως σε πολλούς τομείς όπως υγεία, οικονομία, εκπαίδευση, και κατά επέκταση θα υπάρχει μια πληθώρα από προσωπικά και ευαίσθητα προσωπικά δεδομένα τα οποία θα υφίστανται επεξεργασία, έτσι ώστε να δώσουν κάποια αποτελέσματα-αποφάσεις προς τις εταιρείες-οργανισμούς που χρησιμοποιούν αυτά τα εργαλεία ή ακόμα και να δημιουργήσουν ένα προφίλ για έναν πελάτη, υποψήφιο για θέση εργασίας, ασθενή, για το εάν κάποιος μπορεί να λάβει δάνειο από τραπεζικό ίδρυμα **[7]**.

2.2. Ποιες τεχνολογίες υπάρχουν πίσω από τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ

Οι τεχνολογίες οι οποίες υπάρχουν πίσω από αυτά τα εργαλεία, είναι δύο, και συγκεκριμένα το AI **[4]** και το ML **[5]**.

Το AI, αναφέρεται στην ικανότητα μιας μηχανής να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι η μάθηση, ο σχεδιασμός και η δημιουργικότητα.

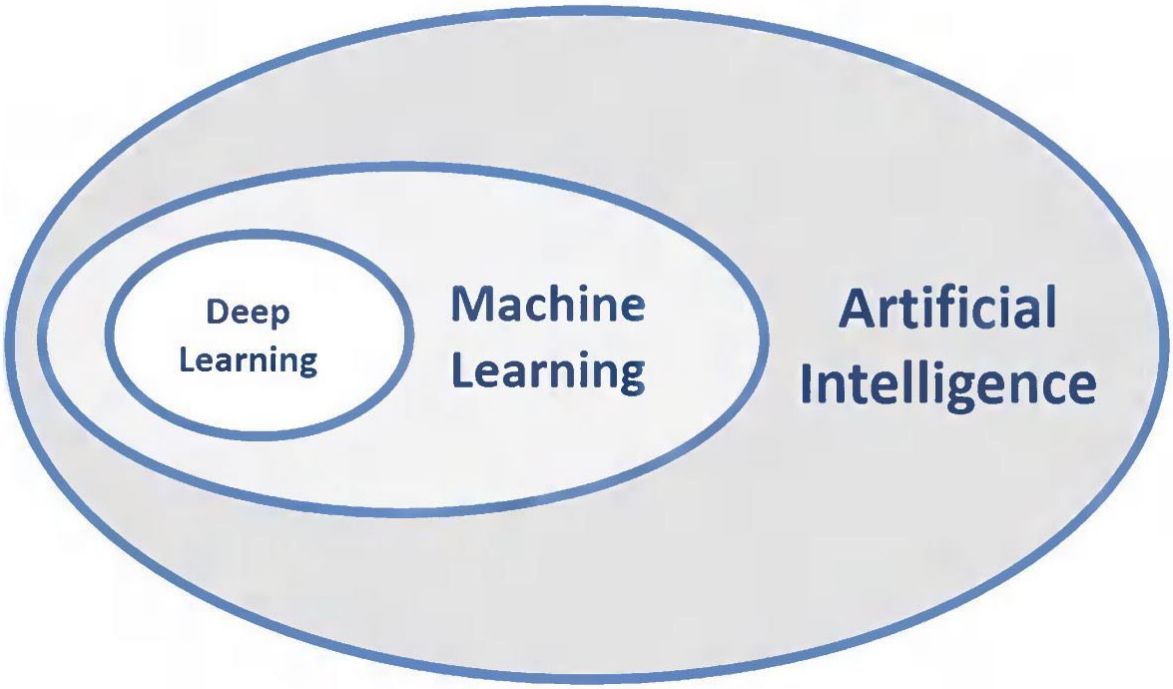
Η τεχνητή νοημοσύνη καθιστά τις μηχανές ικανές να κατανοούν το περιβάλλον τους, να επιλύουν προβλήματα και να δρουν προς την επίτευξη ενός συγκεκριμένου στόχου. Ο υπολογιστής λαμβάνει δεδομένα (ήδη έτοιμα ή συλλεγμένα μέσω αισθητήρων, π.χ. κάμερας), τα επεξεργάζεται και ανταποκρίνεται βάσει αυτών.

Τα συστήματα τεχνητής νοημοσύνης είναι ικανά να προσαρμόζουν τη συμπεριφορά τους, σε ένα ορισμένα βαθμό, αναλύοντας τις συνέπειες προηγούμενων δράσεων και επιλύοντας προβλήματα με αυτονομία **[7]**.

Θα πρέπει να αναφερθεί ότι υπάρχουν διάφοροι τρόποι που μπορούν να χρησιμοποιηθούν για να αναπτυχθούν εργαλεία που βασίζονται στο AI, οι οποίοι φαίνονται στην παρακάτω εικόνα (Εικόνα 2.1).

Εικόνα 2.1: Τύποι AI

Το ML, το οποίο είναι ένα παρακλάδι του AI, (Εικόνα 2.2),



Εικόνα 2.2: Διαχωρισμός AI, ML και DL

αναφέρεται στο πεδίο της επιστήμης των υπολογιστών που μελετά τη δημιουργία αλγορίθμων οι οποίοι «μαθαίνουν» χωρίς να έχουν προγραμματιστεί με συγκεκριμένους κανόνες. Με άλλα λόγια, οι αλγόριθμοι αυτοί χρησιμοποιούν δεδομένα με σκοπό να ανακαλύψουν μοτίβα και σχέσεις ώστε να κάνουν προβλέψεις ή να πάρουν αποφάσεις **[7]**.

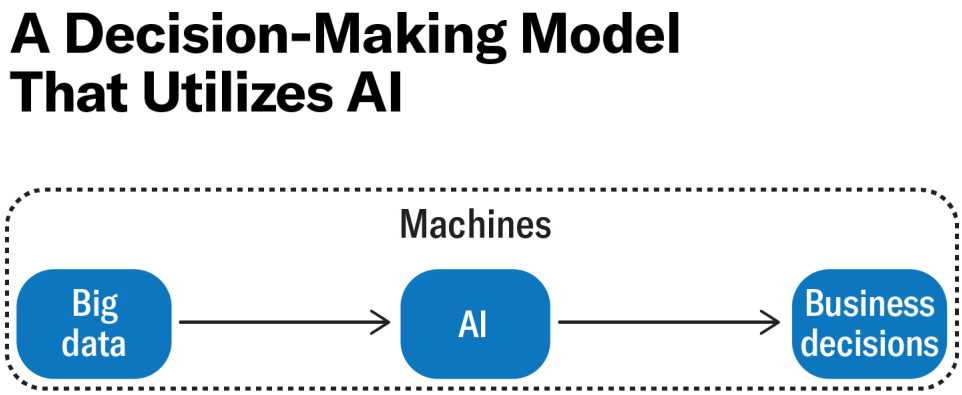
Άρα η διαφορά μεταξύ AI και ML είναι:

1) AI η ιδέα-τρόπος το πως οι υπολογιστές και οι μηχανές θα επιδεικνύουν μια σχεδόν ανθρώπινη συμπεριφορά,

2) ML χρήση ειδικών αλγορίθμων που σαν σκοπό έχουν αυτόματα να μαθαίνουν-εκπαιδεύονται από τα δεδομένα και τις πληροφορίες που δέχονται.

2.3. Τρόπος λειτουργίας των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ

Με βάση όλα τα προαναφερόμενα, γίνεται αντιληπτό ότι τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, με την χρήση AI και ML, έχουν την ικανότητα να παίρνουν αποφάσεις χωρίς την παρέμβαση του ανθρώπινου παράγοντα, και συγκεκριμένα δημιουργούν ένα workflow όπως φαίνεται στην παρακάτω (Εικόνα 2.3).



Εικόνα 2.3: Ενδεικτικός τρόπος λειτουργίας του AI

Το αξιοσημείωτο εδώ είναι ότι από το παραπάνω σχήμα γίνεται αντιληπτό ότι βάσει αυτών των αποφάσεων που λαμβάνονται από τα αυτοματοποιημένα εργαλεία, οι εταιρείες - οργανισμοί μπορούν να βασίζουν τις δικές τους αποφάσεις σε διάφορα θέματα, οπότε θα πρέπει να αναφερθεί το πόσο σημαντικό είναι η σωστή λειτουργία των εργαλείων αυτών αλλά επίσης και το πόσο σημαντικό είναι η ευθυγράμμιση τους με την κείμενη νομοθεσία.

2.4. Η έννοια της αλγοριθμικής εκτίμησης αντικτύπου

Η αλγοριθμική εκτίμηση αντικτύπου έχει προταθεί σαν ένα κανονιστικό πλαίσιο για την βελτίωση και διόρθωση των αρνητικών επιπτώσεων που μπορεί να εισάγει ένα αλγοριθμικό σύστημα, και το οποίο θα απαιτεί από τον δημιουργό του αλγοριθμικού συστήματος να αξιολογήσει τις πιθανές αρνητικές επιπτώσεις που θα έχει στο κοινωνικό επίπεδο πριν από την εφαρμογή του. **[15]**.

Η AIA, έχει σαν αποτέλεσμα να θέτει ένα πλαίσιο λογοδοσίας σε εταιρείες και οργανισμούς, που αναπτύσσουν αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, μέσα από μια φάση αξιολόγησης των προαναφερόμενων εργαλείων **[16]**.

Το σημαντικό και άξιο αναφοράς, είναι ότι η αξιολόγηση αυτή θα πρέπει να γίνεται από ειδικούς που θα μπορούν να αντιληφθούν και θα έχουν την κατάλληλη τεχνογνωσία να καταλάβουν πως λειτουργεί το αλγοριθμικό σύστημα, έτσι ώστε η συγκεκριμένη αξιολόγηση να γίνεται σωστά και να δίνει σωστά αποτελέσματα, ώστε να μπορούν να γίνουν οι απαραίτητες αλλαγές που θα έχουν σαν αποτέλεσμα την βελτίωση των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Κρίσιμο σημείο του σωστού ελέγχου των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, είναι οι εταιρείες ανάπτυξης τέτοιων λογισμικών/εργαλείων να είναι πρόθυμες να συνεργαστούν σε τέτοιους είδους ελέγχους, που θα αποτελέσει την αφετηρία για την σωστή λειτουργία της ΑΙΑ **[15]**.

Κεφάλαιο 3

Επεξεργασία Προσωπικών Δεδομένων – Νομικό Πλαίσιο

Σε αυτό το κεφάλαιο θα παρουσιαστεί το νομικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων, με έμφαση στον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation – GDPR) **[6]**. Ο Κανονισμός αυτός, ο οποίος είναι σε ισχύ από τις 25 Μαϊου 2018, αποτελεί το βασικό νομοθέτημα αυτή τη στιγμή στην Ευρωπαϊκή Ένωση (ΕΕ) για την προστασία των προσωπικών δεδομένων και έχει άμεση εφαρμογή σε όλα τα Κράτη-Μέλη – ενώ, ακόμα περισσότερο, έχει εφαρμογή και για περιπτώσεις οργανισμών εκτός ΕΕ οι οποίοι όμως παρέχουν υπηρεσίες σε πολίτες της ΕΕ.

Ο GDPR αναπτύχθηκε με στόχο να αντιμετωπίσει τις προκλήσεις που απορρέουν αναφορικά με τα θεμελιώδη δικαιώματα της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας, λαμβάνοντας ιδίως υπόψη την πρόοδο των τεχνολογικών εξελίξεων και τους συναφείς κινδύνους για δικαιώματα και ελευθερίες. Ο GDPR στοχεύει να εξασφαλίσει μια ενιαία και συνεπή προσέγγιση για την προστασία των προσωπικών δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση.

Στη συνέχεια αα αναφερθούν βασικοί ορισμοί και έννοιες του Γενικού Κανονισμού Προστασίας Δεδομένων, αλλά και ρόλοι όπως του υπεύθυνου επεξεργασίας δεδομένων, του εκτελούντος την επεξεργασία κτλ.

3.1. Ορισμοί – Άρθρο 4

Το άρθρο 4 του κανονισμού ορίζει αρκετούς σημαντικούς όρους που χρησιμοποιούνται σε ολόκληρο τον κανονισμό. Αυτοί οι ορισμοί είναι σημαντικοί για την κατανόηση του GDPR και του τρόπου εφαρμογής του στην επεξεργασία προσωπικών δεδομένων, και συγκεκριμένα:

Προσωπικά Δεδομένα: Κάθε πληροφορία που σχετίζεται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Αυτό μπορεί να περιλαμβάνει το όνομα, τη διεύθυνση, τη διεύθυνση email ενός

ατόμου, τον αριθμό αναγνώρισης, τα δεδομένα τοποθεσίας ή οποιαδήποτε άλλη πληροφορία που μπορεί να χρησιμοποιηθεί για την άμεση ή έμμεση αναγνώριση ενός ατόμου.

Υποκείμενο δεδομένων: Το φυσικό πρόσωπο που αποτελεί αντικείμενο των προσωπικών δεδομένων – δηλαδή του οποίου τα δεδομένα υφίστανται επεξεργασία (όπως αυτή ορίζεται στη συνέχεια).

Επεξεργασία: Οποιαδήποτε λειτουργία ή σύνολο λειτουργιών που εκτελείται σε προσωπικά δεδομένα, συμπεριλαμβανομένης της συλλογής, καταγραφής, οργάνωσης, δομής, αποθήκευσης, προσαρμογής, τροποποίησης, ανάκτησης, συμβουλευτικής, χρήσης, αποκάλυψης, διάδοσης, διαγραφής ή καταστροφής.

Συγκατάθεση: Οποιαδήποτε ελεύθερα δοθείσα, συγκεκριμένη, κατόπιν πλήρους ενημέρωσης και σαφής ένδειξη των επιθυμιών του υποκειμένου των δεδομένων με την οποία είτε με δήλωση είτε με σαφή θετική ενέργεια, δηλώνει συμφωνία για την επεξεργασία των προσωπικών δεδομένων που το αφορούν.

Υπεύθυνος επεξεργασίας: Το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Εκτελών την επεξεργασία: Φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας.

Στην παρούσα διατριβή επειδή θα ερευνηθεί ο αντίκτυπος των αυτοματοποιημένων εργαλείων αποφάσεων και δημιουργίας προφίλ, ένας σημαντικός ορισμός που υπάρχει στο άρθρο 4, και θα πρέπει να αναφερθεί επίσης είναι ο παρακάτω:

Δημιουργία προφίλ: αναφέρεται σε οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων που αποσκοπεί στην αξιολόγηση ορισμένων προσωπικών πτυχών ενός ατόμου, όπως η απόδοσή του στην εργασία, η οικονομική κατάσταση, η υγεία, οι προσωπικές προτιμήσεις, τα ενδιαφέροντα, η συμπεριφορά ή η τοποθεσία του.

Συνολικά, το άρθρο 4 του GDPR παρέχει ένα πλαίσιο για την κατανόηση των βασικών όρων και εννοιών που έχουν κεντρική θέση στον κανονισμό.

3.2. Αρχές σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα – Άρθρο 5

Το άρθρο 5 του Κανονισμού περιγράφει τις αρχές που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αυτές οι αρχές είναι θεμελιώδεις για τη διασφάλιση της προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων των ατόμων και πρέπει να πληρούνται πάντοτε σε μία επεξεργασία δεδομένων, προκειμένου αυτή να είναι σύννομη και επιτρεπτή

Ειδικότερα, το άρθρο αυτό απαριθμεί έξι αρχές που πρέπει να ακολουθούνται κατά την επεξεργασία προσωπικών δεδομένων. Αυτές είναι:

Νομιμότητα, δικαιοσύνη και διαφάνεια: Η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται νόμιμα, δίκαια και με διαφανή τρόπο.

Περιορισμός σκοπού: Τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο που δεν είναι συμβατός με αυτούς τους σκοπούς.

Ελαχιστοποίηση δεδομένων: Τα προσωπικά δεδομένα πρέπει να είναι επαρκή, σχετικά και να περιορίζονται σε ό,τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους υφίστανται επεξεργασία.

Ακρίβεια: Τα προσωπικά δεδομένα πρέπει να είναι ακριβή και, όπου χρειάζεται, να διατηρούνται ενημερωμένα. Τα ανακριβή δεδομένα θα πρέπει να διαγράφονται ή να διορθώνονται χωρίς καθυστέρηση.

Περιορισμός αποθήκευσης: Τα προσωπικά δεδομένα θα πρέπει να φυλάσσονται σε μορφή που να επιτρέπει την ταυτοποίηση ατόμων για όχι περισσότερο από όσο είναι απαραίτητο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία τα δεδομένα.

Ακεραιότητα και εμπιστευτικότητα: Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία με τρόπο που να διασφαλίζει την κατάλληλη ασφάλεια, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή ζημιά.

Αυτές οι αρχές ισχύουν για όλες τις δραστηριότητες επεξεργασίας προσωπικών δεδομένων, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται ή τον τομέα στον οποίο υποβάλλονται σε

επεξεργασία τα δεδομένα. Παρέχουν ένα πλαίσιο για τους οργανισμούς ώστε να διασφαλίζουν ότι τα προσωπικά δεδομένα υφίστανται επεξεργασία με δίκαιο και διαφανή τρόπο και ότι γίνονται σεβαστά τα δικαιώματα ιδιωτικής ζωής των ατόμων.

Συνολικά, το άρθρο 5 του GDPR είναι ένα σημαντικό εργαλείο για τη διασφάλιση της επεξεργασίας των προσωπικών δεδομένων με υπεύθυνο και ηθικό τρόπο και ότι προστατεύονται τα δικαιώματα και οι ελευθερίες των ατόμων.

3.3. Νομιμότητα της επεξεργασίας – Άρθρο 6

Το άρθρο 6 του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) περιγράφει τις δυνατές νομικές βάσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, , τα προσωπικά δεδομένα μπορούν να υποβληθούν σε επεξεργασία μόνο εάν πληρούνται μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:

Συγκατάθεση: Το υποκείμενο των δεδομένων έχει δώσει ρητή συγκατάθεση για την επεξεργασία των προσωπικών του δεδομένων για συγκεκριμένο σκοπό.

Σύμβαση: Η επεξεργασία προσωπικών δεδομένων είναι απαραίτητη για την εκτέλεση σύμβασης με το υποκείμενο των δεδομένων ή για τη λήψη προσυμβατικών μέτρων κατόπιν αιτήματος του υποκειμένου των δεδομένων.

Νομική υποχρέωση: Η επεξεργασία προσωπικών δεδομένων είναι απαραίτητη για τη συμμόρφωση με νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.

Ζωτικά συμφέροντα: Η επεξεργασία προσωπικών δεδομένων είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.

Δημόσιο συμφέρον: Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση επίσημης εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

Έννομα συμφέροντα: Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν αυτά τα συμφέροντα υπερισχύουν των συμφερόντων, των θεμελιωδών δικαιωμάτων ή των ελευθεριών του υποκειμένου των δεδομένων.

Επιπλέον, εάν τα προσωπικά δεδομένα που επεξεργάζονται είναι ειδικής κατηγορίας (γνωστά ως ευαίσθητα δεδομένα), όπως δεδομένα που αποκαλύπτουν φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικάτα ή δεδομένα σχετικά με την υγεία ή τη σεξουαλική ζωή, πρέπει να πληρούνται πρόσθετες προϋποθέσεις.

Συνολικά, το άρθρο 6 του GDPR παρέχει ένα πλαίσιο για τη διασφάλιση της επεξεργασίας των προσωπικών δεδομένων με νόμιμο και διαφανή τρόπο και ότι γίνονται σεβαστά τα δικαιώματα ιδιωτικής ζωής των ατόμων. Είναι σημαντικό για τους οργανισμούς να κατανοούν τη νομική βάση για την επεξεργασία προσωπικών δεδομένων και να διασφαλίζουν ότι συμμορφώνονται με τον GDPR κατά την επεξεργασία τέτοιων δεδομένων – δηλαδή ότι για κάθε επεξεργασία που κάνουν υπάρχει πράγματι μία έγκυρη νομική βάση από αυτές που απαριθμούνται στο άρθρο 6 του GDPR.

3.4. – Δικαιώματα των φυσικών προσώπων

Τα άρθρα 13 έως 22 του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) αφορούν τα δικαιώματα των υποκειμένων των δεδομένων και τις υποχρεώσεις των υπευθύνων επεξεργασίας και επεξεργασίας δεδομένων σε σχέση με αυτά τα δικαιώματα. Ακολουθεί μια περίληψη κάθε άρθρου:

Άρθρο 13: Πληροφορίες που πρέπει να παρέχονται όταν συλλέγονται προσωπικά δεδομένα από το υποκείμενο των δεδομένων

Αυτό το άρθρο περιγράφει τις πληροφορίες που πρέπει να παρέχονται στα άτομα όταν συλλέγονται τα προσωπικά τους δεδομένα, συμπεριλαμβανομένης της ταυτότητας του υπεύθυνου επεξεργασίας, των σκοπών για τους οποίους θα υποστούν επεξεργασία τα δεδομένα και των δικαιωμάτων του υποκειμένου των δεδομένων.

Άρθρο 14: Πληροφορίες που πρέπει να παρέχονται όταν δεδομένα προσωπικού χαρακτήρα δεν έχουν ληφθεί από το υποκείμενο των δεδομένων

Αυτό το άρθρο περιγράφει τις πληροφορίες που πρέπει να παρέχονται σε άτομα όταν τα προσωπικά τους δεδομένα δεν έχουν ληφθεί απευθείας από αυτά, συμπεριλαμβανομένης της πηγής των δεδομένων και των δικαιωμάτων του υποκειμένου των δεδομένων.

Άρθρο 15: Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

Αυτό το άρθρο δίνει στα άτομα το δικαίωμα να λάβουν επιβεβαίωση για το εάν τα προσωπικά τους δεδομένα υποβάλλονται σε επεξεργασία και, εάν ναι, να έχουν πρόσβαση σε αυτά τα δεδομένα και σε ορισμένες αναλυτικές πληροφορίες σχετικά με την επεξεργασία τους.

Άρθρο 16: Δικαίωμα διόρθωσης

Αυτό το άρθρο δίνει στα άτομα το δικαίωμα να διορθώσουν τα ανακριβή προσωπικά δεδομένα και να συμπληρώσουν ελλιπή προσωπικά δεδομένα.

Άρθρο 17: Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

Αυτό το άρθρο δίνει στα άτομα το δικαίωμα να διαγράφονται τα προσωπικά τους δεδομένα σε ορισμένες περιπτώσεις, όπως όταν τα δεδομένα δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν.

Άρθρο 18: Δικαίωμα περιορισμού της επεξεργασίας

Αυτό το άρθρο δίνει στα άτομα το δικαίωμα να περιορίζουν την επεξεργασία των προσωπικών τους δεδομένων σε ορισμένες περιπτώσεις, όπως όταν αμφισβητείται η ακρίβεια των δεδομένων.

Άρθρο 19: Υποχρέωση κοινοποίησης σχετικά με τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας

Αυτό το άρθρο περιγράφει την υποχρέωση των υπευθύνων επεξεργασίας να ειδοποιούν τρίτα μέρη στα οποία έχουν αποκαλυφθεί τα προσωπικά δεδομένα σχετικά με οποιαδήποτε διόρθωση, διαγραφή ή περιορισμό της επεξεργασίας αυτών των δεδομένων.

Άρθρο 20: Δικαίωμα φορητότητας δεδομένων

Αυτό το άρθρο δίνει στα άτομα, υπό συγκεκριμένες προϋποθέσεις, το δικαίωμα να λαμβάνουν τα προσωπικά τους δεδομένα σε δομημένη, ευρέως χρησιμοποιούμενη και αναγνώσιμη από μηχανήματα μορφή προκειμένου να τα διαβιβάζουν ευχερώς σε άλλον υπεύθυνο επεξεργασίας.

Άρθρο 21: Δικαίωμα εναντίωσης

Αυτό το άρθρο δίνει στα άτομα το δικαίωμα να αντιταχθούν στην επεξεργασία των προσωπικών τους δεδομένων σε ορισμένες περιπτώσεις, όπως όταν η επεξεργασία βασίζεται σε έννομα συμφέροντα.

Άρθρο 22: Αυτοματοποιημένη ατομική λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ

Αυτό το άρθρο περιγράφει τα δικαιώματα των ατόμων σε σχέση με την αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένου του δικαιώματος να μην υπόκεινται σε απόφαση που βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία και του δικαιώματος να αποκτούν ανθρώπινη παρέμβαση και εξήγηση της απόφασης.

Συνολικά, αυτά τα άρθρα του GDPR παρέχουν στα άτομα σημαντικά δικαιώματα και δίνουν στους υπεύθυνους επεξεργασίας και στους εκτελούντες την επεξεργασία συγκεκριμένες υποχρεώσεις όσον αφορά αυτά τα δικαιώματα. Είναι σημαντικό οι οργανισμοί να κατανοούν και να συμμορφώνονται με αυτά τα άρθρα για να διασφαλίζουν την προστασία της ιδιωτικής ζωής και των δεδομένων των ατόμων.

Πριν περιγράψουμε αναλυτικότερα τις διατάξεις του GDPR που έχουν άμεση σχέση με το αντικείμενο της διατριβής, ήδη από τα ανωτέρω προκύπτει ότι ο GDPR θέτει ως κανόνα την απαγόρευση αυτοματοποιημένης λήψης απόφασης: εάν τέτοια εργαλεία πρόκειται να χρησιμοποιηθούν από έναν υπεύθυνο επεξεργασίας, η τελική απόφαση που αφορά ένα φυσικό πρόσωπο θα πρέπει τελικά να λαμβάνεται από άνθρωπο και να μην είναι αμιγώς αυτοματοποιημένη. Περαιτέρω, ο GDPR δίνει έμφαση στη διαφάνεια της επεξεργασίας: στο άρθρο 13, που αφορά την ενημέρωση που πρέπει να παρέχεται στα υποκείμενα των δεδομένων, γίνεται εκτενής αναφορά στο ότι πρέπει να παρέχεται ενημέρωση για όλες οι βασικές πτυχές της επεξεργασίας, συμπεριλαμβανομένης, για την περίπτωση αυτοματοποιημένου εργαλείου λήψης απόφασης, της λογικής αυτού (όπως αναλύεται στη συνέχεια).

3.5. GDPR και έλεγχος αλγοριθμικών συστημάτων λήψης αποφάσεων

Στο σημείο αυτό θα μελετηθεί ο GDPR για το τι αναφέρει όταν γίνεται χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, και συγκεκριμένα:

1) εάν και τι προστασία προβλέπει,

2) εάν και τι εργαλεία χρησιμοποιεί για να ελέγξει την σωστή και νόμιμη λειτουργία των προαναφερόμενων εργαλείων,

3) εάν γίνεται αναφορά στο πως υπολογίζεται η εκτίμηση επιπτώσεων, έτσι ώστε σε καμία περίπτωση να μην υπάρχει παραβίαση των προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών, κατά την διάρκεια επεξεργασίας αυτών με την χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων ή/και δημιουργίας προφίλ.

3.5.1. «Διατρέχοντας» τον GDPR - Μελέτη του GDPR για το τι προβλέπει ως προς τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ

Στο άρθρο 2 του κανονισμού (Material scope), αναφέρεται που μπορεί να εφαρμοστεί ο κανονισμός αυτός εξ ολοκλήρου η εν μέρει, σε ό,τι έχει να κάνει, μεταξύ άλλων, με τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ.

Στο άρθρο 4 του κανονισμού (Definitions), στην παράγραφο 2 αναφέρεται τι είναι η επεξεργασία προσωπικών δεδομένων είτε με αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ είτε όχι, και συγκεκριμένα:

- Επεξεργασία: Οποιαδήποτε λειτουργία ή σύνολο λειτουργιών που εκτελείται σε προσωπικά δεδομένα, συμπεριλαμβανομένης της συλλογής, καταγραφής, οργάνωσης, δομής, αποθήκευσης, προσαρμογής, τροποποίησης, ανάκτησης, συμβουλευτικής, χρήσης, αποκάλυψης, διάδοσης, διαγραφής ή καταστροφής.

και στη παράγραφο 4 αναφέρεται τι είναι η δημιουργία προφίλ ενός πολίτη από αυτοματοποιημένα μέσα, και συγκεκριμένα:

- Δημιουργία προφίλ: αναφέρεται σε οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων που αποσκοπεί στην αξιολόγηση ορισμένων προσωπικών πτυχών ενός ατόμου, όπως η απόδοσή του στην εργασία, η οικονομική κατάσταση, η υγεία, οι προσωπικές προτιμήσεις, τα ενδιαφέροντα, η συμπεριφορά ή η τοποθεσία του.

Επίσης στο άρθρο 13 του κανονισμού, αναφέρεται τι πληροφορίες θα πρέπει να γνωστοποιούνται στον πολίτη στην περίπτωση που η συλλογή των προσωπικών πληροφοριών γίνεται απευθείας από τον ίδιο, και συγκεκριμένα στην παράγραφο 2 γίνεται αναφορά σε ό,τι έχει να κάνει με τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, δηλαδή τις επιπτώσεις από μια τέτοια διαδικασία, συνέπειες κτλ,. Συγκεκριμένα, αναφέρεται το εξής ως προς τις πληροφορίες που θα πρέπει να παρέχονται: «την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και

4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.». Ωστόσο, δεν είναι ξεκάθαρο αν θα δίνεται μια πλήρη εικόνα για το πως για λειτουργούν τα εργαλεία αυτά.

Επίσης στα άρθρα 14 και 15 του κανονισμού, που καθορίζουν γενικές οδηγίες για τι πρέπει να ακολουθείται σε περίπτωση που οι πληροφορίες (προσωπικά ή και ευαίσθητα προσωπικά δεδομένα) αποκτήθηκαν εν αγνοία του υποκειμένου και συγκεκριμένα του πολίτη και τα δικαιώματα του πολίτη ως προς την πρόσβαση στο να μαθαίνει για παράδειγμα τον σκοπό της επεξεργασίας, τα στοιχεία του υπευθύνου επεξεργασίας, το δικαίωμα καταγγελίας σε εποπτική αρχή αλλά και την ύπαρξη αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, αλλά και πάλι αποτυπώνετε μια γενικότητα του νόμου ως προς την ύπαρξη απλά των εργαλείων αυτών και όχι κάτι παραπάνω.

Στο άρθρο 21 του κανονισμού, αναφέρεται πότε ο πολίτης θα μπορεί να ζητήσει να μην υφίστανται καμία επεξεργασία τα προσωπικά του δεδομένα, αναφέρονται συγκεκριμένες περιπτώσεις, και ειδικά όταν έχει να κάνει με την δημιουργία προφίλ του πολίτη, εκτός και εάν ο υπεύθυνος επεξεργασίας αποδείξει ότι υπάρχει σοβαρός λόγος στο να γίνει η επεξεργασία.

Στο άρθρο 22 του κανονισμού, ένα πολύ σημαντικό άρθρο γιατί δίνει στα υποκείμενα των δεδομένων το δικαίωμα να μην υπόκεινται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της δημιουργίας προφίλ, η οποία παράγει νομικά αποτελέσματα ή τα επηρεάζει με παρόμοιο τρόπο σημαντικά.

Η αυτοματοποιημένη λήψη αποφάσεων είναι η διαδικασία λήψης μιας απόφασης χρησιμοποιώντας τεχνολογικά μέσα, χωρίς ανθρώπινη συμμετοχή. Αυτό θα μπορούσε να περιλαμβάνει τη χρήση αλγορίθμων ή άλλων προγραμμάτων υπολογιστή για την ανάλυση δεδομένων και τη λήψη αποφάσεων.

Σύμφωνα με το άρθρο 22, το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει ανθρώπινη παρέμβαση, να εκφράσει την άποψή του και να αμφισβητήσει την απόφαση. Αυτό σημαίνει ότι εάν έχει ληφθεί μια απόφαση για ένα άτομο αποκλειστικά μέσω αυτοματοποιημένης επεξεργασίας, αυτή η απόφαση θα πρέπει να μην είναι η οριστική αλλά να εξεταστεί, και ενδεχομένως να αναθεωρηθεί, από έναν άνθρωπο που μπορεί να δώσει μια εξήγηση και ενδεχομένως να ανατρέψει την απόφαση. Ουσιαστικά αποτελεί μια υποχρέωση για κάθε υπεύθυνο επεξεργασίας: αν χρησιμοποιεί αυτοματοποιημένα εργαλεία για λήψη απόφασης, δεν μπορεί να βασίζεται μόνο σε αυτά προκειμένου να λαμβάνει αποφάσεις.

Ωστόσο, υπάρχουν ορισμένες εξαιρέσεις σε αυτόν τον κανόνα. Η αυτοματοποιημένη λήψη αποφάσεων επιτρέπεται εάν είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας δεδομένων, εάν επιτρέπεται από τη νομοθεσία της ΕΕ ή του κράτους μέλους (όπου βέβαια η νομοθεσία πρέπει να σέβεται σε κάθε περίπτωση τα θεμελιώδη δικαιώματα των ατόμων) ή εάν το υποκείμενο των δεδομένων έχει ρητά συναινέσει στη χρήση αυτοματοποιημένης απόφασης -κατασκευή.

Συνολικά, το άρθρο 22 του GDPR στοχεύει στην προστασία των ατόμων από άδικες και μεροληπτικές αποφάσεις που ενδέχεται να ληφθούν αποκλειστικά μέσω αυτοματοποιημένης επεξεργασίας.

Συνεχίζοντας την μελέτη του GDPR και παραθέτοντας παρακάτω τις εισαγωγικές σκέψεις του κανονισμού για μια πιο λεπτομερή μελέτη του, ως προς το εάν υπάρχουν εργαλεία ελέγχου (και στην φάση ανάπτυξής αλλά και κατά την χρήση των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ), και εάν ναι ποια, ή τουλάχιστον οδηγίες ανάπτυξης τέτοιων εργαλείων, δεν γίνεται πουθενά αναφορά τίποτα από τα δύο, και συγκεκριμένα:

Στην εισαγωγική σκέψη 15 του Κανονισμού, απλά αναφέρεται και γίνεται αντιληπτό ότι η προστασία των πολιτών και των προσωπικών δεδομένων δεν πρέπει να εξαρτάται από τα μέσα επεξεργασίας: είναι τεχνολογικά ουδέτερη και δεν εξαρτάται από τις χρησιμοποιούμενες τεχνικές. Ειδικότερα, η προστασία των φυσικών προσώπων θα πρέπει να εφαρμόζεται τόσο στην επεξεργασία δεδομένων προσωπικού χαρακτήρα με αυτοματοποιημένα μέσα, όσο και στη χειροκίνητη επεξεργασία, εάν τα δεδομένα προσωπικού χαρακτήρα περιέχονται ή προορίζονται να περιληφθούν σε σύστημα αρχειοθέτησης.

Στην εισαγωγική σκέψη 68 του κανονισμού, αναφέρεται ότι το υποκείμενο και συγκεκριμένα ο πολίτης του οποίου τα προσωπικά δεδομένα υφίστανται επεξεργασία με την χρήση αυτοματοποιημένων εργαλείων, έχει δικαίωμα να έχει πρόσβαση στα προσωπικά του δεδομένα, προφανώς οπόταν εκείνος το ζητήσει, με την ενίσχυση της διαλειτουργικότητας, κάτι το οποίο είναι απόλυτα σύννομο και αποτελεί ατομικό δικαίωμα του. Η συγκεκριμένη εισαγωγική σκέψη σχετίζεται με το λεγόμενο δικαίωμα φορητότητας των δεδομένων που προβλέπεται στο άρθρο 20 του GDPR: αν και το εν λόγω δικαίωμα δεν έχει άμεση σχέση με το δικαίωμα του άρθρου 22 (που είναι αυτό που αφορά την αυτοματοποιημένη λήψη αποφάσεων), εν τούτοις μπορεί να θεωρηθεί ότι το περιεχόμενο αυτής της εισαγωγικής σκέψης, και κατ' επέκταση και το δικαίωμα του άρθρου 20, υποδηλώνει ότι δεδομένα που παρήχθησαν από αυτοματοποιημένο εργαλείο λήψης αποφάσεων θα μπορούσαν, εάν το υποκείμενο αυτών ασκήσει το δικαίωμα φορητότητας

(το οποίο με τη σειρά του μπορεί να ασκηθεί μόνο υπό συγκεκριμένες προϋποθέσεις), να του δοθούν σε κατάλληλο μορφότυπο ώστε να καθίσταται εφικτή η διαβίβασή τους σε άλλον υπεύθυνο επεξεργασίας για αντίστοιχη επεξεργασία.

Στην εισαγωγική σκέψη 71 του Κανονισμού, αναφέρεται στην προστασία του πολίτη, έτσι ώστε τυχόν αυτοματοποιημένη επεξεργασία των προσωπικών του δεδομένων, και η απόφαση που θα ληφθεί, να μην λαμβάνει υπόψη προσωπικές πτυχές. Ειδικότερα, «*το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να μην υπόκειται σε απόφαση, η οποία μπορεί να περιλαμβάνει κάποιο μέτρο, με την οποία αξιολογούνται προσωπικές πτυχές που το αφορούν, λαμβανόμενη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο*». Ως χαρακτηριστικά παραδείγματα αποφάσεων που επηρεάζουν σημαντικά το υποκείμενο των δεδομένων αναφέρονται η αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή πρ3ακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση. Γίνεται αναφορά σε εξαιρέσεις όπου μπορούν να υπάρξουν τέτοιες αυτοματοποιημένες αποφάσεις, αλλά σε όλες αυτές τις εξαιρέσεις πρέπει να υπάρχουν κατάλληλα εχέγγυα, όπως ειδική ενημέρωση του υποκειμένου των δεδομένων και το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης, το δικαίωμα διατύπωσης της άποψής του, το δικαίωμα να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω εκτίμησης και το δικαίωμα αμφισβήτησης της απόφασης., Γενικά η εντύπωση που αποκομίζεται είναι ότι ο νόμος και στην συγκεκριμένη περίπτωση απαντάει με ένα ναι ή ένα όχι, χωρίς να είναι ευέλικτος και να προτείνει πιο ουσιαστικές λύσεις και τρόπους σε σχέση με αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ. Σε κάθε δε περίπτωση, το πότε κάποια εχέγγυα είναι ικανοποιητικά δεν έχει πάντα εύκολη απάντηση.

Επίσης αναφέρεται γενικά ότι θα πρέπει να χρησιμοποιούνται οι κατάλληλες μαθηματικές και στατιστικές διαδικασίες έτσι ώστε να γίνεται σωστή λήψη αποφάσεων, αλλά η γενικότητα αυτή αφήνει πολλά κενά στο τι θεωρεί ο κάθε developer κατάλληλο, χωρίς να υπάρχουν συγκεκριμένες αναφορές και ένα ειδικό πλαίσιο ανάπτυξης αυτών των διαδικασιών.

Με τα μέχρι τώρα δεδομένα γίνεται αντιληπτό ότι ο νόμος δημιουργεί ένα πολύ γενικό πλαίσιο προστασίας του πολίτη όσον αφορά τα προσωπικά τους δεδομένα και την επεξεργασία αυτών, κάνοντας χρήση των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ. Είναι αναμφίβολα πολύ σημαντικό το ότι υπάρχουν πλέον αυστηρές νομικές υποχρεώσεις για όσους πρόκειται να πραγματοποιήσουν μία τέτοιου είδους επεξεργασία, η οποία μάλιστα σε πολλές περιπτώσεις δεν είναι πλέον επιτρεπτή (αφού δεν θα πληρούνται οι εν λόγω προϋποθέσεις). Ωστόσο, είναι αμφίβολο αν απλά και μόνο μία νομική πρόβλεψη καταγραφής των

σχετικών προϋποθέσεων νόμιμης επεξεργασίας μπορεί να διασφαλίσει απόλυτα το ότι δεν θα παραβιάζονται στην πράξη θεμελιώδη δικαιώματα και ελευθερίες, αφού εκ των πραγμάτων ένα νομικό κείμενο δεν μπορεί να προσδιορίσει σαφώς του κανόνες τους οποίους τα συστήματα αυτά θα πρέπει να ακολουθούν και κατά την φάση ανάπτυξη τους αλλά και για το συνεχή έλεγχο αυτών ως προς την σωστή λειτουργία τους ή από ποιους θα ελέγχονται αυτά τα εργαλεία έτσι να εξασφαλίζεται η ευθυγράμμιση τους με νόμους, οδηγίες κτλ.

Επίσης, αυτό το οποίο φαίνεται με την ανάγνωση του GDPR είναι απαγόρευση των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ ή μάλλον η χρήση τους να είναι όσο το δυνατόν πιο περιορισμένη **[8]**.

3.5.2. Η έννοια της εκτίμησης αντίκτυπου σχετικά με τα προσωπικά δεδομένα

Σε μια προσπάθεια αποκωδικοποίησης του όρου εκτίμηση αντικτύπου σχετικά με την προστασία προσωπικών δεδομένων στον GDPR, τα 2 σημαντικά άρθρα είναι το 35 και 36 του κανονισμού, και συγκεκριμένα:

- Το άρθρο 35 του Δανονισμού, απαιτεί από τους οργανισμούς να διενεργούν τη λεγόμενη Εκτίμηση Αντικτύπου ως προς την Προστασία Δεδομένων (Data Protection Impact Assessment – DPIA) πριν από την επεξεργασία προσωπικών δεδομένων, εάν η επεξεργασία είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Ο στόχος μιας DPIA είναι ο εντοπισμός, η αξιολόγηση και ο μετριασμός των κινδύνων για την προστασία της ιδιωτικής ζωής και των δεδομένων.

  Η DPIA θα πρέπει να διενεργείται πριν από την έναρξη οποιωνδήποτε δραστηριοτήτων επεξεργασίας και θα πρέπει να διενεργείται από τον υπεύθυνο επεξεργασίας δεδομένων ή τον εκπρόσωπό του. Θα πρέπει να περιλαμβάνει συστηματική περιγραφή των εργασιών επεξεργασίας και των σκοπών της επεξεργασίας, αξιολόγηση της αναγκαιότητας και της αναλογικότητας της επεξεργασίας, αξιολόγηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των ατόμων και τα μέτρα που προβλέπονται για την αντιμετώπιση αυτών των κινδύνων.

  Ο GDPR παρέχει μια λίστα δραστηριοτήτων επεξεργασίας που είναι πιθανό να απαιτούν DPIA λόγω των υψηλών κινδύνων που απορρέουν από αυτές, όπως επεξεργασία ευαίσθητων προσωπικών δεδομένων μεγάλης κλίμακας, συστηματική παρακολούθηση ατόμων και επεξεργασία που περιλαμβάνει δημιουργία προφίλ ή αυτοματοποιημένη λήψη αποφάσεων που επηρεάζει σημαντικά τα άτομα. Ωστόσο, οι οργανισμοί

ενθαρρύνονται επίσης να διενεργούν μια DPIA σε άλλες περιπτώσεις όπου η επεξεργασία είναι πιθανό να οδηγήσει σε υψηλούς κινδύνους.

Τα αποτελέσματα της DPIA θα πρέπει να τεκμηριώνονται και ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να συμβουλεύεται την αρμόδια εποπτική αρχή εάν η DPIA υποδείξει ότι η επεξεργασία θα οδηγήσει σε υψηλό κίνδυνο που δεν μπορεί να μετριαστεί με τα προβλεπόμενα μέτρα. Σε ορισμένες περιπτώσεις, η εποπτική αρχή μπορεί να απαιτήσει από τον υπεύθυνο επεξεργασίας δεδομένων να πραγματοποιήσει ΕΑΠ ή μπορεί να παράσχει καθοδήγηση σχετικά με την καταλληλότητα των προβλεπόμενων μέτρων.

Συνολικά, η απαίτηση DPIA είναι μια σημαντική πτυχή του GDPR που βοηθά να διασφαλιστεί ότι οι οργανισμοί γνωρίζουν και αντιμετωπίζουν τους κινδύνους απορρήτου και προστασίας δεδομένων που σχετίζονται με τις δραστηριότητες επεξεργασίας τους και ότι λαμβάνουν τα κατάλληλα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών των ατόμων.

- Το άρθρο 36 του κανονισμού περιγράφει τις απαιτήσει αναφορικά με την εκπόνηση **DPIA για περιπτώσεις όπου αυτή καταδεικνύει ότι η επεξεργασία οδηγεί σε υψηλό κίνδυνο.** Ουσιαστικά, η βασική απαίτηση είναι η προηγούμενη διαβούλευση με την αρμόδια Αρχή Προστασίας Δεδομένων. Η DPIA είναι μια διαδικασία που βοηθά τους οργανισμούς να εντοπίσουν, να αξιολογήσουν και να μετριάσουν τους κινδύνους προστασίας δεδομένων ενός συγκεκριμένου έργου ή πρωτοβουλίας. Σύμφωνα με το άρθρο 35, απαιτείται ΕΑΠΔ στις ακόλουθες περιπτώσεις:
    - Επεξεργασία που είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Αυτό περιλαμβάνει δραστηριότητες επεξεργασίας που περιλαμβάνουν μεγάλες ποσότητες προσωπικών δεδομένων, την επεξεργασία ευαίσθητων δεδομένων ή τη χρήση νέων τεχνολογιών.
    - Επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων (όπως ορίζονται στο άρθρο 9 παράγραφος 1 του ΓΚΠΔ) ή προσωπικών δεδομένων που σχετίζονται με ποινικές καταδίκες και αδικήματα (όπως ορίζονται στο άρθρο 10 του ΓΚΠΔ).
    - Συστηματική παρακολούθηση μιας δημόσιας προσβάσιμης περιοχής σε μεγάλη κλίμακα.

- Μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων που σχετίζονται με ευάλωτα άτομα, όπως παιδιά.

Εάν οποιαδήποτε από αυτές τις περιστάσεις ισχύει για μια δραστηριότητα επεξεργασίας δεδομένων, ο οργανισμός πρέπει να πραγματοποιήσει DPIA πριν ξεκινήσει τη δραστηριότητα. Η DPIA θα πρέπει να περιλαμβάνει περιγραφή της δραστηριότητας επεξεργασίας, αξιολόγηση της αναγκαιότητας και της αναλογικότητας της επεξεργασίας, εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των ατόμων και μέτρα για την αντιμετώπιση αυτών των κινδύνων.

Συνολικά, το άρθρα 35 και 36 χρησιμεύουν ως σημαντικό εργαλείο για τους οργανισμούς για τον εντοπισμό και τον μετριασμό των κινδύνων προστασίας δεδομένων και τη διασφάλιση της συμμόρφωσης με τον GDPR.

Συνεχίζοντας παρακάτω με τις εισαγωγικές σκέψεις του Κανονισμού και σε αυτή την περίπτωση, βλέπουμε συγκεκριμένα τα εξής:

1) Με βάση την εισαγωγική σκέψη 84 η DPIA είναι μια διαδικασία που εξασφαλίζει σε κάθε περίπτωση ότι η επεξεργασία των προσωπικών δεδομένων του πολίτη, είναι πλήρως ευθυγραμμισμένη με τον GDPR,

2) Με βάση την εισαγωγική σκέψη 90, , σε τέτοιες περιπτώσεις η εκτίμηση αντικτύπου θα πρέπει να λαμβάνει χώρα, πριν την επεξεργασία των προσωπικών δεδομένων του πολίτη,

3) Με βάση την εισαγωγική σκέψη 91, δίνεται έμφαση στο ότι η εκτίμηση αντικτύπου θα πρέπει να λαμβάνει χώρα όταν ο όγκος των προσωπικών δεδομένων προς επεξεργασία θα είναι μεγάλος, όταν η επεξεργασία είναι μιας κλίμακας σε επίπεδο περιφέρειας, χώρας η και σε μεγαλύτερης, αλλά και σε περιπτώσεις που γίνεται επεξεργασία βιομετρικών χαρακτηριστικών, πράξεων που εμπίπτουν σε εγκλήματα κτλ.,

4) Στην εισαγωγική σκέψη 92, αναφέρεται ότι η εκτίμηση αντικτύπου θα πρέπει να λαμβάνει επίσης χώρα σε περίπτωση που υπάρχει μια κοινή πλατφόρμα επεξεργασίας των προσωπικών δεδομένων,

5) Στην εισαγωγική σκέψη 94, αναφέρεται ότι ο υπεύθυνος της επεξεργασίας θα πρέπει πρώτα να μιλάει πρώτα με την εποπτική αρχή, σε περίπτωση που η εκτίμηση αντικτύπου δείχνει ότι θίγονται ατομικές ελευθερίες των πολιτών από την επεξεργασία των προσωπικών του δεδομένων,

6) Η εισαγωγική σκέψη 95, αναφέρεται στην σχέση του εκτελούντος την επεξεργασία και του υπεύθυνου επεξεργασίας, σε σχέση πάντα με τα αποτελέσματα της εκτίμησης του αντικτύπου, και επίσης σε συνεργασία πάντα με την αρμόδια εποπτική αρχή.

Η έννοια λοιπόν αξιολόγηση αντικτύπου στην προστασία δεδομένων στην βάση του GDPR, με βάση τα όσα μελετήθηκαν παραπάνω, είναι μια διαδικασία που εκτελείται πριν την επεξεργασία των προσωπικών δεδομένων, και που έχει σαν σκοπό να εξασφαλιστεί ότι δεν θα θιγούν δικαιώματα και ελευθερίες των πολιτών.

Αναφέρεται ως μια επιπλέον δικλείδα ασφαλείας ως προς το ότι η επεξεργασία που πρόκειται να λάβει χώρα, με δεδομένα εισόδου τα προσωπικά δεδομένα των πολιτών είναι σύννομη και δεν θέτει σε κίνδυνο ατομικές ελευθερίες των πολιτών.

Ένα βασικό συμπέρασμα είναι ότι αν πρόκειται να γίνει χρήση αυτοματοποιημένου εργαλείου λήψης αποφάσεων τότε, λόγω των αναπόφευκτων υψηλών κινδύνων για τα δικαιώματα και τις ελευθερίες των προσώπων, είναι υποχρεωτική η εκπόνηση DPIA. Αυτό όμως που δεν προσδιορίζεται είναι ο τρόπος με τον οποίο θα γίνει η αξιολόγηση/αποτίμηση των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, αν δηλαδή θα πρέπει να ακολουθούνται συγκεκριμένα εργαλεία-τρόπουι, η και ακόμα ποιοι θα είναι υπεύθυνοι να διενεργούν τον έλεγχο αυτό και κατά την φάση της ανάπτυξης αυτών των εργαλείων σε συνεργασία με τους Developers, έτσι ώστε να εξασφαλιστεί η σωστή δόμηση ενός τέτοιου εργαλείου αλλά και ο μετέπειτα έλεγχος κατά την φάση χρήσης ανάλογων εργαλείων. Εξάλλου, η DPIA εφαρμόζεται σε κάθε επεξεργασία υψηλού κινδύνου – όχι μόνο σε αυτές που έχουν να κάνουν με αυτοματοποιημένα εργαλεία λήψης αποφάσεων – το οποίο σημαίνει ότι υπάρχουσες γενικές τεχνικές εκπόνησης DPIA δεν είναι προσαρμοσμένες στις ειδικές απαιτήσεις και προκλήσεις που απορρέουν από τη χρήση τέτοιων εργαλείων – και, άρα, δεν διευκολύνουν το σωστό εντοπισμό των κινδύνων και την εύρεση λύσεων.

Κεφάλαιο 4

Βιβλιογραφική Ανασκόπηση

Στο συγκεκριμένο κεφάλαιο θα ασχοληθούμε με την βιβλιογραφική ανασκόπηση, και συγκεκριμένα θα γίνει μια προσπάθεια για την συλλογή πηγών (δημοσιευμένων άρθρων, βιβλίων κτλ), που είναι σχετικά με το θέμα της παρούσας Μεταπτυχιακής Διατριβής.

Επίσης, στο παρόν κεφάλαιο θα υπάρξει αναφορά στα εργαλεία που υπάρχουν για την εκτέλεση μιας DPIA αλλά και της AIA, μέσα πάντα από σχετική βιβλιογραφία.

4.1. Αλγοριθμική Εκτίμηση επιπτώσεων

Ένα από τα πιο σημαντικά θέματα που κάποιος θα εντοπίσει για την Αλγοριθμική Εκτίμηση επιπτώσεων μέσα στην βιβλιογραφία σε μια αναζήτηση, είναι η επισκόπηση των ηθικών ζητημάτων που περιβάλλουν τους αλγόριθμους και τον αντίκτυπό τους στην κοινωνία **[22]**. Οι συγγραφείς στο [22] υποστηρίζουν ότι οι αλγόριθμοι έχουν γίνει πανταχού παρόντες στη σύγχρονη κοινωνία, επηρεάζοντας πολλές πτυχές της ζωής των ανθρώπων και ότι οι ηθικές συνέπειες της χρήσης τους πρέπει να εξεταστούν προσεκτικά.

Το εν λόγω άρθρο συζητά διάφορα ηθικά ζητήματα που σχετίζονται με τους αλγόριθμους, συμπεριλαμβανομένης της διαφάνειας, της λογοδοσίας, της δικαιοσύνης, των διακρίσεων της ιδιωτικής ζωής και της επιτήρησης του ελέγχου. Οι συγγραφείς υπογραμμίζουν τη σημασία της κατανόησης του πώς λειτουργούν οι αλγόριθμοι και πώς μπορούν να είναι μεροληπτικοί, ιδιαίτερα σε τομείς όπως η απασχόληση, ο δανεισμός και η ποινική δικαιοσύνη.

Επίσης προσδιορίζει επίσης αρκετούς βασικούς τομείς για περαιτέρω έρευνα, συμπεριλαμβανομένης της ανάπτυξης κατευθυντήριων γραμμών δεοντολογίας για τη χρήση αλγορίθμων, του ρόλου της κυβέρνησης και της βιομηχανίας στη ρύθμιση της χρήσης τους και της ανάγκης για μεγαλύτερη ευαισθητοποίηση του κοινού και συμμετοχή σε συζητήσεις σχετικά με τις ηθικές τους επιπτώσεις.

Συνολικά, το άρθρο παρέχει μια χρήσιμη εισαγωγή στο περίπλοκο και ταχέως εξελισσόμενο πεδίο της ηθικής αλγορίθμων και υπογραμμίζει την ανάγκη για συνεχή έρευνα και διάλογο για αυτά τα σημαντικά ζητήματα.

Σε ίδια τροχιά κινείται και το επόμενο άρθρο **[23]** το οποίο παρέχει μια επισκόπηση της τρέχουσας κατάστασης των οδηγιών δεοντολογίας της τεχνητής νοημοσύνης σε όλο τον κόσμο. Οι συγγραφείς υποστηρίζουν ότι καθώς η χρήση της τεχνητής νοημοσύνης γίνεται πιο διαδεδομένη, είναι σημαντικό να αναπτυχθούν ηθικές κατευθυντήριες γραμμές που μπορούν να καθοδηγήσουν την σωστή ανάπτυξη αυτών των τεχνολογιών.

Το άρθρο υπογραμμίζει επίσης τις προκλήσεις και τους περιορισμούς των υφιστάμενων κατευθυντήριων γραμμών δεοντολογίας της τεχνητής νοημοσύνης, συμπεριλαμβανομένης της έλλειψης σωστής εκτέλεσης αυτών και της δυσκολίας εξισορρόπησης των ηθικών αρχών. Οι συγγραφείς ζητούν μεγαλύτερη συνεργασία και συντονισμό μεταξύ των ενδιαφερομένων για την ανάπτυξη κατευθυντήριων γραμμών ηθικής τεχνητής νοημοσύνης, καθώς και την ανάγκη για συνεχή αξιολόγηση και αναθεώρηση αυτών των κατευθυντήριων γραμμών καθώς οι τεχνολογίες τεχνητής νοημοσύνης συνεχίζουν να εξελίσσονται.

Επίσης όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο, και συγκεκριμένα στην μελέτη του GDPR, σημαντικό ρόλο παίζει η ύπαρξη της λογοδοσίας αλλά και η σημασία αυτής στα αλγοριθμικά συστήματα λήψης αποφάσεων **[24]**. Ο συγγραφέας της εν λόγω εργασίας υποστηρίζει ότι καθώς τα αλγοριθμικά συστήματα ενσωματώνονται όλο και περισσότερο στην κοινωνία, είναι σημαντικό να διασφαλιστεί ότι αυτά τα συστήματα είναι διαφανή και υπεύθυνα στο κοινό.

Το εν λόγω άρθρο παρέχει μια επισκόπηση διαφορετικών προσεγγίσεων για τη λογοδοσία στην αλγοριθμική λήψη αποφάσεων, συμπεριλαμβανομένων νομικών πλαισίων, τεχνικών λύσεων και κατευθυντήριων γραμμών δεοντολογίας. Ο συγγραφέας υποστηρίζει ότι ενώ κάθε μία από αυτές τις προσεγγίσεις μπορεί να συμβάλει σε μεγαλύτερη υπευθυνότητα, όλες είναι περιορισμένες στην αποτελεσματικότητά τους και απαιτούν περαιτέρω ανάπτυξη.

Άξιο αναφοράς επίσης είναι και η ονομασία εμπορικών προϊόντων τεχνητής νοημοσύνης που παρουσίασαν μεροληπτική «απόδοση» **[25].** Η εν λόγω εργασία εξετάζει τον αντίκτυπο μιας τέτοιας ενέργειας σε σύνολο προϊόντων τεχνητής νοημοσύνης που παρουσιάζουν μεροληπτική απόδοση. Οι συγγραφείς υποστηρίζουν ότι μια τέτοια στρατηγική μπορεί να είναι ένα αποτελεσματικό εργαλείο για βελτίωση της δικαιοσύνης και της υπευθυνότητας των αλγοριθμικών συστημάτων.

Το άρθρο παρουσιάζει τα αποτελέσματα μιας μελέτης στην οποία οι συγγραφείς έλεγξαν αρκετά εμπορικά προϊόντα τεχνητής νοημοσύνης και κατονόμασαν δημόσια εκείνα που εμφάνισαν μεροληπτική απόδοση σε μια σειρά μετρήσεων. Στη συνέχεια, οι συγγραφείς παρακολούθησαν την ανταπόκριση των εταιρειών των οποίων τα προϊόντα ονομάστηκαν και παρατήρησαν ότι πολλές από αυτές έλαβαν μέτρα για να βελτιώσουν τη δικαιοσύνη των συστημάτων τους ως απάντηση στον δημόσιο έλεγχο.

Συνολικά, το άρθρο παρέχει μια πολύτιμη συμβολή στη συνεχιζόμενη συζήτηση σχετικά με στρατηγικές για την προώθηση της δικαιοσύνης και της λογοδοσίας στα αλγοριθμικά συστήματα, τονίζοντας την πιθανή αποτελεσματικότητα της συγκεκριμένης ενέργειας.

Επίσης σημαντικό είναι και το πώς οι άνθρωποι αντιλαμβάνονται τη δικαιοσύνη των αλγοριθμικών συστημάτων λήψης αποφάσεων **[26]**. Οι συγγραφείς υποστηρίζουν ότι ενώ οι αλγόριθμοι μπορούν να προσφέρουν πολλά οφέλη, η χρήση τους στη λήψη αποφάσεων που επηρεάζουν τη ζωή των ανθρώπων εγείρει σημαντικά ηθικά και κοινωνικά ερωτήματα.

Το άρθρο παρουσιάζει τα αποτελέσματα μιας μελέτης στην οποία οι συγγραφείς πήραν συνέντευξη από τους συμμετέχοντες σχετικά με τις αντιλήψεις τους περί δικαιοσύνης σε μια σειρά αλγοριθμικών σεναρίων λήψης αποφάσεων, συμπεριλαμβανομένων των προσλήψεων, της ασφάλισης και της ποινικής δικαιοσύνης. Οι συγγραφείς διαπίστωσαν ότι οι συμμετέχοντες είχαν μια σειρά από αντιλήψεις σχετικά με το δίκαιο αυτών των σεναρίων, με πολλούς να εκφράζουν ανησυχίες σχετικά με την πιθανότητα μεροληψίας και διάκρισης σε αλγοριθμικά συστήματα.

Το άρθρο υπογραμμίζει επίσης τη σημασία της διαφάνειας και της επεξήγησης στα αλγοριθμικά συστήματα λήψης αποφάσεων και την ανάγκη για μεγαλύτερη συμμετοχή των πολιτών στο σχεδιασμό και την ανάπτυξη αυτών των συστημάτων. Οι συγγραφείς υποστηρίζουν ότι ενώ οι αλγόριθμοι μπορούν να προσφέρουν πολλά οφέλη, πρέπει να σχεδιάζονται και να χρησιμοποιούνται με τρόπο που σέβεται την ανθρώπινη αξιοπρέπεια και προάγει την κοινωνική δικαιοσύνη.

Άλλη μια σημαντική πτυχή στα αλγοριθμικά συστήματα είναι οι «προκαταλήψεις» που μπορεί να έχουν, και που αντικατοπτρίζουν προκαταλήψεις ανθρώπων **[27]**. Στην εν λόγω εργασία, οι συγγραφείς χρησιμοποίησαν αλγόριθμους μηχανικής μάθησης για να αναλύσουν ένα μεγάλο σώμα κειμένου και να εντοπίσουν προκαταλήψεις σε συσχετίσεις λέξεων. Οι συγγραφείς διαπίστωσαν ότι το αυτοματοποιημένο σύστημα αντικατόπτριζε ανθρώπινες προκαταλήψεις, όπως στερεότυπα για το φύλο και τη φυλή. Για παράδειγμα, το σύστημα συσχέτιζε τα γυναικεία

ονόματα με την οικογένεια και τις τέχνες, ενώ τα αντρικά ονόματα συνδέονταν με την καριέρα και την επιστήμη.

Οι συγγραφείς υποστηρίζουν ότι αυτά τα ευρήματα έχουν σημαντικές επιπτώσεις για το σχεδιασμό και τη χρήση αυτοματοποιημένων συστημάτων επεξεργασίας γλώσσας, τα οποία χρησιμοποιούνται όλο και περισσότερο σε μια σειρά εφαρμογών, από την πρόσληψη έως και στα μέσα κοινωνικής δικτύωσης. Οι συγγραφείς προτείνουν ότι πρέπει να ληφθούν μέτρα για τον εντοπισμό και τον μετριασμό των προκαταλήψεων σε αυτά τα συστήματα για να διασφαλιστεί η δικαιοσύνη και να αποτραπούν οι διακρίσεις.

Επίσης αναφορά θα πρέπει να γίνει και στους διάφορους τύπους αλγορίθμων που χρησιμοποιούνται από αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ **[28]**. Στην εν λόγω εργασία οι συγγραφείς παρέχουν μια επισκόπηση διαφόρων τεχνικών μηχανικής μάθησης, όπως δέντρα αποφάσεων, νευρωνικά δίκτυα και μηχανές διανυσμάτων υποστήριξης.

Άλλη περίπτωση είναι των αλγορίθμων μηχανικής μάθησης, συμπεριλαμβανομένης της εποπτευόμενης μάθησης, της μάθησης χωρίς επίβλεψη, και παρέχει παραδείγματα για το πώς μπορούν να χρησιμοποιηθούν σε διαφορετικές εφαρμογές**[29]**.

4.2. Εργαλεία που χρησιμοποιούνται για τον υπολογισμό DPIA

Στο συγκεκριμένο σημείο θα γίνει μια προσπάθεια καταγραφής των εργαλείων που χρησιμοποιούνται για την εκπόνηση της DPIA.

Σε αναζήτηση στο διαδίκτυο αυτό που βλέπουμε είναι ότι υπάρχουν εργαλεία για την εκπόνηση της DPIA, είτε σε μορφή ερωτηματολογίων, είτε ως εφαρμογές οι οποίες άλλες είναι open source και δωρεάν είτε επί πληρωμή, και τα συγκεκριμένα εργαλεία παρέχονται είτε από φορείς είτε από μεμονωμένες εταιρείες.

Επίσης αυτό που γίνεται επίσης αντιληπτό, είναι ότι οι εφαρμογές αυτές και τα ερωτηματολόγια χωρίζονται και ως προς τον τομέα που προορίζονται, δηλαδή είτε για τον τομέα της υγείας, είτε της οικονομίας, της εκπαίδευσης κτλ.

Στο site **[9]**, βρίσκεται ένα πρότυπο (template) ερωτηματολόγιο για όποιον θέλει να εκπονήσει μια DPIA, συγκεκριμένα είναι ένα pdf ερωτηματολόγιο **[10]**, το οποίο όμως δίνει με έναν μάλλον

απλοϊκό τρόπο τι μπορεί να περιέχει ένα τέτοιου είδους ερωτηματολόγιο για την διενέργεια εκτίμησης αντικτύπου ως προς τα προσωπικά δεδομένα στα οποία θα γίνει επεξεργασία. Θα πρέπει να αναφερθεί ότι δεν υπάρχει καμία ερώτηση στο συγκεκριμένο template που να βοηθάει στην εύρεση του αντικτύπου ως προς την προστασία δεδομένων από αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ.

Το λογισμικό της Γαλλικής Αρχής Προστασίας Δεδομένων CNIL **[11]** είναι ένα εργαλείο ανοιχτού κώδικατο οποίο προσφέρει δυνατότητα εκπόνησης εκτίμησης αντικτύπου ως προς τα προσωπικά δεδομένα στα οποία θα γίνει επεξεργασία. Το εν λόγω εργαλείο είναι εύχρηστο, ενώ δίνει μία ελευθερία στον χρήστη ως προς το να καταγράψει διάφορα είδη κινδύνου αλλά εκ των πραγμάτων δεν προσφέρει την δυνατότητα ελέγχου ενός αλγοριθμικού συστήματος σε βάθος, για παράδειγμα τι αλγόριθμος χρησιμοποιείται αλλά και πως λειτουργεί.

Το λογισμικό PrivIQ **[12]**, το οποίο αναφέρει ότι είναι ευθυγραμμισμένο με τον GDPR, μπορεί να εκτελέσει PIA/DPIA, αλλά αντίστοιχα δεν έχει δυνατότητα ελέγχου ενός αλγοριθμικού συστήματος σε βάθος, για παράδειγμα τι αλγόριθμος χρησιμοποιείται αλλά και πως λειτουργεί.

Το λογισμικό DPIA Tool **[13]**, το οποίο και αυτό αναφέρει ότι είναι ευθυγραμμισμένο με τον GDPR, μπορεί να εκτελέσει DPIA αλλά και να αποφασίσει εάν χρειάζεται η διαδικασία DPIA, αλλά όπως και τα προηγούμενα δεν δίνει την δυνατότητα να εκτελέσει μια εκτίμηση αντικτύπου όταν γίνεται χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Το Πανεπιστημίο του Groningen, στα πλαίσια του προγράμματος "Human Subject Research Programme", έχει εκδώσει ένα έγγραφο **[14]**, το οποίο αναφέρει κάποιες πληροφορίες για την εκπόνηση μίας DPIA, και δίνει μια εικόνα για το πως αυτή μπορεί να λάβει χώρα.

Στα διάφορα εργαλεία για την διενέργεια της DPIA που αναφέρθηκαν παραπάνω, δεν υπάρχει καμία ειδική αναφορά για έναν ουσιαστικό έλεγχο των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, πάρα μόνο λαμβάνει υπόψιν εάν χρησιμοποιούνται αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, έτσι ώστε οι σχετικοί κίνδυνοι να το συνυπολογιστούν στην DPIA. Αυτό βέβαια είναι, με βάση και τα όσα ειπώθηκαν στο Κεφάλαιο 3, άμεσα συνυφασμένο με το γεγονός ότι μία DPIA έχει εκ των πραγμάτων γενική φύση.

Σε γενικές γραμμές αυτό που αποτυπώνεται μέσα από τα εργαλεία που χρησιμοποιούνται για τον υπολογισμό της DPIA, είναι ότι, λόγω του εγγενούς γενικού χαρακτήρα τους, δεν μπορούν να ελέγξουν ουσιαστικά και σε βάθος αυτοματοποιημένα εργαλεία λήψης αποφάσεων και

δημιουργίας προφίλ, εάν έχουν αναπτυχθεί με τους πλέον σωστούς τρόπους, και κατά συνέπεια εάν λειτουργούν σε ένα πλαίσιο όσο γίνεται ευθυγραμμισμένο με τον GDPR, έτσι ώστε να μην υπάρχει ο κίνδυνος να θιγούν ατομικές ελευθερίες και δικαιώματα των πολιτών, και να εξάγουν χρήσιμα συμπεράσματα, έτσι ώστε να χρησιμοποιηθούν και να υπάρξουν συγκεκριμένες βελτιώσεις ώστε να είναι σύννομη η χρήσης τους, και έτσι να μην θίγονται ατομικές ελευθερίες και δικαιώματα των πολιτών όταν γίνεται η χρήση τους.

4.3. Εργαλεία που χρησιμοποιούνται για την εκτέλεση Αλγοριθμικής Εκτίμησης Επιπτώσεων

Στο συγκεκριμένο σημείο θα γίνει μια προσπάθεια καταγραφής εργαλείων που χρησιμοποιούνται για την εκπόνηση Αλγοριθμικής Εκτίμησης Επιπτώσεων .

Το πρώτο είναι ένα ερωτηματολόγιο του Υπουργείου Οικονομικών του Καναδά **[18]**, που αποτελείται από 48 ερωτήσεις που καθορίζουν το ρίσκο που εισάγει η χρήση του συγκεκριμένου εργαλείου προς αξιολόγηση, και επίσης 33 ερωτήσεις για την βοήθεια του μετριασμού του ρίσκου που εισάγει η χρήση του συγκεκριμένου εργαλείου.

Το συγκεκριμένο ερωτηματολόγιο είναι ένα open source project και είναι ελεύθερη η χρήση του, το οποίο ανανεώνεται σε τακτική βάση και δίνεται η δυνατότητα όποιος θέλει και έχει την απαιτούμενη γνώση να συμβάλει στην εξέλιξη του εργαλείου αυτού το οποίο είναι διαθέσιμο και στο GitHub **[17]**.

Ένα άλλο σχετικό εργαλείο είναι το λεγόμενο AI Fairness 360 **[30]**. Πρόκειται για μια εργαλειοθήκη ανοιχτού κώδικα που αναπτύχθηκε από την IBM που παρέχει αλγόριθμους και μετρήσεις για να βοηθήσει τους προγραμματιστές να δοκιμάσουν και να μετριάσουν την προκατάληψη στα μοντέλα μηχανικής εκμάθησης τους.

Το εργαλείο What-If της Google**[31]**,εργαλείο επιτρέπει στους χρήστες να δοκιμάσουν και να οπτικοποιήσουν την απόδοση των μοντέλων μηχανικής εκμάθησης τους σε διαφορετικά υποσύνολα δεδομένων. Μπορεί να χρησιμοποιηθεί για την κατανόηση του αντίκτυπου διαφορετικών αλγοριθμικών αποφάσεων σε διαφορετικές ομάδες ανθρώπων.

Ένα άλλο εργαλείο είναι το InterpretML**[32]**,.Πρόκειται για μια εργαλειοθήκη ανοιχτού κώδικα που παρέχει μια σειρά εργαλείων για την ερμηνεία και την οπτικοποίηση των αποτελεσμάτων των μοντέλων μηχανικής εκμάθησης. Μπορεί να χρησιμοποιηθεί για να βοηθήσει στον εντοπισμό και τον μετριασμό πιθανών πηγών μεροληψίας σε αλγόριθμους.

Οι λεγόμενες κάρτες μοντέλων**[33]**είναι μια τυποποιημένη μορφή για την τεκμηρίωση της απόδοσης και του πιθανού αντίκτυπου των μοντέλων μηχανικής εκμάθησης. Έχουν σχεδιαστεί για να παρέχουν διαφάνεια και υπευθυνότητα για την αλγοριθμική λήψη αποφάσεων.

Το LIME (Local Interpretable Model-Agnostic Explanations)**[34]** είναι ένα εργαλείο που παρέχει πληροφορίες για το πώς τα μοντέλα μηχανικής μάθησης κάνουν προβλέψεις. Μπορεί να χρησιμοποιηθεί για να βοηθήσει στον εντοπισμό και τον μετριασμό των πηγών μεροληψίας στους αλγόριθμους.

Κεφάλαιο 5

Συσχέτιση της AIA με τις υποχρεώσεις που απορρέουν από τον GDPR

Σε αυτό το κεφάλαιο θα γίνει μια σύγκριση μεταξύ των διαφόρων εργαλείων λογοδοσίας του GDPR και της AIA, έτσι ώστε να αποτυπωθεί εάν ο συνδυασμός τουςμπορεί να επιφέρει μια καλύτερη προστασία και έλεγχο όταν γίνεται χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, μέσα από ένα κοινό μεθοδολογικό πλαίσιο.

5.1. Γενική αποτύπωση του GDPR σε σχέση με νέες τεχνολογίες - συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ.

Μπορεί να γίνει αντιληπτό ότι πλέον η εισαγωγή των νέων τεχνολογιών - αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ στην καθημερινή ζωή των πολιτών είναι κάτι αναπόφευκτο, λαμβάνοντας υπόψιν και τον τεράστιο όγκο δεδομένων που έχει δημιουργηθεί και διακινείται καθημερινά, κάτι που έχει σαν αποτέλεσμα ο ανθρώπινος παράγοντας να μην έχει την δυνατότητα να μπορεί να επεξεργαστεί, χωρίς την βοήθεια υπολογιστικών συστημάτων και νέων τεχνολογιών όπως το AI και το ML **[20]**.

Μελετώντας τον GDPR **[6] [19]**, όπως αποτυπώθηκε και στο Κεφάλαιο 3, μπορεί να γίνει κατανοητό επίσης ότι για νέες τεχνολογίες όπως για παράδειγμα AI και ML αλλά και για τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, δεν δημιουργείται ένα ξεκάθαρο πλαίσιο προστασίας προσωπικών και ευαίσθητων προσωπικών δεδομένων για την περίπτωση όπου γίνεται χρήση των προαναφερόμενων τεχνολογιών αλλά και εργαλείων.,

Επίσης, κατά την μελέτη του GDPR υπάρχει μια αναφορά, γενική, ως προς τις νέες τεχνολογίες και τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, χωρίς όμως αυτό να προσφέρει μια συνολική εικόνα για τον τρόπο χρήσης των εργαλείων αυτών και των νέων τεχνολογιών, δημιουργώντας ένα κατά τη γνώμη μας ένα κενό, το οποίο αποτελεί την βάση για αμφισβητήσεις, διενέξεις, και φόβο, ως προς την χρήση αυτών.

Φυσικά δεν μπορεί να υπάρξει αμφισβήτηση του GDPR ως προς την προστασία προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών, εάν γίνεται χρήση νέων τεχνολογιών και των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Συγκεκριμένα και στην βάση του GDPR, η χρήση τέτοιων τεχνικών/τεχνολογιών θα μπορούσε να είναι επιτρεπτή εφόσον:

- Δεν θίγεται η αρχή του περιορισμού του σκοπού με την χρήση των νέων τεχνολογιών και των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, δηλαδή η περαιτέρω επεξεργασία των δεδομένων που συλλέχθηκαν δεν έρχεται σε αντίθεση με τον σκοπό που συλλέχθηκαν τα δεδομένα,

- Δεν θίγεται, η αρχή της ελαχιστοποίησης δεδομένων το οποίο σημαίνει ότι δεν υφίστανται επεξεργασία περισσότερα δεδομένα από ό,τι πρέπει – ενώ, αν η αρχή της ελαχιστοποίησης απαιτεί ανωνυμοποίηση ή ψευδωνυμοποίηση των δεδομένων, αυτό θα πρέπει να υλοποιείται,

- Παρέχεται πλήρης πληροφόρηση και διαφάνεια στους πολίτες, με ό,τι έχει να κάνει με νέες τεχνολογίες και αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ,

- Υπάρχει νομική βάση συγκεκριμένη για την επεξεργασία, ιδίως η συγκατάθεση των ατόμων ή σχετική νομική υποχρέωση του υπευθύνου επεξεργασίας.

Σε γενικές γραμμές αυτό που αποτυπώνεται μελετώντας τον GDPR ως προς νέες τεχνολογίες και αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, είναι ότι ναι μεν υπάρχει αναφορά προς αυτά όπως στα άρθρα 22 και 35, αλλά πάντα στην βάση του προσδιορισμού γενικών κανόνων για την προστασία των προσωπικών δεδομένων των πολιτών και όχι στο να ελέγξουν πρακτικά τα συγκεκριμένα εργαλεία είτε στο στάδιο της ανάπτυξής τους, έτσι ώστε τυχόν ασυνέπειες του τρόπου λειτουργιάς τους να διορθωθούν πριν την χρήση τους, είτε κατά την φάση χρήσης των εργαλείων αυτών, τα οποία θα πρέπει να βρίσκονται κάτω από

συνεχή έλεγχο και να γίνονται η απαραίτητες διορθώσεις (με την χρήση patches), και με βάση πάντα τις αλλαγές που μπορεί να υπάρχουν στην κείμενη νομοθεσία ως προς τον τρόπο λειτουργίας των εργαλείων αυτών είτε με βάση τον GDPR, είτε με κανονισμούς που θα δημοσιεύονται, είτε με οδηγίες κτλ.

5.2. Γενική αποτύπωση AIA σε σχέση με νέες τεχνολογίες - συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ.

Έχοντας προαναφέρει τις σχετικές προβλέψεις του GDPR και το τι ειδικότερα αναφέρει για τις νέες τεχνολογίες και τα αυτοματοποιημένα εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, σε σχέση με το πλαίσιο της προστασίας, έχει γίνει αντιληπτό ότι η αναφορά είναι ένα γενικό πλαίσιο, χωρίς φυσικά να μπορεί να ελέγξει τα συγκεκριμένα εργαλεία σε βάθος και κατ' επέκταση να εξάγει χρήσιμες και σημαντικές πληροφορίες.

Η AIA αναφέρεται ως μια ειδικής μορφής διασφάλιση της λογοδοσίας **[16],** σε ό,τι έχει να κάνει με νέες τεχνολογίες (AI και ML) και τα αυτοματοποιημένα εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, τα οποία χρησιμοποιούνται για την επεξεργασία προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών.

Το σημαντικό με την AIA είναι ότι θέτει ένα πλαίσιο λογοδοσίας σε σχέση με τις νέες τεχνολογίες και τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, ως προς την σχεδίαση, την συντήρηση και τον χειρισμό τους, γεγονός που δημιουργεί την ευθύνη για την εξήγηση, τον εντοπισμό, και την βελτίωση σε περίπτωση που τα προαναφερόμενα βλάπτουν τους πολίτες, κατά την διάρκεια της επεξεργασίας των προσωπικών τους και ευαίσθητων προσωπικών δεδομένων τους, αλλά και με βάση των αποφάσεων που λαμβάνουν.

Βέβαια αυτό που θα πρέπει να αναφερθεί είναι από την φάση της σχεδίασης ενός εργαλείου AIA, μέχρι και την φάση της χρήσης του, εμπλέκονται πολλοί (ατομικά ή ομαδικά) και γίνεται αντιληπτό ότι θα πρέπει να υπάρχει μια ισορροπημένη και ξεκάθαρη επικοινωνία, μέσα σε μια ομάδα που απαρτίζεται από διάφορες ειδικότητες με το ανάλογο μερίδιο ευθύνης, για τα σωστά αποτελέσματα, και συγκεκριμένα για την δημιουργία ενός εργαλείου που θα μπορεί να δώσει χρήσιμα συμπεράσματα για τυχόν νέες τεχνολογίες και αυτοματοποιημένα εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ που θα χρησιμοποιηθούν για την επεξεργασία προσωπικών και ευαίσθητων προσωπικών δεδομένων των πολιτών, και με βάση αυτά τα συμπεράσματα να

μπορέσουν να γίνουν όλες οι απαραίτητες διορθωτικές αλλαγές σε περίπτωση που υπάρχει κάποια παραβίαση του τρόπου λειτουργίας των νέων τεχνολογιών και των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Η εφαρμογή των εργαλείων ΑΙΑ δεν θα επιλύσει πλήρως τα προβλήματα τα οποία γεννιούνται με την χρήση νέων τεχνολογιών και των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, αλλά θα παρέχουν ένα πιο ειδικό πλαίσιο μέσα από το οποίο θα εξάγονται χρήσιμα συμπεράσματα, τα οποία θα βοηθήσουν στην ενημέρωση αλλά και στον εμπλουτισμό της γνώσης, έτσι ώστε να δημιουργείται η βάση για την ανάπτυξη νέων τεχνολογιών και αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ που δεν θα παραβιάζουν ατομικά δικαιώματα και ελευθερίες, και επίσης θα δημιουργείτε το κατάλληλο πλαίσιο για έναν εποικοδομητικό διάλογο που σαν αποτέλεσμα θα έχει να ενισχύεται η βάση η οποία προαναφέρθηκε.

Τα σημαντικότερα σημεία στα οποία θα βοηθήσει η ΑΙΑ, είναι τα εξής;

- Να δίνονται όλες οι απαραίτητες πληροφορίες στους πολίτες, όσον αφορά νέες τεχνολογίες και αυτοματοποιημένα εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ που μπορεί να επηρεάζουν την ζωή τους, και σε τι βαθμό,

- Μέσα από τις πληροφορίες - γνώση που συλλέγονται από την χρήση των εργαλείων ΑΙΑ, να αυξάνεται ο αριθμός των ειδικών που μπορούν να αξιολογήσουν νέες τεχνολογίες και αυτοματοποιημένα εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ,

- Ένα συνεχές πλαίσιο λογοδοσίας, που σαν αποτέλεσμα έχει την συνεχή αξιολόγηση και έλεγχο των νέων τεχνολογιών και των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, με αποτέλεσμα τον άμεσο εντοπισμό προβλημάτων και την επίλυση αυτών,

- Και το πιο σημαντικό ότι το πολίτες έχουν την απαραίτητη γνώση να καταλάβουν τι είναι τα συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ, πώς επηρεάζουν την ζωή τους, έτσι ώστε να είναι σε θέση από μόνοι τους να μπορούν να καταλάβουν πότε υπάρχει παραβίαση των ατομικών τους δικαιωμάτων και ελευθεριών τους.

Όπως έχει προαναφερθεί οι ΑΙΑ δεν είναι θα λύσουν πλήρως τα προβλήματα που υπάρχουν και εμφανίζονται από την χρήση των νέων τεχνολογιών και των αυτοματοποιημένων εργαλείων

λήψης αποφάσεων και δημιουργίας προφίλ, αλλά θα αποτελέσουν εκείνα τα πρακτικά εργαλεία για την απόκτηση χρήσιμης πληροφορίας από το στάδιο ανάπτυξης των συστημάτων αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ αλλά και από τη μετέπειτα χρήσης τους, που θα αποτελέσει βάση για τις οποίες διορθωτικές κινήσεις θα πρέπει να γίνουν, και ειδικά στο στάδιο την ανάπτυξης αυτών και πριν την χρήση τους.

Επίσης πολύ σημαντικό είναι ότι η AIA, θα προσφέρει γνώση, που σημαίνει ότι εάν διασφαλιστεί ότι γνωστοποιείται σωστά, ξεκάθαρα και αμερόληπτα,, θα βοηθήσει και τους απλούς πολίτες να καταλάβουν τι είναι τα συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ, πώς και πόσο επηρεάζουν την ζωή τους, το οποίο θα τους δώσει την δυνατότητα ακόμα και μέσα από ειδικά φόρουμ που μπορούν να σχεδιαστούν να εκφράζουν την άποψη τους, διότι όπως αποτυπώνεται η βελτίωση των νέων τεχνολογιών και των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ δεν βασίζεται στην άποψη μόνο των ειδικών που έχουν την απαραίτητη γνώση αλλά στο σύνολο πολιτών, με αποτέλεσμα να δημιουργείται μια συνολική εικόνα για τα συγκεκριμένα συστήματα.

Παράδειγμα ενός τέτοιου εργαλείου για τον έλεγχο αλγοριθμικών συστημάτων είναι ερωτηματολόγιο του Υπουργείου Οικονομικών του Καναδά **[18]**, (βλ. και Κεφάλαιο 4),το οποίο εισάγει αμιγώς τεχνικές ερωτήσεις και κατά συνέπεια μια σε βάθος έρευνα – έλεγχο στο πώς τα συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ λειτουργούν, μέσα από ένα σύνολο 13 ενοτήτων με ερωτήσεις, και συγκεκριμένα:

Στην ενότητα που ζητάει πληροφορίες σχετικά με το σύστημα (About the system),

- Πληροφορίες που έχουν να κάνουν με το προς χρήση σύστημα, όπως για παράδειγμα εάν υπάρχει ανάλυση κειμένου και ομιλίας,
- Αναγνώριση εικόνων και αντικειμένων.

Στην ενότητα που ζητάει πληροφορίες σχετικά με τον προς χρήση αλγόριθμο (About the Algorithm),

- Εάν ο αλγόριθμος που θα χρησιμοποιηθεί θα είναι ένα «εμπορικό μυστικό», και άρα δεν υπάρχουν πληροφορίες για το πως λειτουργεί,
- Επίσης ο αλγόριθμος που θα χρησιμοποιηθεί θα είναι δύσκολος να εξηγηθεί το πως λειτουργεί, και κατά συνέπεια απλοί πολίτες χωρίς την απαραίτητη τεχνογνωσία, θα τους είναι δύσκολο να καταλάβουν επίσης το πως λειτουργεί.

Στην ενότητα που ζητάει πληροφορίες σχετικά με το εάν η απόφαση εμπίπτει με συγκεκριμένες κατηγορίες δεδομένων (About the Decision),

- Στο τομέα της υγείας,
- Στο τομέα της οικονομίας,
- Στην περίπτωση που έχει να κάνει με την έκδοση αδειών (σε διάφορους τομείς).

Στην ενότητα που ζητάει πληροφορίες για το είδος των πληροφοριών που θα υποβληθούν σε επεξεργασία (About the Data),

- Όπως για παράδειγμα εάν το σύστημα για την επεξεργασία θα χρησιμοποιήσει προσωπικές πληροφορίες των πολιτών, που χρήζουν ειδικής μεταχείρισης,
- Ποιος είναι υπεύθυνος για την επεξεργασία των προσωπικών πληροφοριών,
- Το συγκεκριμένο σύστημα θα έχει αλληλεπίδραση με κάποιο άλλο σύστημα.

Γίνεται αντιληπτό λοιπόν ότι έστω και μέσα από τις λιγοστές προαναφερόμενες ερωτήσεις, στα πλαίσια μιας AIA, ότι οι πληροφορίες οι οποίες θα εξαχθούν θα είναι όχι απλά πολύτιμες αλλά κάτι περισσότερο, αφού θα δώσουν γνώση και για τους ειδικούς αλλά και για τους απλούς πολίτες, για το πως λειτουργούν τα συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ, εάν θα πρέπει να βελτιωθεί και να διορθωθεί κάτι και σε τι έκταση, αλλά και γνώση στους απλούς πολίτες για το είναι αυτά τα εργαλεία και πως μπορεί να επηρεάσουν την ζωή τους.

5.3. Ανάπτυξη ενός ενοποιημένου μεθοδολογικού πλαισίου με χρήση του GDPR και AIA.

Με τα όσα έχουν αναφερθεί μέχρι τώρα, γίνεται αντιληπτό ότι ο GDPR λειτουργεί στην βάση της προστασίας των ατομικών δικαιωμάτων και ελευθεριών των πολιτών, και η φύση του είναι να προστατεύσει τους πολίτες, μέσα από ένα γενικό πλαίσιο.

Απόρροια του ανωτέρω είναι ότι ναι μεν αναφέρονται υποχρεώσεις που πρέπει να τηρούν οι οργανισμοί, εταιρείες, και δημόσιοι φορείς όταν κάνουν χρήση νέων τεχνολογιών και αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, αλλά μέσα από ένα πλαίσιο που μπορεί να αναφερθεί ως μη σαφώς προσδιορισμένο λόγω της μη εξειδίκευσης των κατάλληλων μηχανισμών που θα θέσουν

ένα πιο συγκροτημένο και ξεκάθαρο πλαίσιο προστασίας όταν γίνεται η χρήση νέων τεχνολογιών και αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Εμφανές λοιπόν είναι ότι αυτό το γενικό πλαίσιο δεν μπορεί να υπάρξει απόλυτη εγγύηση για μια ορθή προστασία σε ό,τι έχει να κάνει με την χρήση νέων τεχνολογιών και αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, και αυτό γίνεται ακόμα πιο εμφανές όταν ληφθεί υπόψη ότι όχι απλά υπάρχουν συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ, αλλά ότι υπάρχουν και χρησιμοποιούνται σε πολλούς τομείς της καθημερινότητας και αυτό συνεπάγεται ότι ανάλογα σε ποιον τομέα χρησιμοποιούνται διαφέρουν και ως προς στο είδος των προσωπικών πληροφοριών που θα επεξεργαστούν για να εξάγουν μια απόφαση η να συγκροτήσουν ένα προφίλ πολίτη. Εξάλλου, οι τεχνολογίες «προχωρούν» πολύ πιο γρήγορα από τους νομοθέτες: ο GDPR οριστικοποιήθηκε το 2016, ενώ έκτοτε έχουν υπάρξει σημαντικές εξελίξεις σε επιστήμες όπως η ανάλυση δεδομένων και η τεχνητή νοημοσύνη.

Οπότε γίνεται αντιληπτό ότι αυτή η ποικιλομορφία των πληροφοριών που τα συστήματα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ έρχονται να επεξεργαστούν, ίσων δημιουργεί ένα επιπλέον πρόβλημα που έχει να κάνει με το ότι θα πρέπει να χρησιμοποιούνται ποικιλόμορφα εργαλεία AIA για τον έλεγχο των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, ανάλογα με το είδος των πληροφοριών που θα επεξεργαστούν τα συγκεκριμένα εργαλεία, έτσι ώστε να εξασφαλίζεται η σωστή τους λειτουργία και είτε οι αποφάσεις τους είτε η δημιουργία προφίλ να είναι όσο το δυνατόν πιο «δίκαιες» και ταυτόχρονα να εξασφαλίζεται η προστασία ατομικών δικαιωμάτων και ελευθεριών των πολιτών.

Με βάση όλα τα παραπάνω ενισχύεται η άποψη ότι ο GDPR, με τα εργαλεία που παρέχει, δεν μπορεί να προσφέρει την δέουσα, αυστηρή και ξεκάθαρη προστασία όταν γίνεται χρήση συστημάτων αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ.

Από την άλλη πλευρά με τα όσα έχουν αναφερθεί για την AIA, γίνεται εμφανές ότι παρέχουν ένα πιο εξειδικευμένο πλαίσιο ελέγχου ως προς την χρήση νέων τεχνολογιών και αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Η χρήση της έχει σαν σκοπό να ελέγξει σε βάθος τις συγκεκριμένες νέες τεχνολογίες και αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ από την φάση

ανάπτυξης τους αλλά και κατά την διάρκεια της χρήσης αυτών των συστημάτων, και το σημαντικό είναι μπορεί να προβλέψει πιθανά προβλήματα κατά την φάση ανάπτυξης τους και την επίλυση αυτών πριν την χρήση τους, και έτσι να αποφευχθούν τυχόν παραβιάσεις που εμπίπτουν στην προστασία των προσωπικών δεδομένων, όπως αναφέρονται στον GDPR.

Αμέσως γίνεται αντιληπτό ότι ακόμα και εάν δεν αναφέρεται πουθενά η AIA μέσα στον GDPR, υπάρχει μια κατά κάποιο τρόπο «αόρατη» σχέση που εάν μετουσιωθεί σε ορατή, και συγκεκριμένα να υπάρξουν οι απαραίτητες αλλαγές στον GDPR, όπως για παράδειγμα να γίνεται σαφές ότι θα γίνεται χρήση εργαλείων AIA σε περιπτώσεις νέων τεχνολογιών και αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, θα υπάρξει ένα πιο ολοκληρωμένο, βελτιωμένο και ευέλικτο πλαίσιο προστασίας.

Θα υπάρχει λοιπόν ένας έλεγχος των συστημάτων αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ χρησιμοποιώντας την AIA, που προφανώς η βάση του κάθε ένα από αυτά τα εργαλεία της AIA θα είναι η φύση των προς επεξεργασία πληροφοριών, με το σκεπτικό της ποικιλομορφίας των πληροφοριών που υπάρχουν δεδομένου ότι τα συστήματα αυτά χρησιμοποιούνται σε πολλούς τομείς της κοινωνίας, και σε δεύτερο στάδιο με βάση την εξαγωγή των απαραίτητων πληροφοριών ύστερα από τους ελέγχους που θα έχουν γίνει να καθορίζεται εάν υπάρχει παραβίαση προσωπικών δεδομένων και εάν σε τι βαθμό στη βάση του GDPR μέσω μιας DPIA.

Εδώ θα πρέπει να αναφερθεί ότι γίνεται αντιληπτό επίσης ένα πολύ σημαντικό στοιχείο, και συγκεκριμένα αυτό της βελτίωσης και της αποτελεσματικότητας των εργαλείων λογοδοσίας του GDPR αλλά και των εργαλείων AIA, αφού μέσα από την συγκεκριμένη αλληλεπίδραση και συνεργασία θα προκύψουν σημαντικές πληροφορίες, οι οποίες θα αποτελέσουν την βάση για τις απαραίτητες βελτιώσεις – συμπληρώσεις μέσα στον GDPR αλλά και στο τρόπο λειτουργίας των εργαλείων AIA.

Η αποτίμηση μέχρι εδώ που διαφαίνεται είναι ότι προφανώς δεν υπάρχει άρνηση στην χρήση νέων τεχνολογιών και αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, αρκεί να υπάρχει εκείνο το πλαίσιο που κατά την χρήση τους θα εξασφαλίζεται η σωστή λειτουργία τους και η μη παραβίαση ατομικών δικαιωμάτων και ελευθεριών των πολιτών, και συνεπώς η επιτυχία του συγκεκριμένου στόχου δεν είναι άλλο από την συνεργασία είτε σε επίπεδο ανθρώπων είτε σε επίπεδο νόμων-εργαλείων.

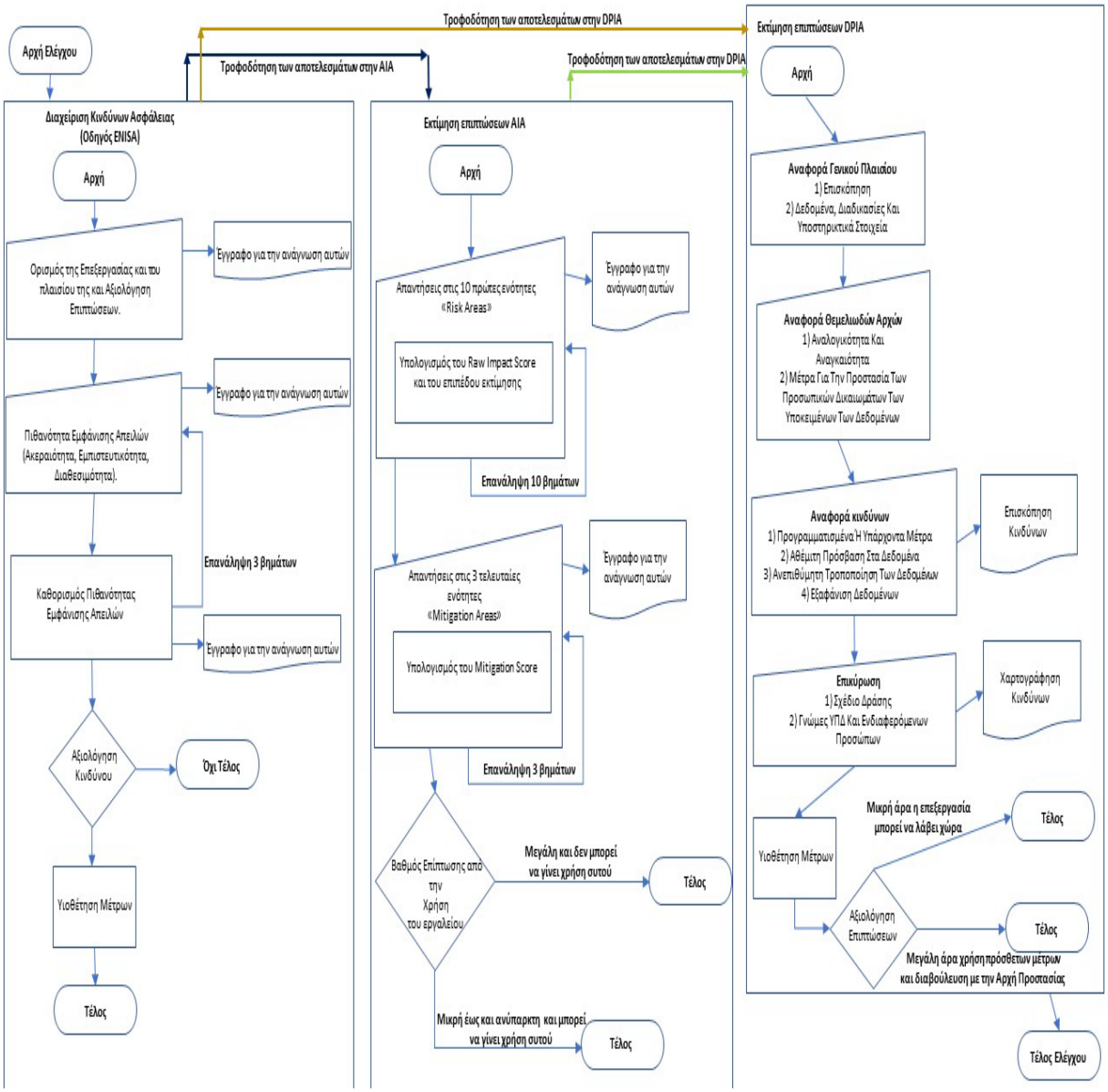
Κεφάλαιο 6 –

Μελέτη περίπτωσης

Όπως έχει ήδη αναφερθεί, θα ακολουθήσει μία ρεαλιστική μελέτη περίπτωσης (Υποθετικό Σενάριο) στο Δημόσιο Τομέα, και συγκεκριμένα ενός αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, που θα μπορούσε να χρησιμοποιηθεί από φορείς του Υπουργείου Μετανάστευσης και Ασύλου στα πλαίσια της παραχώρησης ασύλου στους αιτούντες άσυλο.

Στα πλαίσια της μελέτης περίπτωσης τα βήματα που θα ακολουθηθούν θα είναι τα εξής:

- Εκπόνηση security risk analysis
- Εκπόνηση AIA
- Εκπόνηση DPIA, όπου για την εκτέλεσή της λαμβάνονται υπόψη οι αποφάσεις που ήδη ελήφθησαν στα Α και Β, όπως φαίνεται και παρακάτω (εικόνα 6.1),



Εικόνα 6.1: Γραφική αναπαράσταση των ελέγχων.

Μια συνοπτική ανάλυση των παραπάνω σταδίων που αναφέρθηκαν είναι η εξής:

- Οι μεθοδολογίες διαχείρισης κινδύνων ασφάλειας (security risk analysis), εστιάζουν αποκλειστικά σε εκτίμηση κινδύνων ασφαλείας (ήτοι κίνδυνοι για απώλεια εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας),
- Οι AIA εστιάζουν σε κινδύνους για δικαιώματα και ελευθερίες από επεξεργασίες που αφορούν χρήση συστημάτων AI για αυτοματοποιημένη λήψη αποφάσεων,
- Η DPIA είναι ένα γενικό πλαίσιο εκτίμησης αντικτύπου για την προστασία των δεδομένων, που αφορά οποιαδήποτε επεξεργασία υψηλού κινδύνου και καλύπτει και ζητήματα ασφάλειας αλλά και ζητήματα θεμελιωδών ελευθεριών και δικαιωμάτων.

6.1. Περιγραφή του σεναρίου

Η πορεία της αίτησης ενός αιτούντος η μιας αιτούσας για άσυλο, με τον τρόπο που γίνεται έως τώρα, είναι μια χρονοβόρα διαδικασία η οποία περνάει από πολλά στάδια και στο κάθε στάδιο μπορεί να αλλάξει αρκετούς υπαλλήλους, μέχρι στην έκδοση της τελικής απόφασης (ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4939 ΦΕΚ Α 111/10.6.2022).

Από την πρώτη ημέρα, που ο αιτών ή η αιτούσα θα φθάσει στην Ελλάδα μπορεί να περάσει ένα μεγάλο χρονικό διάστημα, για να βγει η τελική απόφαση παραχώρησης ή όχι ασύλου.

Ενδεικτικά αναφέρονται τα στάδια:

- Έλεγχος του αιτούντος ή της αιτούσας για COVID,
- Εάν είναι αρνητικός η αρνητική Καταγραφή-Ταυτοποίηση, εάν είναι θετικός ή θετική τίθεται σε καραντίνα,
- Στάδιο της Συνέντευξης, κατά την οποία ο αιτών ή η αιτούσα αναφέρει τους λόγους για τους οποίους ζητάει άσυλο,
- Παραλαβή Απόφασης
    - Εάν είναι θετική, παραχώρηση άδειας διαμονής και ταξιδιωτικά έγγραφα,
    - Εάν είναι αρνητική, προσφυγή 2^{ου} βαθμού,
- Τελική απόφαση.

Το συγκεκριμένο αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ, από την πρώτη καταγραφή θα λαμβάνει αποφάσεις, βάσει των οποίων θα εξαρτάται εάν η αίτηση του αιτούντος ή της αιτούσας για άσυλο θα προχωράει στα επόμενα στάδια εξέτασης.

Η λήψη απόφασης στην οποία θα φθάνει το συγκεκριμένο αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ, θα βασίζεται σε ένα μεγάλο αριθμό προσωπικών και ευαίσθητων προσωπικών δεδομένων των αιτούντων για άσυλο, όπως για παράδειγμα χώρα προέλευσης, φύλο, θρησκεία, οικογενειακή κατάσταση, πολιτικές

πεποιθήσεις, υγεία κτλ, και αμέσως γίνεται αντιληπτό ότι η ανάπτυξη και χρήση ενός τέτοιου εργαλείου μόνο εύκολη υπόθεση δεν είναι, όταν θα πρέπει να λάβει αποφάσεις σημαντικές για το μέλλον ενός ανθρώπου (έστω και αν, σύμφωνα με τις προβλέψεις του άρθρου 22 του GDPR, οι τελικές αποφάσεις θα πρέπει να λαμβάνονται τελικά από άνθρωπο και να μη γίνονται δεκτές χωρίς ανθρώπινη κρίση οι αυτοματοποιημένες αποφάσεις).

Το συγκεκριμένο αυτοματοποιημένο εργαλείο λήψης αποφάσεων θα χρησιμοποιεί, βάσει του υποθετικού σεναρίου μας, αλγόριθμο RNN (recurrent neural network και δεν θα γίνει κάποια περεταίρω ανάλυση αυτού καθώς ξεφεύγει από τα πλαίσια της παρούσας διατριβής), ο οποίος είναι ένας τύπος αλγορίθμου βαθιάς μάθησης που χρησιμοποιείται συνήθως σε εργασίες επεξεργασίας φυσικής γλώσσας, και έτσι τα διαθέσιμα δεδομένα που θα περιλαμβάνουν δεδομένα κειμένου, όπως έγγραφα ή δηλώσεις από αιτούντες άσυλο, θα μπορούν να αναλυθούν για την εξαγωγή σχετικών πληροφοριών και για να γίνουν προβλέψεις.

Σε όλα τα παραπάνω θα πρέπει να γίνει αναφορά για την χρήση υπολογιστικών συστημάτων είτε παρωχημένης τεχνολογίας είτε με όχι τις κατάλληλες δικλείδες ασφαλείας και υπαλλήλων όχι τόσο εξοικειωμένων με την τεχνολογία.

6.2. Παράγοντες που επηρεάζουν την επεξεργασία

Άξιοι αναφοράς είναι οι παράγοντες που θα επηρεάσουν την διαδικασία της επεξεργασίας των προσωπικών και ευαίσθητων προσωπικών δεδομένων, και κατά συνέπεια το αποτέλεσμα της απόφασης που θα λάβει το αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ.

Συγκεκριμένα αυτοί είναι:

- Δηλώσεις ψευδών στοιχείων των αιτούντων άσυλο, οπότε αμέσως γίνεται αντιληπτό ότι θα πρέπει να υπάρχουν οι απαραίτητες δικλείδες ασφαλείας για την αποφυγή λανθασμένων αποφάσεων που κατά επέκταση θα λάβει το αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ,
- Περιστατικά τα οποία μπορεί να λάβουν χώρα κατά την διαμονή των αιτούντων άσυλο, και αφότου έχει ήδη χρησιμοποιηθεί το αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ και έχει λάβει μια απόφαση, με

αποτέλεσμα η απόφαση να είναι λανθασμένη, παραδείγματα τέτοιων περιπτώσεων:

- αν σε άλλο μέλος της οικογένειες έχει ήδη γίνει δεκτό το αίτημά του.

6.3. Υπεύθυνος επεξεργασίας

Στην συγκεκριμένη μελέτη περίπτωσης Υπεύθυνος Επεξεργασίας, έτσι όπως ορίζεται από το νομικό-κανονιστικό πλαίσιο, θα είναι ο ίδιος ο φορέας και οφείλει αρχικά να ερευνήσει αν απαιτείται διενέργεια "Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων" (ΕΑΠΔ) για τη συγκεκριμένη επεξεργασία.

Δεδομένου ότι πρόκειται για μια επεξεργασία προσωπικών και ευαίσθητων προσωπικών δεδομένων μεγάλης κλίμακας, και λαμβάνοντας υπόψιν το τι αναφέρει ο GDPR (περιπτώσεις της παραγράφου 3 του άρθρου 35), σε περιπτώσεις επεξεργασίας προσωπικών και ευαίσθητων προσωπικών δεδομένων μιας τέτοιας κλίμακας, θα πρέπει να διενεργηθεί μια Εκτίμηση Αντικτύπου, και μάλιστα είναι υποχρέωση όπως ρητά αναφέρεται στον GDPR.

Εν συνεχεία, επειδή δεν έχουμε απλά να κάνουμε με μια επεξεργασία προσωπικών και ευαίσθητων προσωπικών δεδομένων, αλλά με μια επεξεργασία η οποία θα λάβει χώρα με την χρήση ενός αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ το οποίο θα αναπτυχθεί, θα πρέπει να ελεγχθεί και ο τρόπος λειτουργίας του συγκεκριμένου εργαλείου, μέσω της AIA.

Σε όλα τα παραπάνω θα πρέπει να αναφερθεί ξανά ότι για το υποθετικό σενάριό μας έχουμε κάνει τις εξής (ρεαλιστικές) παραδοχές:

- Γίνεται χρήση υπολογιστικών συστημάτων είτε παρωχημένης τεχνολογίας είτε με όχι κατάλληλες δικλείδες ασφαλείας,
- Υπάρχουν υπάλληλοι όχι τόσο εξοικειωμένοι με την τεχνολογία

6.3.1. Εκπόνηση διαχείρισης κινδύνων ασφαλείας

Στα πλαίσια μια επεξεργασίας προσωπικών και ευαίσθητων προσωπικών δεδομένων και μάλιστα μεγάλης κλίμακας, σύμφωνα και με την κείμενη νομοθεσία του GDPR, πρέπει σε πρώτη φάση να γίνει μια αξιολόγηση κινδύνων ασφαλείας, για το κατά πόσο ατομικά δικαιώματα και ελευθερίες των πολιτών θίγονται από μια τέτοια επεξεργασία.

Στα πλαίσια της αξιολόγησης αυτής, θα χρησιμοποιηθεί ο οδηγός του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας ENISA**[21]**, που είναι ένα σύνολο από οδηγίες, για το πως θα γίνει αυτή η αξιολόγηση. Ο λόγος που επελέγη, στο πλαίσιο της έρευνάς μας, η συγκεκριμένη μεθοδολογία είναι το ότι είναι προσανατολισμένη ακριβώς σε κινδύνους ασφάλειας για περιπτώσεις επεξεργασιών προσωπικών δεδομένων (και όχι γενικά για ασφάλεια κάθε είδους δεδομένων, όπως είναι προσανατολισμένες άλλες κλασικές μεθοδολογίες διαχείρισης κινδύνων ασφάλειας – π.χ. ISO 27001 **[https://www.iso.org/isoiec-27001-information-security.html]** και Octave **[https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html]**).

Η μέθοδος αυτή αξιολόγησης αποτελείται από 5 βήματα και συγκεκριμένα:

- Ορισμός της Επεξεργασίας και του πλαισίου της,
- Αξιολόγηση Επιπτώσεων,
- Πιθανότητα εμφάνισης Απειλών,
- Αξιολόγηση Κινδύνου,
- Υιοθέτηση Μέτρων Ασφάλειας

6.3.1.1. Ορισμός της επεξεργασίας της και του πλαισίου της

Σε αυτό το βήμα θα πρέπει να αναφερθούν πληροφορίες όπως τα δεδομένα προς επεξεργασία, ο σκοπός της, το υποκείμενο των δεδομένων, τα μέσα που θα χρησιμοποιηθούν στην εκτέλεση της επεξεργασίας.

Η καταγραφή αυτή μπορεί να γίνει με την χρήση πίνακα, όπως αυτού που ακολουθεί.

Πληροφορίες επεξεργασίας για τους αιτούντες άσυλο	
Σκοπός επεξεργασίας	Έκδοση απόφασης για το εάν ο αιτών ή η αιτούσα θα λάβει άσυλο
Μέσα επεξεργασίας	Ηλεκτροτεχνικός εξοπλισμός στα κατά τόπους περιφερειακά γραφεία ασύλου και πρώτης υποδοχής
Που λαμβάνει χώρα η επεξεργασία	Στα κατά τόπους περιφερειακά γραφεία ασύλου πρώτης υποδοχής
Προσωπικά δεδομένα προς επεξεργασία	Προσωπικά στοιχεία (όνομα, επίθετο, φύλο, ηλικία, τηλέφωνο), δεδομένα υγείας, πολιτικές και θρησκευτικές

	πεποιθήσεις, χώρα διαμονής, οικογενειακή κατάσταση, βιομετρικά δεδομένα και άλλα
Υποκείμενο δεδομένων	Οι αιτούντες άσυλο
Παραλήπτες δεδομένων	Διάφοροι δημόσιοι φορείς, βάσει των σχετικών διατάξεων

Πίνακας 6.1: Πληροφορίες επεξεργασίας για τους αιτούντες άσυλο

6.3.1.2. Αξιολόγηση επιπτώσεων

Το επόμενο βήμα είναι να υπολογισθεί ο αντίκτυπος που θα έχει στο υποκείμενο της επεξεργασίας πιθανή απώλεια στην Εμπιστευτικότητα, στην Ακεραιότητα και τη Διαθεσιμότητα των προσωπικών και ευαίσθητων προσωπικών δεδομένων που υφίστανται επεξεργασία.

Για να υπολογισθεί ο συγκεκριμένος αντίκτυπος, βάσει μιας συγκεκριμένης κλίμακας και συγκεκριμένα σε επίπεδα (low, medium, high, very high).

Ακεραιότητα των πληροφοριών

Έχει να κάνει με την μη μεταβολή των πληροφοριών από άτομα που δεν έχουν εξουσιοδότηση.

Με βάση την επεξεργασία που πρόκειται να γίνει στα προσωπικά και ευαίσθητα προσωπικά δεδομένα των αιτούντων άσυλο, γίνεται αντιληπτό ότι μια μεταβολή σε αυτά εκούσια η ακούσια, θέτει σε πολύ μεγάλο κίνδυνο το αποτέλεσμα της απόφασης για το εάν θα λάβουν άσυλο ή όχι.

Η απόφαση αυτή έχει να κάνει με το μέλλον της ζωή τους και ως εκ τούτου λαμβάνοντας υπόψιν όλα τα παραπάνω, μια απώλεια ακεραιότητας των πληροφοριών θα μπορούσε να τεθεί στο επίπεδο διαβάθμισης VERY HIGH.

Απώλεια Εμπιστευτικότητας

Έχει να κάνει με το να μην μπορούν να έχουν πρόσβαση στις πληροφορίες άτομα που δεν έχουν εξουσιοδότηση.

Μια τέτοια περίπτωση αποκάλυψης των προσωπικών και ευαίσθητων προσωπικών δεδομένων των αιτούντων άσυλο, σε μη εξουσιοδοτημένα άτομα μπορεί να θέσουν σε

κίνδυνο δυσμενούς και άνισης μεταχείρισης, αλλά ακόμα και της σωματικής ακεραιότητας των αιτούντων, λόγω, π.χ. αποκάλυψης δεδομένων φυλετικής προέλευσης, εάν ληφθεί υπόψιν ότι υπάρχουν κοινότητες με τα δικά τους πιστεύω, πολιτικές και θρησκευτικές πεποιθήσεις κτλ. με ακραίες επιδιώξεις.

Για παράδειγμα υπάρχουν εθνικότητες που δεν δέχονται την ομοφυλοφιλία, η οποία τιμωρείται με θάνατο.

Μετά από τα παραπάνω, το επίπεδο στην απώλεια της εμπιστευτικότητας τίθεται στο VERY HIGH.

Απώλεια Διαθεσιμότητας

Η συγκεκριμένη απώλεια έχει να κάνει με το να είναι προσβάσιμες οι πληροφορίες ανά πάσα ώρα και στιγμή, διότι σε περίπτωση που δεν είναι αυτό θα δημιουργήσει σοβαρό πρόβλημα στους υπαλλήλους στην εκτέλεση των καθημερινών τους καθηκόντων.

Το παραπάνω θα έχει σαν αποτέλεσμα, να καθυστερούν οι διαδικασίες για την έκδοση απόφασης ασύλου, και αυτό θα έχει αντίκτυπο στους αιτούντες που θα πρέπει να διαμένουν σε δομές φιλοξενίας, και μερικές φορές σε όχι τόσο καλές συνθήκες, εάν στο μεσοδιάστημα της απώλειας υπάρχουν και νέες αφίξεις.

Μετά από τα παραπάνω, το επίπεδο στην απώλεια της διαθεσιμότητας τίθεται στο HIGH.

Ο συνολικός αντίκτυπος σε αυτή τη συγκεκριμένη περίπτωση καθορίζεται από το υψηλότερο επίπεδο διαβάθμισης που εντοπίστηκε.

ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ		
Ακεραιότητα	**Εμπιστευτικότητας**	**Διαθεσιμότητας**
VERY HIGH	VERY HIGH	HIGH

Πίνακας 6.2: Εκτίμηση Επιπτώσεων

Άρα ο βαθμός του αντικτύπου, σύμφωνα με τα όσα ορίζει σχετικώς η μεθοδολογία του ENISA, είναι VERY HIGH.

6.3.1.3. Πιθανότητα εμφάνισης απειλών

Στο βήμα αυτό θα γίνει μια συνολική αποτύπωση των απειλών που μπορεί να υπάρξουν στο περιβάλλον επεξεργασίας των προσωπικών και ευαίσθητων προσωπικών δεδομένων των αιτούντων άσυλο, αλλά και της πιθανότητας εμφάνισης αυτών.

Υπάρχουν 4 στάδια ερωτήσεων, σαφώς καθορισμένα, όπου το καθένα ελέγχει συγκεκριμένες παραμέτρους, και συγκεκριμένα:

- Το δίκτυο και τους τεχνικούς πόρους (υλικό και λογισμικό),
- Τις διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων,
- Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας,
- Στον τομέα και την κλίμακα της επεξεργασίας.

Δίκτυο & Τεχνικοί Πόροι:

Αξιολόγηση της πιθανότητα εμφάνισης απειλής μέσω Δικτύου και Τεχνικών πόρων:

1) Πραγματοποιείται οποιοδήποτε μέρος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω του διαδικτύου;

Τα προσωπικά και ευαίσθητα προσωπικά δεδομένα των αιτούντων άσυλο, θα είναι σε ψηφιακή μορφή μιας και θα καταχωρούνται αμέσως στα πληροφοριακά συστήματα των κατά τόπους ΠΓΑ (Περιφερειακά Γραφεία Ασύλου) αλλά θα κρατείται και φυσικός φάκελος του αιτών ή της αιτούσας.

Πρόσβαση σε αυτά μπορεί να έχουν είτε διαδικτυακά είτε μέσω Intranet, αλλά υπάρχει και η δυνατότητα της απομακρυσμένης σύνδεσης μέσω διαφορών εργαλείων.

Επίσης, πρόσβαση σε αυτά μπορεί να υπάρξει και από την ύπαρξη Shared Drive (είτε με την χρήση AD είτε local).

2) Είναι δυνατή η παροχή πρόσβασης σε εσωτερικό αρχείο δεδομένων προσωπικού χαρακτήρα μέσω του διαδικτύου;

Ναι αφού όπως αναφέρθηκε μπορεί να υπάρξει απομακρυσμένη σύνδεση είτε μέσω διαδικτύου, είτε μέσω Intranet, είτε μέσω διαφορών εργαλείων, είτε Shared Drive (είτε με την χρήση AD είτε local).

3) Είναι το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα διασυνδεδεμένο με άλλο εξωτερικό ή εσωτερικό πληροφοριακό σύστημα ή υπηρεσία;

Ναι υπάρχει η διασύνδεση με άλλα πληροφοριακά συστήματα, μιας και θα πρέπει όλα τα στοιχεία που δηλώνουν οι αιτούντες άσυλο αλλά και οι αποφάσεις να είναι προσβάσιμες και από άλλους δημόσιους φορείς, οι οποίοι θα πρέπει να έχουν πρόσβαση σε αυτές τις πληροφορίες.

Ενδεικτικά αναφέρονται φορείς όπως Αστυνομία, Λιμενικό.

4) Μπορούν μη εξουσιοδοτημένα άτομα να έχουν εύκολα πρόσβαση στο περιβάλλον του συστήματος επεξεργασίας δεδομένων;

Ναι το φυσικό περιβάλλον αυτή την στιγμή είναι, με βάση το σενάριό μας, μια μεγάλη αδυναμία, και ως αποτέλεσμα μπορεί να αποτελέσει ένα κενό ασφαλείας που μπορεί κάποιος σχετικά εύκολα να εκμεταλλευτεί, και να έχει μη εξουσιοδοτημένη πρόσβαση.

5) Το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα έχει σχεδιαστεί, υλοποιηθεί ή συντηρείται χωρίς να ακολουθεί τις σχετικές βέλτιστες πρακτικές;

Τα συστήματα επεξεργασίας στα κατά τόπους ΠΓΑ και γραφεία πρώτης υποδοχής δεν ακολουθούν, με βάση το σενάριό μας, βέλτιστες πρακτικές συντήρησης, αφού υπάρχουν υπολογιστές παλιάς γενιάς, για παράδειγμα μη υποστήριξη bit locker για την κρυπτογράφηση του σκληρού δίσκου, αλλά και επίσης με λειτουργικά που δεν υποστηρίζονται πλέον από τον κατασκευαστή όπως για παράδειγμα Windows XP και Windows 7.

Έχοντας σαν αναφορά τα παραπάνω ερωτήματα που θέτει η μεθοδολογία ENISA μπορεί να γίνει μια πρώτη καταγραφή των ευπαθειών και απειλών που σχετίζονται με το Δίκτυο και τους Τεχνικούς Πόρους και είναι οι εξής:

Αιτία/Ευπάθεια	Απειλή
Δυνατότητα απομακρυσμένης εκτέλεσης της επεξεργασίας (remote desktop)	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου) ή/και παράνομης πρόσβασης/θέασης των αρχείων
Δυνατότητα σύνδεσης κακόβουλου χρήστη στο πληροφοριακή σύστημα που εκτελείται η επεξεργασία μέσω του Intranet	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου), Κοινολόγηση προσωπικών δεδομένων
Δυνατότητα διασύνδεσης του πληροφοριακού συστήματος με άλλα πληροφοριακά συστήματα, μέσω δικτύου	Διαδικτυακή πρόσβαση μη εξουσιοδοτημένου χρήστη, Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου), Κοινολόγηση προσωπικών δεδομένων
Έλλειψη περιορισμών στη χρήση εφαρμογών διαμοιρασμού αρχείων (πχ dropbox, onedrive κλπ)	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού (μέσω διαδικτύου), τροποποίηση των αρχείων, δημιουργία πλαστών αρχείων
Δυνατότητα να εισέλθουν στο χώρο επεξεργασίας και άτομα που δε σχετίζονται με αυτή	Κοινολόγηση προσωπικών δεδομένων (λόγω αμέλειας κλειδώματος του υπολογιστή κατά την απουσία του εκτελούντος της επεξεργασία), Πρόσβαση μη εξουσιοδοτημένου χρήστη (απουσία ελέγχου εισόδου στο χώρο)
Παρωχημένος τεχνολογικός εξοπλισμός, που δε συντηρείται βάσει βέλτιστων πρακτικών	Απώλεια προσωπικών δεδομένων λόγω αστοχίας του τεχνολογικού εξοπλισμού

Πίνακας 6.3: Καταγραφή των ευπαθειών και απειλών που σχετίζονται με το Δίκτυο και τους Τεχνικούς Πόρους

Με βάση όλα τα παραπάνω, μπορεί να υπολογισθεί η πιθανότητα εμφάνισης μια απειλής, στο κομμάτι του «Δίκτυο & Τεχνικοί Πόροι», σύμφωνα με τα όσα ορίζει η μεθοδολογία του ENISA.

Τομέας Εκτίμησης	Πιθανότητα	
Δίκτυο & Τεχνικοί Πόροι	**Επίπεδο**	**Σκορ**
	Χαμηλή	1
	Μεσαία	2
	Μεγάλη	3

Πίνακας 6.4: Πιθανότητα εμφάνισης απειλής

Με βάση όλα τα προαναφερόμενα και δεδομένου ότι όλες οι απαντήσεις στις προηγούμενες ερωτήσεις είναι καταφατικές, το σκορ που λαμβάνει το να εμφανιστεί μια απειλή στο τομέα «Δίκτυο & Τεχνικοί Πόροι» είναι το 3, και το επίπεδο Μεγάλη.

Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων:

Αξιολόγηση της πιθανότητας εμφάνισης απειλής μέσω των Διαδικασίων/διεργασιών που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων:

1) Είναι οι ρόλοι και οι ευθύνες όσον αφορά την επεξεργασία των προσωπικών δεδομένων σαφώς καθορισμένοι;

Με βάση το σενάριό μας, δεν είναι ξεκάθαροι οι ρόλοι αυτών που εκτελούν την επεξεργασία, και μάλιστα σε πολλές περιπτώσεις έχουμε την συχνή αλλαγή καθηκόντων των υπαλλήλων, χωρίς σαφώς καταγεγραμμένες διαδικασίες, που αυτό δημιουργεί μια μη σταθερή και ξεκάθαρη κατάσταση για το ποιος/οι θα εκτελεί/ούν την επεξεργασία.

2) Είναι σαφώς καθορισμένο το ποιος θα κάνει χρήση του δικτύου, του συστήματος και των φυσικών πόρων εντός του οργανισμού που εκτελείται η επεξεργασία;

Και πάλι, με βάση το σενάριό μας, δεν υπάρχουν σαφείς οδηγίες για το ποιος θα κάνει χρήση του δικτύου, η των πληροφοριακών συστημάτων, και κατά επέκταση δεν τίθεται περιορισμός.

Σαν αποτέλεσμα μπορεί να θεωρηθεί, για το σενάριό μας, ότι το σύνολο των υπαλλήλων εντός των ΠΓΑ και γραφείων πρώτης υποδοχής να έχουν πρόσβαση και στο δίκτυο αλλά και στα πληροφοριακά συστήματα.

3) Επιτρέπεται στους εργαζόμενους να φέρνουν και να χρησιμοποιούν τις δικές τους συσκευές για να συνδεθούν στο σύστημα επεξεργασίας των προσωπικών δεδομένων;

Και πάλι εδώ θεωρούμε το δυσμενέστερο, από πλευράς ασφάλειας δεδομένων, σενάριο – δηλαδή ότι δεν υπάρχει καμία πολιτική που να το απαγορεύει αυτό.

4) Επιτρέπεται στους εργαζόμενους να μεταφέρουν, να αποθηκεύουν ή να επεξεργάζονται με άλλο τρόπο δεδομένα προσωπικού χαρακτήρα εκτός των εγκαταστάσεων του οργανισμού;

Ομοίως με ανωτέρω, θεωρούμε ότι δεν υπάρχει ούτε εδώ καμία πολιτική που να το απαγορεύει αυτό, και επίσης σε πολλές περιπτώσεις οι υπάλληλοι χρησιμοποιούν προσωπικές φορητές συσκευές αποθήκευσης, και κατά συνέπεια δεν μπορεί να αποκλειστεί ότι κάποιος υπάλληλος μπορεί να μεταφέρει πληροφορίες και εκτός των εγκαταστάσεων ενός ΠΓΑ ή ενός γραφείου πρώτης υποδοχής.

5) Μπορούν οι δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα να διεξάγονται χωρίς δημιουργία αρχείων καταγραφής;

Σε κάποιες από τις δραστηριότητες κατά την φάση της επεξεργασίας των προσωπικών και ευαίσθητων προσωπικών δεδομένων υπάρχουν αρχεία καταγραφής αλλά σε κάποιες όχι.

Έχοντας σαν αναφορά τα παραπάνω ερωτήματα, μπορούμε να γίνει μια πρώτη καταγραφή των ευπαθειών και απειλών που σχετίζονται με τις Διαδικασίες/Διεργασίες της επεξεργασίας και είναι οι εξής:

Αιτία/Ευπάθεια	**Απειλή**
Έλλειψη ελέγχου ως προς τη χρήση του δικτύου και των πόρων κατά την εκτέλεση της επεξεργασίας	Αστοχία συστήματος και αδυναμία ολοκλήρωσης της επεξεργασίας λόγω κακής χρήσης πόρων
Προσβολή του συστήματος από κακόβουλο λογισμικό που προήλθε από τη σύνδεση στο δίκτυο ήδη "μολυσμένης" προσωπικής συσκευής χρήστη (USB, Laptop κλπ.)	Απώλεια προσωπικών δεδομένων από κακόβουλο λογισμικό, δυσλειτουργία συστήματος/απώλεια διαθεσιμότητας υπηρεσιών ή/και αρχείων
Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού μέσω αφαιρούμενων μέσων αποθήκευσης (USB, φορητός σκληρός δίσκος)	Μεταφορά αρχείων προσωπικών δεδομένων εκτός οργανισμού από κακόβουλο χρήστη
Έλλειψη μηχανισμού καταγραφής (logging)	Μη δυνατότητα διερεύνησης περιστατικών ασφάλειας (για παράδειγμα, Αλλοίωση ή

	διαγραφή των δεδομένων εισόδου μη εξουσιοδοτημένου χρήστη)

Πίνακας 6.5: Καταγραφή των ευπαθειών και απειλών που σχετίζονται με τις Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων

Με βάση όλα τα παραπάνω, μπορεί να υπολογισθεί η πιθανότητα εμφάνισης μια απειλής, στο τομέα του «Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων».

Τομέας Εκτίμησης	**Πιθανότητα**	
Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων	**Επίπεδο**	**Σκορ**
	Χαμηλή	1
	Μεσαία	2
	Μεγάλη	3

Πίνακας 6.6: Πιθανότητα εμφάνισης απειλής

Με την ίδια λογική όπως αναφέρθηκε και προηγουμένως, το σκορ που λαμβάνει το να εμφανιστεί μια απειλή στο τομέα «Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων» είναι το 3, και το επίπεδο Μεγάλη.

Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας:

Αξιολόγηση της πιθανότητας εμφάνισης απειλής μέσω των διαφορετικών τμημάτων και ατόμων που συμμετέχουν στη διαδικασία επεξεργασίας:

1) Πραγματοποιείται η επεξεργασία δεδομένων προσωπικού χαρακτήρα από μη καθορισμένο αριθμό υπαλλήλων;

Ναι, και όπως έχουμε προαναφέρει και σε προηγούμενο ερώτημα λόγω της συχνής αλλαγής των καθηκόντων των υπαλλήλων του ΠΓΑ, ανάλογα με τις συχνές και αναγκαίες αλλαγές στο λεγόμενο workflow, δεν υπάρχει ούτε συγκεκριμένος αριθμός υπαλλήλων που διενεργούν την επεξεργασία αλλά και ούτε συγκεκριμένοι υπάλληλοι.

2) Εκτελείται οποιοδήποτε μέρος της διαδικασίας επεξεργασίας δεδομένων από εργολάβο/συνεργάτη (εκτελών την επεξεργασία δεδομένων);

Με βάση το σενάριό μας, δεν υπάρχει εκτελών την επεξεργασία. Η οποιαδήποτε επεξεργασία διενεργείται από υπαλλήλους εντός του φορέα και συγκεκριμένα των ΠΓΑ και γραφείων πρώτης υποδοχής,

3) Είναι οι υποχρεώσεις των μερών που εμπλέκονται στην επεξεργασία δεδομένων σαφώς καθορισμένες;

Η απάντηση στο συγκεκριμένο ερώτημα, λαμβάνοντας υπόψιν τις απαντήσεις στα προηγούμενα ερωτήματα, είναι όχι.

4) Είναι το προσωπικό που εμπλέκεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα εξοικειωμένο με θέματα ασφάλειας πληροφοριών;

Θα θεωρήσουμε και εδώ, για το σενάριό μας, ότι συντρέχει η δυσμενέστερη περίπτωση, δηλαδή ότι η απάντηση είναι όχι, και μάλιστα ότι δεν λαμβάνουν χώρα κάποια ειδικά σεμινάρια, έτσι ώστε οι υπάλληλοι να αποκτήσουν όλοι την απαραίτητη γνώση που έχει να κάνει με θέματα ασφάλειας πληροφοριών.

5) Τα πρόσωπα/μέρη που εμπλέκονται στην επεξεργασία δεδομένων αμελούν να αποθηκεύουν ή/και να καταστρέφουν με ασφάλεια τα δεδομένα προσωπικού χαρακτήρα;

Για το σενάριό μας θεωρούμε ότι κατά κανόνα γίνεται ασφαλής καταστροφή εγγράφων, καθώς και ψηφιακών μέσων. Ωστόσο, μπορούμε να θεωρήσουμε ότι κάποιες φορές ενδέχεται - εκ παραδρομής - να μη γίνεται χρήση των καταστροφέων εγγράφων, με αποτέλεσμα να υπάρχει μεγάλος κίνδυνος το να μπορέσει να βρει κάποιος έγραφα μη κατεστραμμένα που περιέχουν προσωπικά και ευαίσθητα προσωπικά δεδομένα των αιτούντων άσυλο.

Αιτία/Ευπάθεια	**Απειλή**
Αμέλεια καταστροφής του φυσικού αρχείου από τους χρήστες, ενώ έχει ολοκληρωθεί ο σκοπός επεξεργασίας του ή δε χρειάζεται για τους σκοπούς της επεξεργασίας	Έκθεση προσωπικών δεδομένων σε μη εξουσιοδοτημένα άτομα
Έλλειψη κατάρτισης του προσωπικού σε βασικά θέματα ασφάλειας	Μόλυνση υπολογιστών από ιούς που θα προέλθει από ενέργεια ενός χρήστη, χωρίς φυσικά δόλο

Έλλειψη ελέγχου ως προς τη χρήση του δικτύου και των πόρων κατά την εκτέλεση της επεξεργασίας	Αστοχία συστήματος και αδυναμία ολοκλήρωσης της επεξεργασίας λόγω έλλειψης πόρων

Πίνακας 6.7: Καταγραφή των ευπαθειών και απειλών που σχετίζονται με «Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας»

Με βάση όλα τα παραπάνω, μπορεί να υπολογισθεί η πιθανότητα εμφάνισης μια απειλής, στο τομέα του «Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας».

Τομέας Εκτίμησης	**Πιθανότητα**	
Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας	**Επίπεδο**	**Σκορ**
	Χαμηλή	1
	Μεσαία	2
	Μεγάλη	3

Πίνακας 6.8: Πιθανότητα εμφάνισης απειλής

Με την ίδια λογική όπως αναφέρθηκε και προηγουμένως, το σκορ που λαμβάνει το να εμφανιστεί μια απειλή στο τομέα «Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας» είναι το 3, και το επίπεδο Μεγάλη.

Τομέας και κλίμακα της επεξεργασίας:

Αξιολόγηση της πιθανότητα εμφάνισης απειλής βάσει του τομέα και της κλίμακας της επεξεργασίας:

1) Θεωρείτε ότι ο τομέας που δραστηριοποιείται ο φορέας είναι επιρρεπής σε κυβερνοεπιθέσεις;

Ο τομέας των υπηρεσιών Ασύλου δεν αποτελεί βασικό στόχο κυβερνοεπιθέσεων αφού δεν έχουν υπάρξει αναφορές για κάποια κυβερνοεπίθεση, αλλά δεδομένης της δραματικής αύξησης των κυβερνοεπιθέσεων τα τελευταία χρόνια και λαμβάνοντας υπόψιν απαντήσεις σε προηγούμενα ερωτήματα, όπως ότι χρησιμοποιείται απαρχαιωμένος εξοπλισμός αλλά και free προγράμματα, υπάρχει μεγάλος κίνδυνος στο μέλλον να αποτελέσει στόχος κυβερνοεπιθέσεων.

2) Έχει υποστεί ο φορέας οποιαδήποτε κυβερνοεπίθεση ή άλλου είδους παραβίαση της ασφάλειας τα τελευταία δύο χρόνια;

Μπορούμε να θεωρήσουμε, για το σενάριό μας, ότι έχουν υπάρξει μολύνσεις μηχανημάτων από ιούς μέσω του διαδικτύου, αλλά ιδίως από χρήστες που χρησιμοποιούν μολυσμένα φορητά μέσα αποθήκευσης.

3) Έχετε λάβει οποιεσδήποτε κοινοποιήσεις ή/και καταγγελίες σχετικά με την ασφάλεια του πληροφοριακού συστήματος που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων κατά το τελευταίο έτος;

Σε συνάφεια και με την ερώτηση 1, θεωρούμε ότι δεν έχει υπάρξει κάποια καταγγελία, που να αναφέρει κάτι τέτοιο.

4) Θεωρείτε η συγκεκριμένη επεξεργασία, αποτελεί επεξεργασία δεδομένων μεγάλης κλίμακας;

Η συγκεκριμένη επεξεργασία θεωρείται από τις πλέον μεγάλες σε κλίμακα επεξεργασία, λαμβάνοντας υπόψιν ότι υπάρχουν προσωπικά και ευαίσθητα προσωπικά δεδομένα προς επεξεργασία, που έχουν να κάνουν με χιλιάδες ανθρώπους, από κάθε μεριά της γης.

5) Υπάρχουν βέλτιστες πρακτικές ασφάλειας για τον συγκεκριμένο τομέα υπηρεσιών που δεν έχουν ακολουθηθεί επαρκώς;

Δεν υπάρχουν βέλτιστες πρακτικές, επομένως δεν μπορεί να αποτυπωθεί εάν και ποιες έχουν εφαρμοστεί πλήρως και ποιες όχι.

Η πιθανότητα εμφάνισης απειλής είναι ΥΨΗΛΗ, καθώς αφορά σε μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, και πρόκειται να υλοποιηθεί σε πληροφοριακά συστήματα που βρίσκονται σε δίκτυο που έχει εμφανίσει σημεία τρωτότητας.

Με βάση όλα τα παραπάνω, μπορεί να υπολογισθεί η πιθανότητα εμφάνισης μια απειλής, στην κατηγορία «Τομέας και κλίμακα της επεξεργασίας».

Τομέας Εκτίμησης	**Πιθανότητα**	
Τα διαφορετικά τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας	**Επίπεδο**	**Σκορ**
	Χαμηλή	1
	Μεσαία	2
	Μεγάλη	3

Πίνακας 6.9: Πιθανότητα εμφάνισης απειλής

Με την ίδια λογική όπως αναφέρθηκε και προηγουμένως, το σκορ που λαμβάνει το να εμφανιστεί μια απειλή στο τομέα «Τομέας και κλίμακα της επεξεργασίας» είναι το 3, και το επίπεδο Μεγάλη.

Λαμβάνοντας υπόψιν όλες τις απαντήσεις στα παραπάνω ερωτήματα, και με βάση τον οδηγό-πρότυπο του ENISA, έχουμε:

ΤΟΜΕΑΣ ΑΞΙΟΛΟΓΗΣΗΣ	**ΠΙΘΑΝΟΤΗΤΑ**	
	Διαβάθμιση	**SCORE**
Δίκτυο & Τεχνικοί Πόροι	Χαμηλή	1
	Μέτρια	2
	Υψηλή	3
Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων	Χαμηλή	1
	Μέτρια	2
	Υψηλή	3
Τμήματα και άτομα που συμμετέχουν στη διαδικασία επεξεργασίας	Χαμηλή	1
	Μέτρια	2
	Υψηλή	3
Τομέας & Κλίμακα επεξεργασίας	Χαμηλή	1
	Μέτρια	2
	Υψηλή	3
Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής		**12**

Πίνακας 6.10: Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής

Ακολουθώντας το πρότυπο ENISA, η πιθανότητα εμφάνισης απειλής συνολικά, χαρακτηρίζεται ως ΥΨΗΛΗ.

Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής	**Επίπεδο Πιθανότητας Εμφάνισης Απειλής**
4 - 5	Χαμηλό
6 - 8	Μέτριο
9 - 12	Υψηλό

Πίνακας 6.11: Συνολικό Άθροισμα Πιθανότητας Εμφάνισης Απειλής/ Επίπεδο Πιθανότητας Εμφάνισης Απειλής

η πιθανότητα εμφάνισης απειλής συνολικά, χαρακτηρίζεται ως ΥΨΗΛΗ.

6.3.1.4. Αξιολόγηση κινδύνου

Βάσει της αξιολόγησης που πραγματοποιήθηκε και δεδομένου ότι ο συνολικός κίνδυνος για τη συγκεκριμένη περίπτωση θεωρείται ΥΨΗΛΟΣ, κρίνεται απαραίτητη η υιοθέτηση απαραίτητων μέτρων ασφάλειας για τον μετριασμό/αποφυγή των κινδύνων που απειλούν τη διαδικασία της επεξεργασίας.

Επίπεδο Επίπτωσης				
Πιθανότητα Εμφάνισης Απειλής		**Χαμηλό**	**Μέτριο**	**Υψηλό**
	Χαμηλό			
	Μέτριο			
	Υψηλό			✓

Πίνακας 6.12: Επίπεδο Επίπτωσης/ Πιθανότητα Εμφάνισης Απειλής

Η παραπάνω ανάλυση κινδύνων με βάση το πρότυπο του ENISA, είχε σαν σκοπό να παρουσιάσει την δεδομένη στιγμή την κατάσταση που επικρατεί, στο υποθετικό μας σενάριο, σε ένα ΠΓΑ αλλά και πρώτης υποδοχής, ως προς την πιθανότητα εμφάνισης κινδύνου (συνολικού αλλά και κατά τομέα). Απώτερος σκοπός είναι ότι τα αδύναμα σημεία σε θέματα ασφάλειας επεξεργασίας θα χρησιμοποιηθούν για την εκπόνηση μελέτης της εκτίμησης αντικτύπου ως προς την προστασία των προσωπικών και ευαίσθητων προσωπικών δεδομένων όπως ορίζει ο GDPR.

6.3.1.5. Υιοθέτηση Μέτρων Ασφαλείας

Καθώς ο μεγαλύτερος κίνδυνος αφορά το Δίκτυο, τον εξοπλισμό, αλλά και την μη γνώση των χρηστών σε θέματα ασφάλειας, τα μέτρα που επιβάλλεται να παρθούν αφορούν κυρίως:

Νέο τεχνολογικό εξοπλισμό (server και τερματικά), για να ελαχιστοποιηθούν οι πιθανότητες αστοχίας του υλικού

Κατάλληλο λογισμικό προκειμένου να δημιουργήσει ένα ασφαλές περιβάλλον επεξεργασίας των δεδομένων

Προμήθεια συστημάτων παρακολούθησης (monitoring) της κίνησης του δικτύου προς αποφυγή κυβερνοεπιθέσεων

Εγκατάσταση κάποιου συστήματος που θα παρέχει υπηρεσίες καταλόγου στο δίκτυο (πχ Active Directory)

Απομακρυσμένη πρόσβαση θα είναι επιτρεπτή μόνο από σαφώς καταγεγραμμένους έμπιστους χρήστες, μόνο μέσω εικονικού ιδιωτικού δικτύου (VPN).

Εκπόνηση διαδικασιών διαχείρισης προσωπικού, που μεταξύ άλλων θα προβλέπει το τι θα συνεπάγεται τυχόν μετακίνηση προσωπικού ως προς την επικαιροποίηση των δικαιωμάτων πρόσβασης

Οι ρόλοι και οι ευθύνες που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να ορίζονται σαφώς και να κατανέμονται σύμφωνα με την πολιτική ασφαλείας,

Θα πρέπει να εκχωρούνται συγκεκριμένα δικαιώματα ελέγχου πρόσβασης σε κάθε ρόλο (που εμπλέκεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα) σύμφωνα με την αρχή της ανάγκης γνώσης,

Εφαρμογή πολιτικών ασφαλείας έτσι ώστε οι χρήστες να μην είναι σε θέση να μπορούν να αλλάξουν ρυθμίσεις όπως για παράδειγμα του antivirus, να κάνουν απεγκατάσταση εφαρμογών,

Την εκπαίδευση των χρηστών σε θέματα ασφάλειας

Επιπλέον πρέπει να υιοθετηθούν και συγκεκριμένες πολιτικές που θα πρέπει να ακολουθούν οι χρήστες και θα αφορούν:

Τη χρήση ασφαλών κωδικών πρόσβασης (password)

Τη χρήση αφαιρούμενων μέσων αποθήκευσης

Την ασφάλεια δικτύου και ασύρματου δικτύου του φορέα

Την χρήση προσωπικών υπολογιστών αλλά και κινητών

Αυτά είναι κάποια από τα ενδεικτικά μέτρα τα οποία αναφέρονται στον οδηγό του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας ENISA**[21]**.

6.4. Εκτίμηση επιπτώσεων με την χρήση της AIA

Στο συγκεκριμένο στάδιο θα εκπονηθεί μια AIA, με σκοπό τον υπολογισμό της εκτίμησης των επιπτώσεων, μιας επεξεργασίας προσωπικών και ευαίσθητων προσωπικών δεδομένων των αιτούντων άσυλο με την χρήση ενός μελλοντικού αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ.

Για την συγκεκριμένη εκτίμηση θα χρησιμοποιηθεί το εργαλείο της καναδικής κυβέρνησης, το οποίο αναφέρθηκε ήδη σε προηγούμενο κεφάλαιο **[1]**, και επιλέχθηκε το συγκεκριμένο εργαλείο γιατί μέσα από ένα πλήρες σύνολο ερωτήσεων καταφέρνει τα εξής:

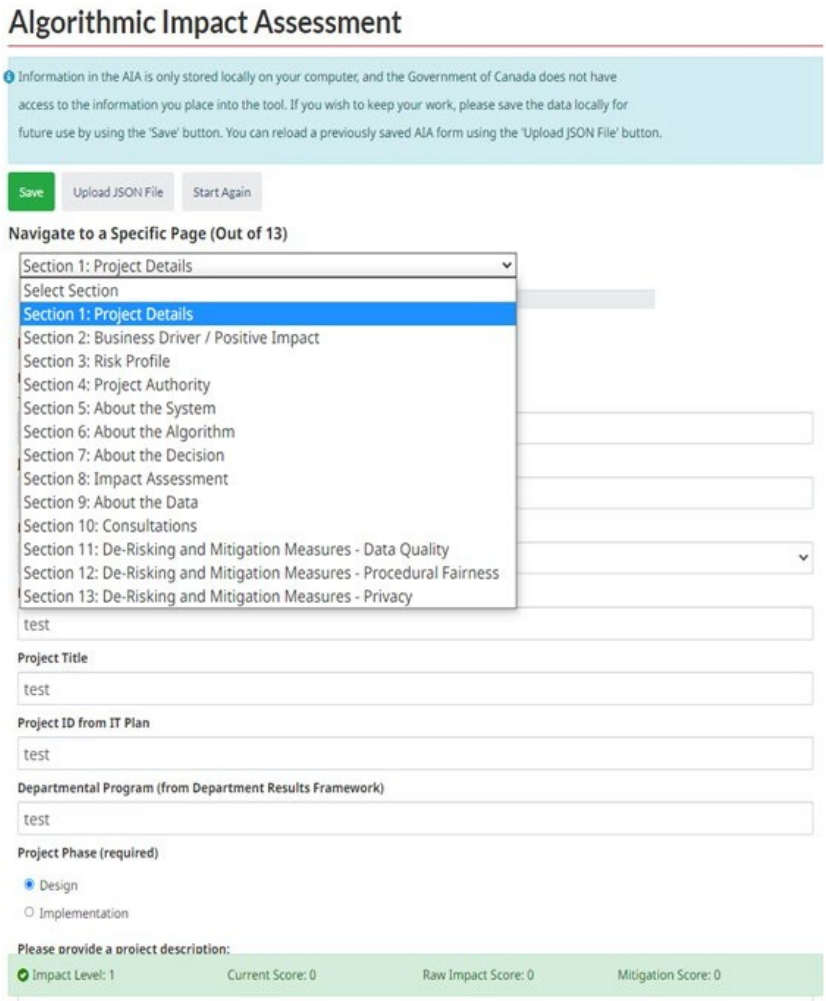
- Διασφάλιση της συμμόρφωσης με νόμους και κανονισμούς: Οι οργανισμοί που χρησιμοποιούν συστήματα τεχνητής νοημοσύνης πρέπει να συμμορφώνονται με νόμους και κανονισμούς που προστατεύουν τα ανθρώπινα δικαιώματα, αποτρέπουν τις διακρίσεις και διασφαλίζουν δικαιοσύνη. Χρησιμοποιώντας το συγκεκριμένο εργαλείο, οι οργανισμοί μπορούν να αξιολογήσουν τους πιθανούς κινδύνους και τις επιπτώσεις των συστημάτων τεχνητής νοημοσύνης τους, να προσδιορίσουν τομείς ανησυχίας και να λάβουν τα κατάλληλα μέτρα για την αντιμετώπιση τυχόν ζητημάτων.
- Προώθηση της ηθικής στην ανάπτυξη τεχνητής νοημοσύνης: Το εργαλείο βοηθά τους οργανισμούς να δώσουν προτεραιότητα σε ηθικά ζητήματα κατά την ανάπτυξη και την ανάπτυξη συστημάτων τεχνητής νοημοσύνης. Εντοπίζοντας πιθανές επιπτώσεις στα ανθρώπινα δικαιώματα, τη διαφορετικότητα και την ένταξη, οι οργανισμοί μπορούν να λάβουν μέτρα για να ελαχιστοποιήσουν τη βλάβη και να μεγιστοποιήσουν τα οφέλη.
- Ενίσχυση της εμπιστοσύνης και της διαφάνειας: Η χρήση του εργαλείου μπορεί να βοηθήσει τους οργανισμούς να ενισχύσουν την διαφάνεια σχετικά με τα συστήματα τεχνητής νοημοσύνης τους και τις πιθανές επιπτώσεις σε άτομα και κοινότητες. Αυτό μπορεί να βοηθήσει στην οικοδόμηση εμπιστοσύνης με τα ενδιαφερόμενα μέρη και να προωθήσει πιο ανοιχτή και υπεύθυνη ανάπτυξη τεχνητής νοημοσύνης.
- Μετριασμός κινδύνων και μείωση ευθύνης: Με τη διεξαγωγή μιας AIA, οι οργανισμοί μπορούν να εντοπίσουν και να μετριάσουν πιθανούς κινδύνους και βλάβες που σχετίζονται με τα συστήματα τεχνητής νοημοσύνης τους. Αυτό μπορεί να μειώσει τον κίνδυνο νομικής ευθύνης και βλάβης της φήμης που θα μπορούσε να προκύψει από τη χρήση μεροληπτικών ή μεροληπτικών συστημάτων τεχνητής νοημοσύνης.

6.4.1. Πως λειτουργεί το συγκεκριμένο εργαλείο

Πριν εκπονηθεί η AIA, καλό θα είναι μια αναφορά για το πως λειτουργεί το συγκεκριμένο εργαλείο, που αποτελείται από 48 ερωτήσεις που καθορίζουν το ρίσκο που εισάγει η χρήση του συγκεκριμένου εργαλείου προς αξιολόγηση, και επίσης 33 ερωτήσεις για την βοήθεια του μετριασμού του ρίσκου που εισάγει η χρήση του συγκεκριμένου εργαλείου.

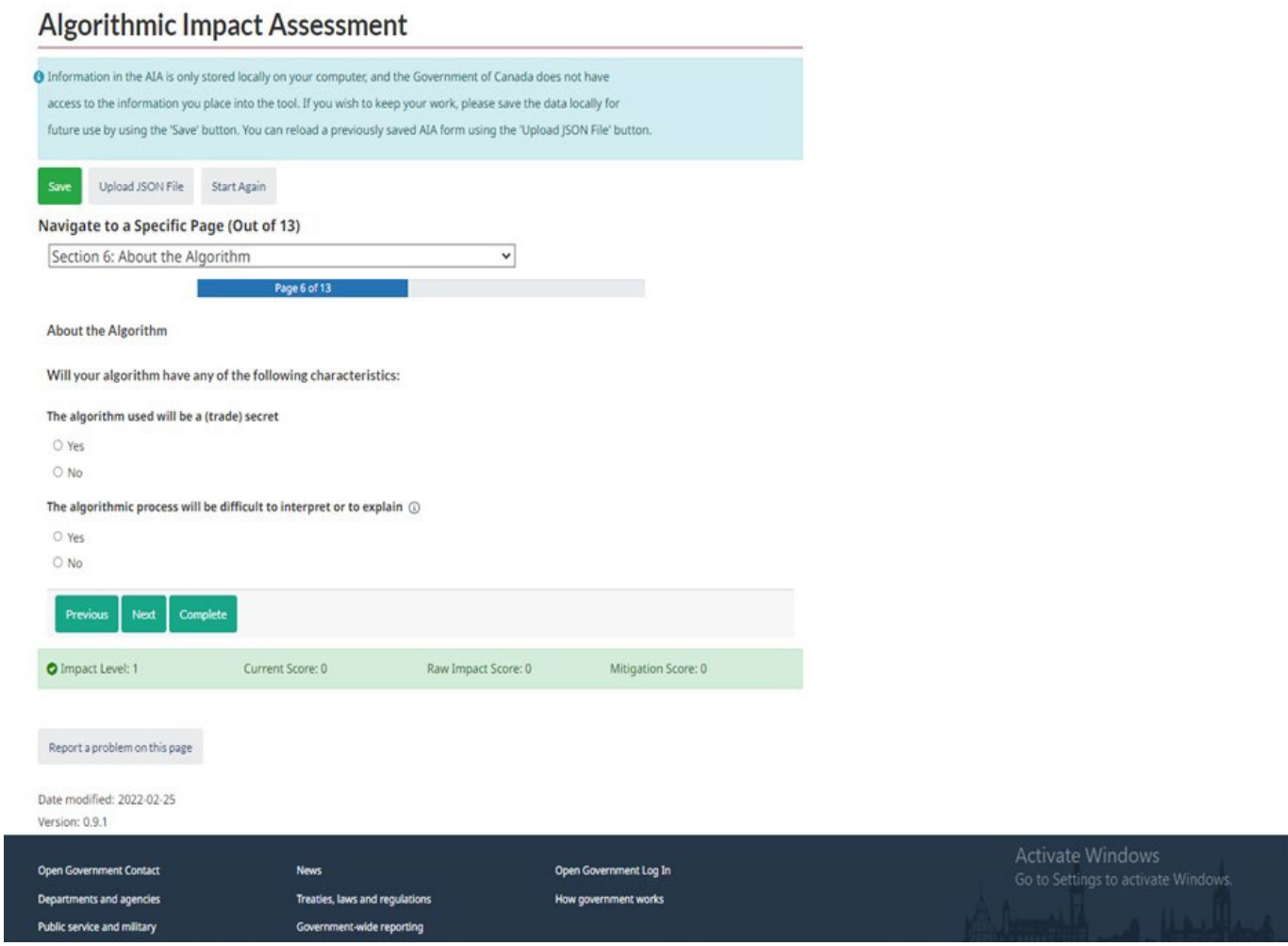
Το συγκεκριμένο ερωτηματολόγιο είναι ένα open source project και είναι ελεύθερη η χρήση του, το οποίο ανανεώνεται σε τακτική βάση και δίνεται η δυνατότητα όποιος θέλει και έχει την απαιτούμενη γνώση να συμβάλει στην εξέλιξη του εργαλείου αυτού το οποίο είναι διαθέσιμο και στο GitHub **[4]**.

Το συγκεκριμένο ερωτηματολόγιο αποτελείται από 13 ενότητες, όπως φαίνεται παρακάτω (εικόνα 6.2),

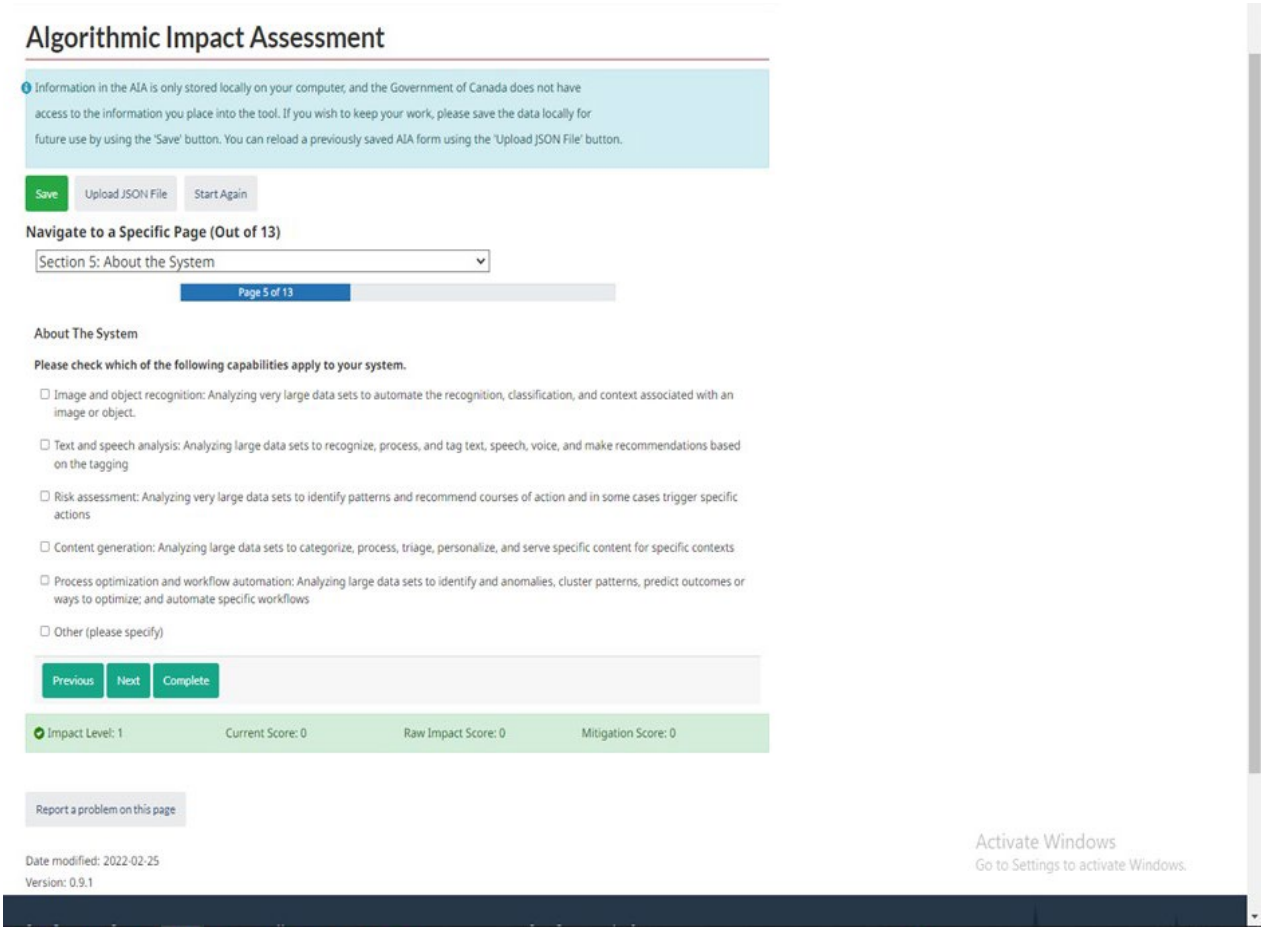


Εικόνα 6.2: Βασικές λεπτομέρειες του Project

Οι πληροφορίες που δίνονται είναι από γενικής φύσεως όπως λεπτομέρειες για το Project αλλά και πληροφορίες μέχρι για τον αλγόριθμο, το σύστημα την εκτίμηση αντικτύπου και άλλα, όπως φαίνεται παρακάτω (εικόνες 6.3 και 6.4),



Εικόνα 6.3: Πληροφορίες για τον αλγόριθμο



Εικόνα 6.4: Πληροφορίες για το πληροφοριακό σύστημα

Άξια αναφοράς στις συγκεκριμένες ενότητες είναι οι ερωτήσεις που γίνονται στην ενότητα του αλγόριθμου, για παράδειγμα το πόσο δύσκολο θα είναι ο αλγόριθμος να εξηγηθεί το πως δουλεύει, η για παράδειγμα στην ενότητα για το σύστημα τι δεδομένα θα επεξεργάζεται όπως για παράδειγμα αναγνώριση εικόνων και αντικειμένων, ανάλυση ομιλίας ή κειμένου, όπως και στην ενότητα για την εκτίμηση αντικτύπου όπου υπάρχουν ερωτήσεις όπως για το εάν η απόφαση που θα λάβει το αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ μπορεί να είναι διαφορετική εάν η απόφαση ληφθεί από έναν άνθρωπο, η εάν το αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ χρησιμοποιείται από υπαλλήλους της εταιρείας ή του οργανισμού και δεν ανήκουν στο τμήμα που ανέπτυξε το συγκεκριμένο εργαλείο.

Η αξιολόγηση γίνεται σύμφωνα με την κείμενη νομοθεσία για την προστασία από την χρήση των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ της Κυβέρνησης του Καναδά, και της συνεργασίας αυτής με την γραμματεία του Υπουργείου Οικονομικών, της Ακαδημαϊκής Κοινότητας αλλά και άλλους δημόσιους φορείς, και γίνεται αντιληπτό, όπως επισημαίνεται στην ιστοσελίδα του εν λόγω εργαλείου, ότι αυτή η συνεργασία συμβάλει στα

μέγιστα για την ανάπτυξη ενός σωστού πλαισίου ελέγχου των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Το συγκεκριμένο εργαλείο που χρησιμοποιείται στα πλαίσια της AIA, αποτελείται από διάφορες ερωτήσεις που χωρίζονται σε ενότητες όπως έχει προαναφερθεί, έτσι ώστε να γίνει εκτίμηση του κίνδυνου στους τομείς αυτούς, όπως φαίνεται παρακάτω (πίνακας 6.13),

Risk area definitions	
Risk areas	**Definition**
1. Project	
Project phase	Project owner, description and stage (design or implementation)
Business drivers / positive impacts	Motivation for introducing automation into the decision-making process
Risk profile	High-level risk indicators for the project
Project authority	Need to seek new policy authority for the project
2. System	
About the system	Capabilities of the system (that is, image recognition, risk assessment)
3. Algorithm	
About the algorithm	Transparency of the algorithm, whether it is easily explained
4. Decision	
About the decision	Classification of the decision being automated (that is, health services, social assistance, licensing)
5. Impact	
Impact assessment	Duration, reversibility and area impacted (freedom, health, economy or environment)
6. Data	

Source	Provenance and security classification of data used to automate decisions
Type	Nature of the data used as structured or unstructured (audio, text, image or video)

Πίνακας 6.13: Ενότητες του εργαλείου αξιολόγησης

Επίσης το συγκεκριμένο εργαλείο προσφέρει μέτρα μετριασμού των κινδύνων που έχουν εντοπιστεί, μέσα από ένα σύνολο ερωτήσεων όπως φαίνεται παρακάτω (πίνακας 6.14),

Mitigation area definitions	
Mitigation areas	**Definition**
1. Consultation	
Internal and external stakeholders	Internal and external stakeholders consulted, such as privacy and legal experts
2. De-risking and mitigation measures	
Data quality	Processes to ensure that data is representative and unbiased, as well as transparency measures related to those processes
Procedural fairness	Procedures to audit the system and its decisions, as well as the recourse process
Privacy	Measures to safeguard personal information

Πίνακας 6.14: Μέτρα μετριασμού των κινδύνων

Ο βασικός τρόπος του συγκεκριμένου εργαλείου βασίζεται σε ένα σύστημα «σκορ», αφού κάθε απάντηση σε κάθε ερώτηση που ανήκει σε κάθε μία από την ενότητα που προαναφέρθηκαν, συμβάλει στο μέγιστο «σκορ», σε κάθε έναν από τους τομείς.

Το πόσο σημαντική είναι η ερώτηση και κατά επέκταση ο βαθμός που παίρνει η κάθε απάντηση της, είναι σταθμισμένος με βάση την επίπτωση αλλά και τον μετριασμό αυτής της επίπτωσης, όπως φαίνεται παρακάτω (πίνακες 6.15 και 6.16),

Raw impact score from the risk areas

Risk area	No. of questions	Maximum score
1. Project	15	15
2. System	1	0
3 Algorithm	2	6
4. Decision	1	6
5. Impact	16	36
6. Data	13	44
Raw impact score	**48**	**107**

Πίνακας 6.15: Περιοχές ελέγχου και τα σκορ που μπορεί να λάβουν

Mitigation score from the mitigation areas		
Mitigation area	**No. of questions**	**Maximum score**
1. Consultations	**2**	**2**
2. De-risking and mitigation measures	**31**	**43**
Mitigation score	**33**	**45**

Πίνακας 6.16: Περιοχές αντιμέτρων και τα σκορ που μπορεί να λάβουν

Ο πρώτος από τους δύο πίνακες μετράει τις επιπτώσεις που θα έχει η χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, ενώ ο δεύτερος πίνακας δείχνει εάν και κατά πόσο έχουν αντιμετωπιστεί οι επιπτώσεις από την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ.

Στην παραπάνω περίπτωση γίνεται αντιληπτό ότι η AIA θέτει ένα πιο ειδικό πλαίσιο ελέγχου των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ, το οποίο σε καμία περίπτωση δεν βρέθηκε στον GDPR, εκτός από γενικές αναφορές όπως το άρθρο 22, ή το άρθρο 35.

Θα μπορούσε να αναφερθεί εδώ ότι σε σχέση με τα αυτοματοποιημένα εργαλεία λήψης αποφάσεων και δημιουργίας προφίλ, ο GDPR θέτει ένα πλαίσιο προστασίας των ατομικών ελευθεριών και δικαιωμάτων του πολίτη, αλλά η AIA από την άλλη παρέχει ένα πιο ειδικό πλαίσιο ελέγχου των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

6.4.2. Εκπόνηση της AIA

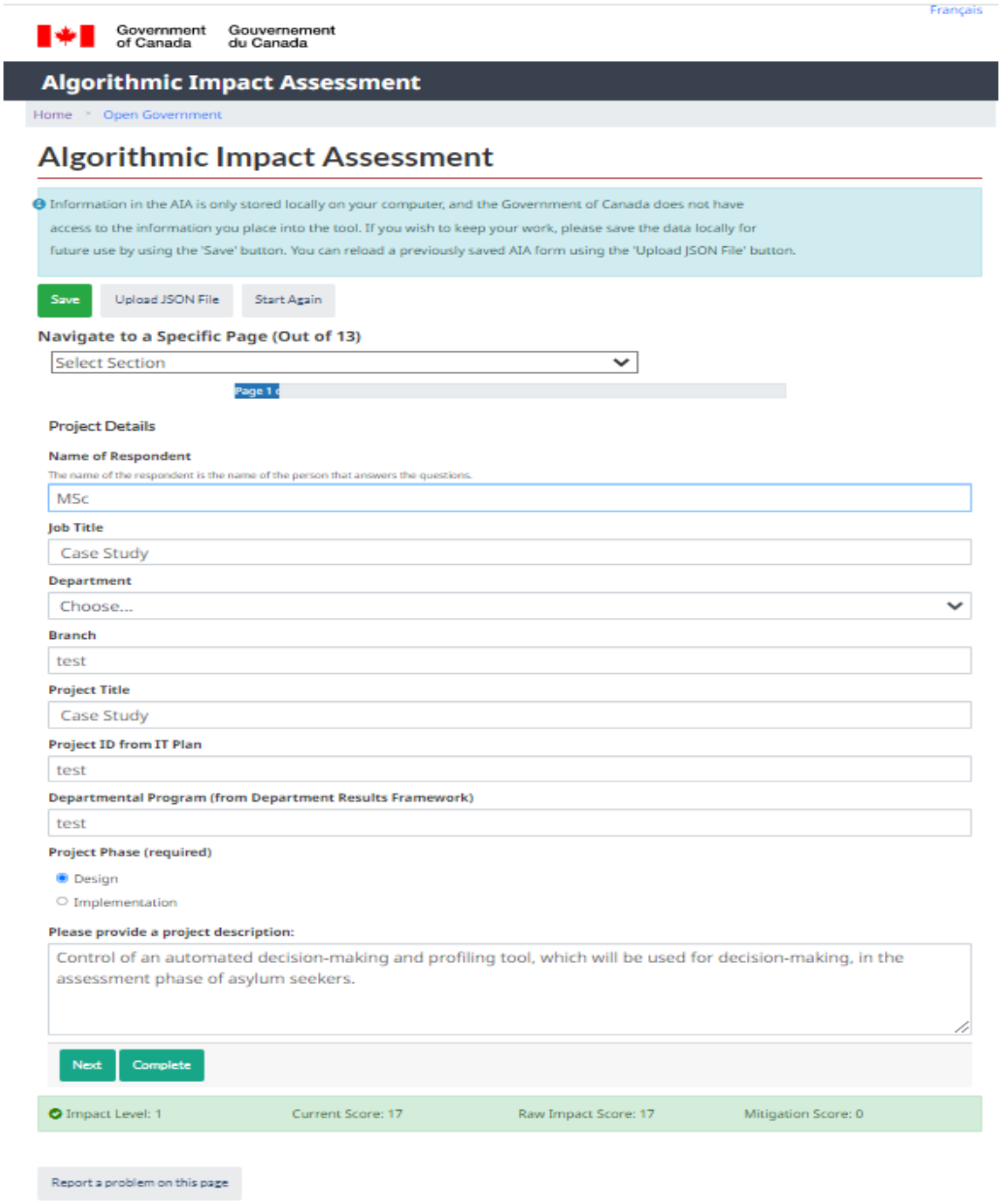
Κατά την εκπόνηση της AIA θα υπάρξουν 2 στάδια, και συγκεκριμένα των 10 πρώτων ενοτήτων που θα καθορίσουν το «σκορ επίπτωσης» που θα λάβει το αυτοματοποιημένο εργαλείο λήψης αποφάσεων, και εν συνεχεία και με βάση το σκορ το επίπεδο επίπτωσης της χρήσης αυτού.

Και στο δεύτερο στάδιο, θα είναι οι τελευταίες 3 ενότητες που προτείνουν μέτρα τα οποία εάν ληφθούν θα μετριάσουν την επίπτωση αυτή.

6.4.2.1. Εύρεση Αντικτύπου

Κατά την διενέργεια της AIA, όπως έχει αναφερθεί στις πρώτες 10 ενότητες υπάρχουν ερωτήσεις που σαν σκοπό έχουν να υπολογίσουν το επίπεδο της επίπτωσης αλλά και το σκορ.

Ξεκινώντας με την πρώτη ενότητα έχουμε να κάνουμε με γενικές ερωτήσεις όπως για παράδειγμα, το όνομα αυτού που συμπληρώνει το ερωτηματολόγιο, το τμήμα που ανήκει, το όνομα του project, εάν είναι σε φάση σχεδιασμού η σε φάση εγκατάστασης και χρήσης, όπως φαίνεται παρακάτω (εικόνα 6.5),



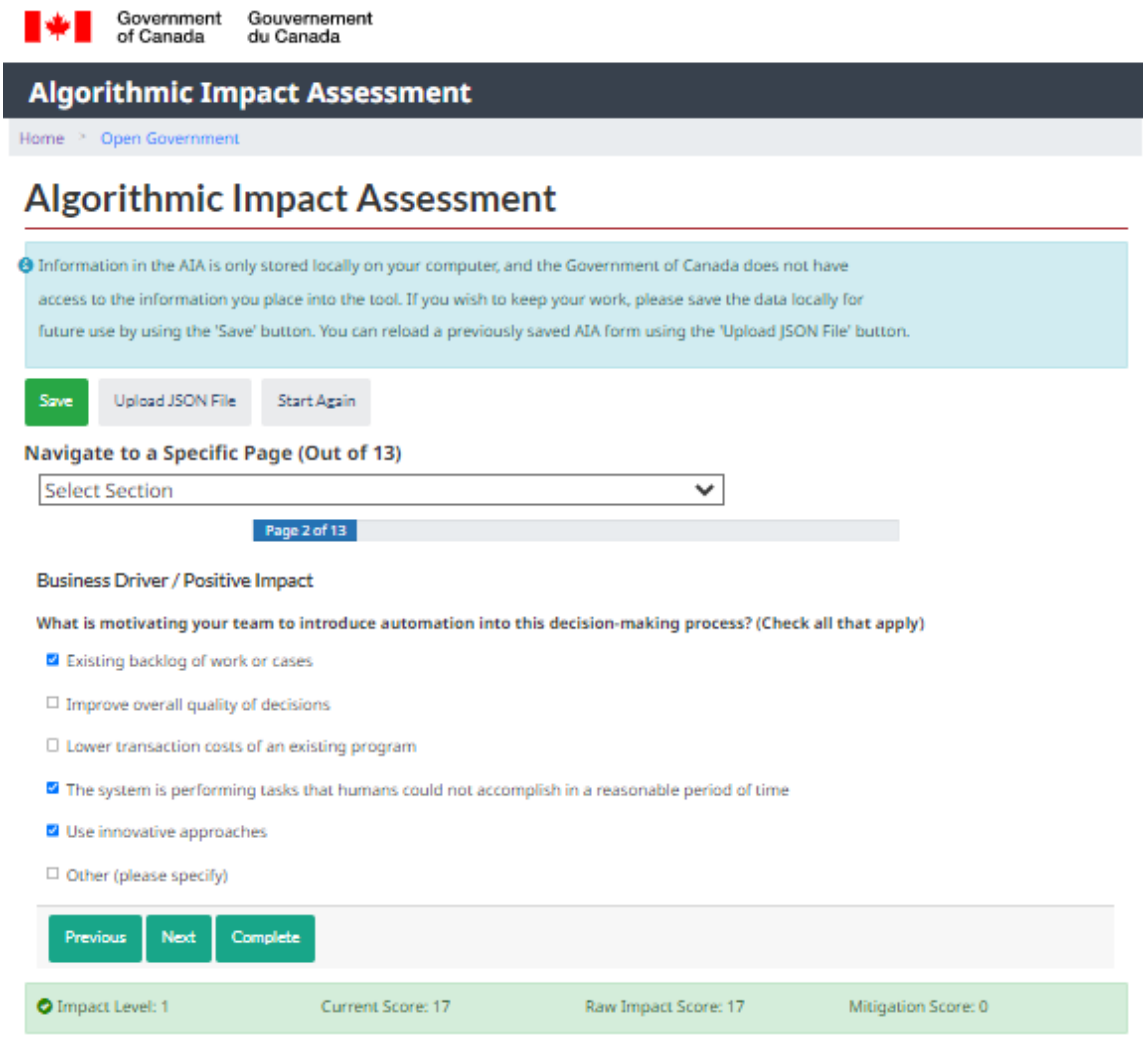
Εικόνα 6.5: Βασικές πληροφορίες για Project ελέγχου

Στο κάτω μέρος της εικόνας φαίνεται το επίπεδο επίπτωσης (Impact Level), το τρέχον σκορ (Current Score), το Raw Impact Score το οποίο είναι αυτό που αυξάνει ή όχι και καθορίζει το επίπεδο επίπτωσης ανάλογα με το σκορ, και τέλος υπάρχει και το Mitigation Score το οποίο θα υπολογιστεί στις 3 τελευταίες ενότητες.

Στην συνέχεια στην ενότητα 2, θα πρέπει να απαντηθεί γιατί υπάρχει η ανάγκη για την χρήση αυτό και η απαντήσεις εδώ είναι, με βάση την μελέτη περίπτωσης:

- Υφιστάμενες καθυστερήσεις εργασιών ή υποθέσεων,
- Το σύστημα εκτελεί καθήκοντα που οι άνθρωποι δεν μπορούσαν να ολοκληρώσουν σε εύλογο χρονικό διάστημα,
- Χρήση καινοτόμων τεχνολογιών

Όπως φαίνεται παρακάτω (εικόνα 6.6),



Εικόνα 6.6: Λόγοι για την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων

Στην ενότητα 3, υπάρχουν ερωτήσεις που καθορίζουν σε μεγάλο βαθμό το ρίσκο, και συγκεκριμένα:

Το έργο βρίσκεται σε περιοχή έντονου δημόσιου ελέγχου (π.χ. λόγω ανησυχιών για την ιδιωτική ζωή) ή/και συχνών αντιδικιών;

Η απάντηση στην ερώτηση αυτή είναι ναι, αφού το συγκεκριμένο εργαλείο θα χρησιμοποιηθεί για έκδοση αποφάσεων, που γίνονται γνωστές σε δικηγόρους, μη κρατικούς οργανισμούς, και θα υπάρχουν πολλές φορές συγκρούσεις λόγω των απόψεων.

Είναι οι πελάτες σε αυτόν τον τομέα δραστηριότητας ιδιαίτερα ευάλωτοι;

Ασφαλώς και είναι, δεδομένου ότι πρόκειται για αιτούντες ασύλου και ήδη έχουν στερηθεί βασικά ατομικά δικαιώματά τους.

Είναι πολύ υψηλό το διακύβευμα των αποφάσεων;

Ναι είναι, αφού έχει να κάνει με το εάν θα κριθεί κάποιος ευάλωτος, η εάν θα περάσει από συνέντευξη για την παροχή Ασύλου.

Θα έχει αυτό το έργο σημαντικές επιπτώσεις στο προσωπικό, είτε ως προς τον αριθμό είτε τους ρόλους του;

Ναι θα έχει, εάν αναλογιστεί κανείς ότι η χρήση του συγκεκριμένου εργαλείου, θα έχει σαν αποτέλεσμα μελλοντικά να απαλλαγεί το προσωπικό από κάποιες διαδικασίες αφού οι αποφάσεις θα βγαίνουν πιο γρήγορα, και κατά επέκταση και τα καθήκοντα αυτών θα επαναπροσδιοριστούν (πχ. μετακίνηση κάποιων σε άλλες θέσεις ευθύνης που ενδεχομένως επιθυμούν).

Στην ενότητα 4, υπάρχει ερώτηση για το εάν είναι αναγκαία μια νέα πολιτική για αυτό το έργο:

Δεδομένου ότι το συγκεκριμένο εργαλείο θα χρησιμοποιηθεί πρώτη φορά, για την επεξεργασία προσωπικών και ευαίσθητων προσωπικών δεδομένων και η κλίμακα αυτών των δεδομένων θα είναι πολύ μεγάλη εάν αναλογιστεί κανείς ότι υπάρχουν αιτούντες άσυλο από πάρα πολλές χώρες με τις όποιες ιδιαιτερότητες, ναι θα πρέπει να υπάρξει μια νέα πολιτική.

Στην ενότητα 5, υπάρχουν ερωτήσεις που έχουν να κάνουν με το τι δυνατότητες έχει το συγκεκριμένο εργαλείο, και οι απαντήσεις είναι οι εξής:

- Εκτίμηση κινδύνου: Ανάλυση πολύ μεγάλων συνόλων δεδομένων για τον εντοπισμό προτύπων και τη σύσταση τρόπων δράσης και σε ορισμένες περιπτώσεις για την ενεργοποίηση συγκεκριμένων ενεργειών,

- Δημιουργία περιεχομένου: Ανάλυση μεγάλων συνόλων δεδομένων για κατηγοριοποίηση, επεξεργασία, διαλογή, εξατομίκευση και προβολή συγκεκριμένου περιεχομένου για συγκεκριμένα περιβάλλοντα,

- Βελτιστοποίηση διαδικασιών και αυτοματοποίηση ροής εργασιών: Ανάλυση μεγάλων συνόλων δεδομένων για εντοπισμό και ανωμαλίες, πρόβλεψη αποτελεσμάτων ή τρόπους βελτιστοποίησης. και αυτοματοποίηση συγκεκριμένων ροών εργασίας

Όλες οι παραπάνω απαντήσεις, έχουν να κάνουν με τον όγκο των προς επεξεργασία δεδομένων, την αυτοματοποίηση εργασιών και λήψης αποφάσεων με την χρήση AI και του ML.

Στην ενότητα 6, υπάρχουν ερωτήσεις που αναφέρονται στο αλγόριθμο που θα χρησιμοποιηθεί στο συγκεκριμένο εργαλείο, οι απαντήσεις είναι οι εξής:

Ο αλγόριθμος που χρησιμοποιείται θα είναι (εμπορικό) μυστικό;

Όχι δεν θα είναι εμπορικό μυστικό.

Η αλγοριθμική διαδικασία θα είναι δύσκολο να ερμηνευτεί ή να εξηγηθεί;

Δεδομένου, ότι ένα μεγάλο ποσοστό των αιτούντων για άσυλο, προέρχονται από χώρες με χαμηλό μορφωτικό επίπεδο, σε μια προσπάθεια να εξηγηθεί τι επίπτωση μπορεί να έχει η χρήση του συγκεκριμένου εργαλείου στην ζωή τους, ως ένα βαθμό μπορεί να γίνει κατανοητό αλλά όχι πλήρως, άρα η απάντηση εδώ είναι ναι.

Στην ενότητα 7, υπάρχουν ερωτήσεις εάν η απόφαση ανήκει και σε ποια κατηγορία από τις παρακάτω, και συγκεκριμένα:

Υπηρεσίες σχετικές με την υγεία, αφού μια απόφαση αρνητική ως προς το ενδεχόμενο να περάσει ή όχι συνέντευξη ο αιτών ή η αιτούσα άσυλο, δημιουργεί μια προβληματική κατάσταση (γραφειοκρατίας), που έχει άμεσα αντίκτυπο στο εάν χρειαστεί να προσφερθεί ιατροφαρμακευτική περίθαλψη.

Κοινωνική βοήθεια (αιτήματα αναπηρίας), και εδώ μια αρνητική απόφαση στο εάν θα περάσει ή όχι συνέντευξη, ή εάν ανήκει ή όχι σε ευπαθή ομάδα, μπορεί να αποτελέσει τροχοπέδη στο να λάβει ή όχι κοινωνική βοήθεια.

Με το ίδιο σκεπτικό, η απόφαση ανήκει και στις 2 παρακάτω ομάδες.

Πρόσβαση και κινητικότητα (άδειες ασφαλείας, συνοριακές διελεύσεις),

Αδειοδότηση και έκδοση αδειών διαμονής.

Στην ενότητα 8, θα μπορούσε να αναφερθεί ότι υπολογίζεται σε μεγάλο βαθμό η επίπτωση της χρήσης του αυτοματοποιημένου εργαλείου λήψη αποφάσεων, και συγκεκριμένα:

Θα χρησιμοποιηθεί το σύστημα μόνο για να βοηθήσει έναν υπεύθυνο λήψης αποφάσεων;

Ναι.

Θα αντικαταστήσει το σύστημα μια απόφαση που διαφορετικά θα λάμβανε ένας άνθρωπος;

Όχι, δεδομένης της νομικής απαίτησης που απορρέει από τον GDPR.

Θα αντικαταστήσει το σύστημα τις ανθρώπινες αποφάσεις που απαιτούν κρίση ή διακριτικότητα;

Όχι (βλ. προηγούμενη ερώτηση).

Περιγράψτε τις αποφάσεις που θα αυτοματοποιηθούν:

Εάν ο αιτών άσυλο ανήκει είτε όχι σε μια ευάλωτη ομάδα, εάν θα πραγματοποιηθεί συνέντευξη ή όχι, το είδος της συνέντευξης ανάλογα με το φύλο του, τις θρησκευτικές πεποιθήσεις κ.λπ. Σε κάθε περίπτωση, η τελική απόφαση θα λαμβάνεται από άνθρωπο, λαμβάνοντας βεβαίως υπόψη και την έκβαση του αλγορίθμου.

Χρησιμοποιείται το σύστημα από διαφορετικό μέρος του οργανισμού από εκείνους που το ανέπτυξαν;

Η ανάπτυξη του συγκεκριμένου αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, θα γίνει από εξωτερικό συνεργάτη, που θα επιλεγεί μέσα από διεθνή διαγωνισμό.

Είναι οι επιπτώσεις που προκύπτουν από την απόφαση αναστρέψιμες;

Προφανώς και θα είναι, αλλά θα χρειάζεται περισσότερος χρόνος αφού ο αιτών ή αιτούσα θα πρέπει να κάνει προσφυγή κατά της απόφασης του αυτοματοποιημένου εργαλείου.

Πόσο καιρό θα διαρκέσουν οι επιπτώσεις από την απόφαση;

Κάποιες ίσως και μερικούς μήνες.

Περιγράψτε γιατί οι επιπτώσεις που προκύπτουν από την απόφαση είναι σύμφωνα με την παραπάνω επιλεγμένη επιλογή:

Για παράδειγμα, εάν ένας από τους αιτούντες άσυλο κατά λάθος δεν χαρακτηριστεί ως ευάλωτος, τότε η διαδικασία έκδοσης ή μη ασύλου θα ακολουθήσει διαφορετικό δρόμο με ό,τι αυτό συνεπάγεται.

Οι επιπτώσεις που θα έχει η απόφαση στα δικαιώματα ή τις ελευθερίες των ατόμων θα είναι πιθανώς:

Θα είναι πολύ μεγάλες.

Περιγράψτε γιατί είναι οι επιπτώσεις που προκύπτουν από την απόφαση (σύμφωνα με την παραπάνω επιλεγμένη επιλογή):

Στην περίπτωση των ομοφυλόφιλων και του δικαιώματος της γενετήσιας επιλογής, είναι άτομα που σε ποσοστό έως και 95% δεν έχουν οικογένεια είναι μόνα τους, και η ιδιαιτερότητα τους δεν είναι αποδεκτή στην χώρα τους αλλά και από τους συμπατριώτες τους.

Σε περίπτωση που γίνει μια λήψη απόφασης ότι δεν ανήκει στην συγκεκριμένη ευάλωτη ομάδα, και κατά επέκταση η κράτηση του σε ξεχωριστή περιοχή της δομής, αυτό έχει σαν αποτέλεσμα να κινδυνεύει ακόμα και η ίδια του η ζωή.

Σε κάθε περίπτωση, η μη χορήγηση ασύλου συνεπάγεται μεγάλο περιορισμό ατομικών ελευθεριών.

Οι επιπτώσεις που θα έχει η απόφαση στην υγεία και την ευημερία των ατόμων θα είναι πιθανώς:

Θα είναι πολύ μεγάλες.

Περιγράψτε γιατί είναι οι επιπτώσεις που προκύπτουν από την απόφαση (σύμφωνα με την παραπάνω επιλεγμένη επιλογή):

Σε περίπτωση που ληφθεί απόφαση ότι δεν υπάρχει σοβαρό πρόβλημα υγείας και δεδομένου ότι κάποιοι από τους αιτούντες αποκρύψουν κάποιες πληροφορίες για την κατάσταση της υγείας τους, μέχρι να εξεταστούν από τις Ιατρικές Εποπτικές Αρχές εδώ δεν θα υπάρξει η δέουσα μεταχείριση τους, με αποτέλεσμα να κινδυνεύει και σε αυτήν την περίπτωση η ίδια τους η ζωή, σε περίπτωση επιδείνωσης της υγείας τους.

Οι επιπτώσεις που θα έχει η απόφαση στα οικονομικά συμφέροντα των ατόμων θα είναι πιθανώς:

Θα είναι πολύ μεγάλες.

Περιγράψτε γιατί είναι οι επιπτώσεις που προκύπτουν από την απόφαση (σύμφωνα με την παραπάνω επιλεγμένη επιλογή):

Σε περίπτωση απόφασης του συγκεκριμένου αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ, που θα κρίνει ότι δεν θα πρέπει να περάσει από συνέντευξη, γίνεται αντιληπτό ότι ο αιτών ή η αιτούσα, δεν θα μπορέσουν να έχουν την ευκαιρία να λάβουν άσυλο και κατά επέκταση την δυνατότητα να μεταβούν σε όποια ευρωπαϊκή χώρα, να βρούνε μια δουλειά και κατά επέκταση ένα σταθερό εισόδημα, με αποτέλεσμα εάν ληφθεί υπόψιν ότι για να φτάσουν μέχρι εδώ για να ζητήσουν άσυλο, πούλησαν σε μερικές περιπτώσεις ακόμα και όλη την περιουσία τους.

Οι επιπτώσεις που θα έχει η απόφαση στη διαρκή βιωσιμότητα ενός περιβαλλοντικού οικοσυστήματος, πιθανότατα θα είναι:

Μικρή η έως ανύπαρκτη.

Στην ενότητα 9, υπάρχουν ερωτήσεις για να αποτυπωθεί καλύτερα, ο τύπος των δεδομένων στα οποία θα γίνει η επεξεργασία, με την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, αλλά και ο τρόπος συλλογής τους, συγκεκριμένα:

Το Αυτοματοποιημένο Σύστημα Αποφάσεων θα χρησιμοποιεί προσωπικές πληροφορίες ως δεδομένα εισόδου;

Όπως έχει ήδη αναφερθεί, το συγκεκριμένο αυτοματοποιημένο εργαλείο λήψης αποφάσεων θα χρησιμοποιεί αλγόριθμο RNN (recurrent neural network), είναι ένας τύπος αλγορίθμου βαθιάς μάθησης που χρησιμοποιείται συνήθως σε εργασίες επεξεργασίας φυσικής γλώσσας, και έτσι τα διαθέσιμα δεδομένα που θα περιλαμβάνουν δεδομένα κειμένου, όπως έγγραφα ή δηλώσεις από αιτούντες άσυλο, θα μπορούν να αναλυθούν για την εξαγωγή σχετικών πληροφοριών και για να γίνουν προβλέψεις.

Επομένως, ναι, όπως έχει ήδη προαναφερθεί, θα χρησιμοποιηθούν προσωπικά και ευαίσθητα προσωπικά δεδομένα, όπως για παράδειγμα όνομα, επίθετο, φύλο, ηλικία, τηλέφωνο), δεδομένα υγείας, πολιτικές και θρησκευτικές πεποιθήσεις, χώρα διαμονής, οικογενειακή κατάσταση, κτλ.

Έχετε επαληθεύσει ότι η χρήση προσωπικών πληροφοριών περιορίζεται μόνο σε ό,τι σχετίζεται άμεσα με την παροχή ενός προγράμματος ή μιας υπηρεσίας;

Ναι.

Χρησιμοποιούνται τα προσωπικά στοιχεία των ατόμων σε μια διαδικασία λήψης αποφάσεων που επηρεάζει άμεσα αυτά τα άτομα;

Ναι, εφόσον η απόφαση κρίνει το μέλλον της ζωής τους, όπως έχει προαναφερθεί και σε προηγούμενες ενότητες.

Έχετε επαληθεύσει εάν το σύστημα χρησιμοποιεί προσωπικές πληροφορίες με τρόπο που να συνάδει με: (α) τις τρέχουσες Τράπεζες Προσωπικών Πληροφοριών (PIB) και τις Εκτιμήσεις Επιπτώσεων Απορρήτου (PIA) των προγραμμάτων σας ή (β) προγραμματισμένες ή υλοποιημένες τροποποιήσεις στα PIB ή PIA που λαμβάνουν υπόψη νέες χρήσεις και διαδικασίες;

Δεν έχει άμεση εφαρμογή στην περίπτωσή μας.

Ποια είναι η υψηλότερη ταξινόμηση ασφαλείας των δεδομένων εισόδου που χρησιμοποιούνται από το σύστημα; (Επέλεξε ένα):

Η ταξινόμηση είναι υψηλή, αφού θα γίνει επεξεργασία προσωπικών και ευαίσθητων προσωπικών δεδομένων.

Ποιος ελέγχει τα δεδομένα;

Ο έλεγχος των δεδομένων υπόκειται σε επίπεδο περιφερειακών γραφείων ασύλου και πρώτης υποδοχής.

Θα χρησιμοποιεί το σύστημα δεδομένα από πολλές διαφορετικές πηγές;

Με βάση το υποθετικό σενάριό μας, δεν μπορεί να αποκλειστεί η διασύνδεση και με άλλα συστήματα τα οποία χρησιμοποιούνται μέχρι τώρα, μεταξύ διαφόρων Υπουργείων.

Θα απαιτήσει το σύστημα δεδομένα εισόδου από μια συσκευή συνδεδεμένη στο Διαδίκτυο ή στην τηλεφωνία; (π.χ. Internet of Things, αισθητήρας)

Όχι.

Θα διασυνδέεται το σύστημα με άλλα συστήματα πληροφορικής;

Ναι, και έχει ήδη προαναφερθεί.

Ποιος συνέλεξε τα δεδομένα που χρησιμοποιήθηκαν για την εκπαίδευση του συστήματος;

Με βάση το υποθετικό σενάριό, θα υπάρξει μια συνεργασία του Τμήματος της Πληροφορικής του Υπουργείου, των κατά τόπους γραφείων πρώτης υποδοχής και ταυτοποίησης, και ΠΓΑ.

Ποιος συνέλεξε τα δεδομένα εισόδου που χρησιμοποιήθηκαν από το σύστημα;

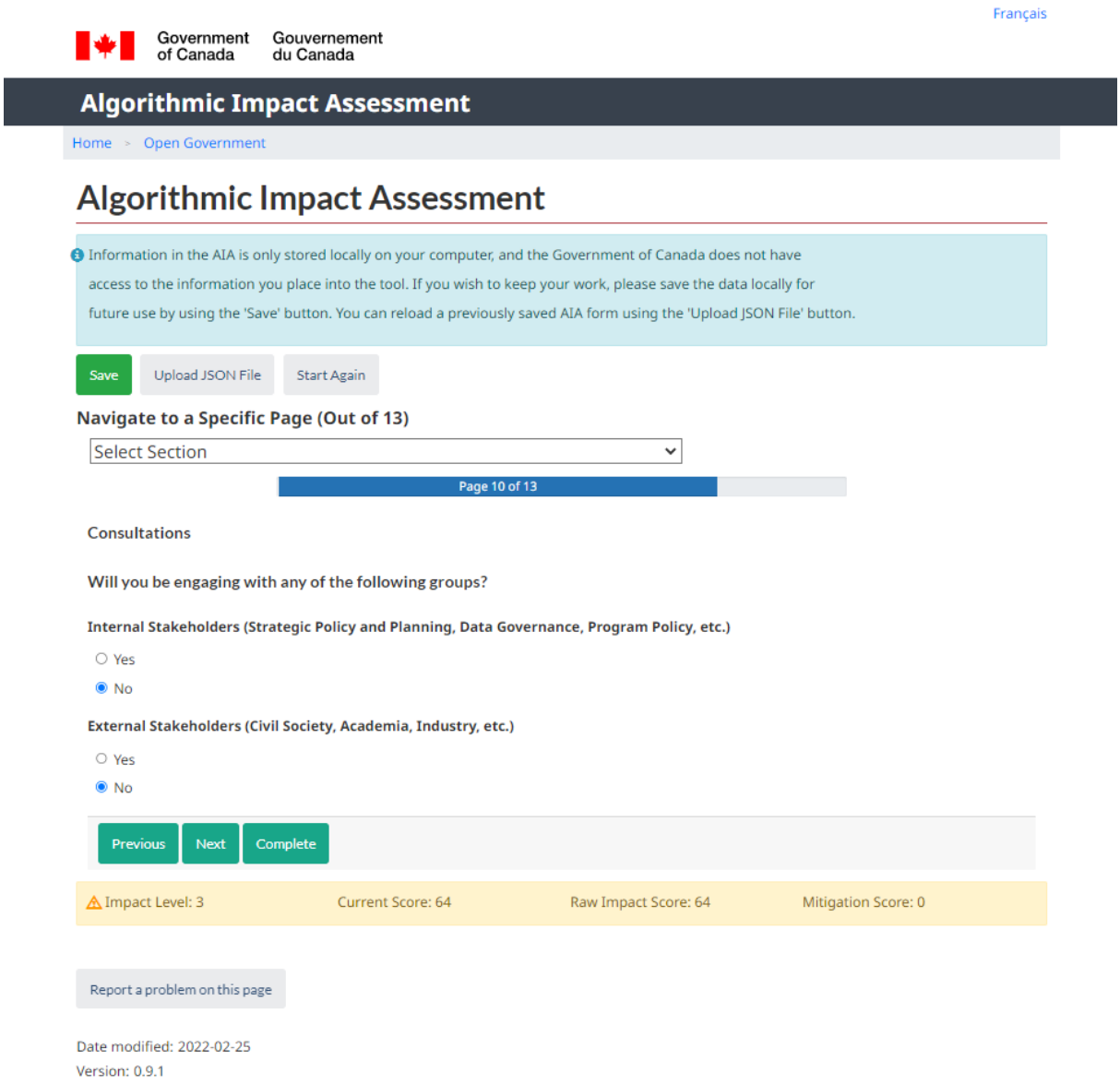
Με βάση το σενάριό μας, θα υπάρξει μια συνεργασία του Τμήματος της Πληροφορικής του Υπουργείου, των κατά τόπους γραφείων πρώτης υποδοχής και ταυτοποίησης, και ΠΓΑ.

Θα απαιτήσει το σύστημα την ανάλυση μη δομημένων δεδομένων για να δώσει μια σύσταση ή μια απόφαση;

Όχι.

Τέλος στην ενότητα 10 (Διαβουλεύσεις), το οποίο κάνει αναφορά εάν θα υπάρξει κάποια συνεργασία με εξωτερικούς συνεργάτες όπως για παράδειγμα Ακαδημαϊκή κοινότητά, Βιομηχανία κτλ, και οι απαντήσεις εδώ είναι όχι.

Μετά το πέρας και της 9ης ενότητας, και όπως φαίνεται παρακάτω (εικόνα 6.7),



Εικόνα 6.7: Ενότητα 10 (Διαβουλεύσεις), για την αναφορά συνεργασιών με εξωτερικούς συνεργάτες

η επίπτωση της χρήσης του συγκεκριμένου αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, λαμβάνει ένα σκορ 64, και το επίπεδο πλέον έχει ανέβει στο 3, και με βάση τον πίνακα **(αριθμός)** που κάνει αναφορά για το μέγιστο σκορ που μπορεί να λάβει και συγκεκριμένα το 107, φαίνεται ότι η επίπτωσή που θα έχει η χρήση του συγκεκριμένου εργαλείου θα είναι της τάξεως του 59,81%.

Με βάση τα παραπάνω μπορεί να αναφερθεί ότι η επίπτωση είναι μεγάλη.

6.4.2.2. Μέτρα άρσης κινδύνου και μετριασμού

Στις 3 τελευταίες ενότητες όπως έχει αναφερθεί, υπάρχουν μια σειρά από μέτρα που εάν εφαρμοστούν θα μετριάσουν τον βαθμό επίπτωσης από την χρήση του συγκεκριμένου αυτοματοποιημένου εργαλείου λήψης αποφάσεων.

Συγκεκριμένα οι ενότητες αφορούν:

- Μέτρα άρσης κινδύνου και μετριασμού - Ποιότητα Δεδομένων
- Μέτρα άρσης κινδύνου και μετριασμού - Διαδικαστική Δικαιοσύνη
- Μέτρα άρσης κινδύνου και μετριασμού – Απόρρητο

Μέτρα άρσης κινδύνου και μετριασμού - Ποιότητα Δεδομένων

Θα διαθέτετε τεκμηριωμένες διαδικασίες για τον έλεγχο των συνόλων δεδομένων έναντι προκαταλήψεων και άλλων απροσδόκητων αποτελεσμάτων; (Αυτό θα μπορούσε να περιλαμβάνει εμπειρία στην εφαρμογή πλαισίων, μεθόδων, κατευθυντήριων γραμμών ή άλλων εργαλείων αξιολόγησης).

Ναι, μόνο εξουσιοδοτημένα άτομα θα κάνουν review και θα θεμελιώνουν/καταγράφουν το σκεπτικό της απόφασής τους.

Θα δημοσιοποιήσετε αυτές τις πληροφορίες;

Όχι, αλλά θα εξετάζονται εσωτερικά στον οργανισμό.

Θα αναλάβετε μια Ανάλυση με βάση το φύλο;

Όχι είναι και η απάντηση και εδώ αφού δεν υπάρχει, με βάση το σενάριό μας, πρόθεση, να διενεργηθεί μια τέτοια ανάλυση.

Θα δημοσιοποιήσετε αυτές τις πληροφορίες;

Όχι, αλλά θα εξετάζονται εσωτερικά στον οργανισμό.

Έχετε αναθέσει την ευθύνη στο ίδρυμά σας για το σχεδιασμό, την ανάπτυξη, τη συντήρηση και τη βελτίωση του συστήματος;

Όλα τα παραπάνω δεν πρόκειται να εκτελεστούν από προσωπικό που ανήκει στο συγκεκριμένο Υπουργείο, αλλά από εξωτερικό συνεργάτη που θα προκύψει από διεθνή διαγωνισμό.

Θα έχετε μια τεκμηριωμένη διαδικασία για να διαχειριστείτε τον κίνδυνο να χρησιμοποιηθούν παλιά ή αναξιόπιστα δεδομένα για τη λήψη μιας αυτοματοποιημένης απόφασης;

Ναι.

Θα δημοσιοποιήσετε αυτές τις πληροφορίες;

Όχι, αλλά θα εξετάζονται εσωτερικά στον οργανισμό.

Τα δεδομένα που χρησιμοποιούνται για αυτό το σύστημα θα αναρτηθούν στην Πύλη Ανοικτής Κυβέρνησης;

Όχι. Θα διερευνηθεί μόνο αν ανώνυμα στατιστικά εμπίπτουν σε αυτά που αποκαλούνται «ανοιχτά δεδομένα» (για την Ελλάδα, βλ. https://www.data.gov.gr/)

Μέτρα άρσης κινδύνου και μετριασμού - Διαδικαστική Δικαιοσύνη

Θα προσδιορίσει η διαδρομή ελέγχου την αρχή ή την εξουσιοδοτημένη αρχή που προσδιορίζεται στη νομοθεσία;

Ναι – θεωρούμε ότι θα υπάρξει πρόβλεψη για αυτό.

Θα παρέχει το σύστημα μια διαδρομή ελέγχου που θα καταγράφει όλες τις συστάσεις ή τις αποφάσεις που λαμβάνονται από το σύστημα;

Για το υποθετικό σενάριό μας θα θεωρήσουμε το δυσμενές σενάριο, ότι δηλαδή δεν θα υπάρχει η δυνατότητα καταγραφής των αποφάσεων που λαμβάνονται από το συγκεκριμένο αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ, και φυσικά δεν υπάρχει η πρόθεση να εφαρμοστεί ένας μηχανισμός για την ύπαρξη συστάσεων.

Θα μπορούν να εντοπιστούν όλα τα βασικά σημεία λήψης αποφάσεων στη διαδρομή ελέγχου;

Όχι δεν θα είναι δυνατόν, αφού το αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ όπως έχει προαναφερθεί θα αναπτυχθεί από εξωτερικό συνεργάτη, σε συνεργασία φυσικά με όλους τους εμπλεκόμενους που γνωρίζουν τις διαδρομές των αποφάσεων. Με βάση το σενάριό μας, θα υπάρχει σχετική πρόβλεψη στη σύμβαση με τον εξωτερικό συνεργάτη.

Όλα τα βασικά σημεία λήψης αποφάσεων εντός της λογικής του αυτοματοποιημένου συστήματος θα συνδέονται με τη σχετική νομοθεσία, πολιτική ή διαδικασία;

Ναι.

Θα διατηρείτε ένα αρχείο καταγραφής με όλες τις αλλαγές που έγιναν στο μοντέλο και το σύστημα;

Θα τεθεί αυτό ως προϋπόθεση για την επιλογή αναδόχου.

Η διαδρομή ελέγχου θα καθορίζει με σαφήνεια όλα τα σημεία απόφασης που λαμβάνονται από το σύστημα;

Όχι δεν θα μπορεί να καθοριστεί, απλά θα υπάρχει η έκδοση μιας απόφασης.

Θα μπορούσε η διαδρομή ελέγχου που δημιουργείται από το σύστημα να χρησιμοποιηθεί για τη δημιουργία κοινοποίησης της απόφασης (συμπεριλαμβανομένης της αιτιολογίας ή άλλης κοινοποίησης) όπου απαιτείται;

Η κοινοποίηση θα γίνεται μόνο στον αιτών ή αιτούσα άσυλο, σε καμία άλλη περίπτωση δεν θα μπορεί να χρησιμοποιηθεί, και μόνο με φυσική παρουσία, άρα στην γενική απάντηση της ερώτησης είναι όχι.

Θα προσδιορίσει η διαδρομή ελέγχου με ακρίβεια ποια έκδοση του συστήματος χρησιμοποιήθηκε για κάθε απόφαση που υποστηρίζει;

Θα τεθεί αυτό ως προϋπόθεση για την επιλογή αναδόχου.

Θα δείξει η διαδρομή ελέγχου ποιος είναι ο εξουσιοδοτημένος λήπτης των αποφάσεων;

Όχι και εδώ δεν θα μπορεί να δειχθεί ποιος είναι ο εξουσιοδοτημένος λήπτης αποφάσεων, μιας και υπάρχει ένα "απρόσωπο" αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ. Ο αρμόδιος υπάλληλος θα είναι κάθε φορά διαφορετικός. Τα δικαιώματα πρόσβασης θα οριστούν σε άλλο επίπεδο (επίπεδο ελέγχου πρόσβασης του φορέα).

Θα μπορεί το σύστημα να αιτιολογεί τις αποφάσεις ή τις συστάσεις του όταν απαιτείται;

Για τις ανάγκες του σεναρίου μας, θα θεωρήσουμε το σενάριο ότι τέτοια δυνατότητα κατ' αρχάς δεν θα υπάρχει.

Θα υπάρξει διαδικασία για τη χορήγηση, παρακολούθηση και ανάκληση άδειας πρόσβασης στο σύστημα;

Δεν υπάρχει ακόμα κάποια απόφαση για το εάν το συγκεκριμένο αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ, θα αναπτυχθεί ως μια Web εφαρμογή η ως μιας εφαρμογής που θα εγκαθίσταται τοπικά στους υπολογιστές, και εάν θα υπάρξει η χρήση ADDS για την ύπαρξη των προαναφερόμενων δυνατοτήτων. Σε κάθε περίπτωση όμως, δυνατότητα πρόσβασης θα δοθεί μόνο σε εξουδιοτημένους χρήστες, βάσει του ρόλου του, η οποία θα ανακαλείται εάν χρειάζεται (π.χ. μετακίνηση/αποχώρηση υπαλλήλου).

Θα πρέπει να αναφερθεί ότι οι υπολογιστές δεν ανήκουν σε κάποιο Domain.

Θα υπάρχει μηχανισμός για τη λήψη σχολίων από τους χρήστες του συστήματος;

Θα τεθεί αυτό ως προϋπόθεση για την επιλογή αναδόχου.

Θα υπάρξει προγραμματισμένη ή καθιερωμένη διαδικασία προσφυγής για πελάτες που επιθυμούν να αμφισβητήσουν την απόφαση;

Ναι.

Το σύστημα θα επιτρέψει την ανθρώπινη παράκαμψη των αποφάσεων του συστήματος;

Ναι, αφού, σύμφωνα και με το άρθρο 22 του ΓΚΠΔ., η τελική απόφαση λαμβάνεται πάντα από άνθρωπο.

Θα υπάρχει κάποια διαδικασία για την καταγραφή των περιπτώσεων κατά τις οποίες πραγματοποιήθηκαν παρακάμψεις;

Ναι.

Η διαδρομή ελέγχου θα περιλαμβάνει διαδικασίες ελέγχου αλλαγών για την καταγραφή τροποποιήσεων στη λειτουργία ή την απόδοση του συστήματος;

Δεν υπάρχει καμία οδηγία για το εάν και τι έλεγχοι θα γίνονται και τι θα καταγράφεται σε αυτούς.

Ολοκληρώνοντας και την δεύτερη ενότητα που περιλαμβάνει αντίμετρα τα οποία μπορεί να ληφθούν, για τον μετριασμό της επίπτωσης της χρήσης του συγκεκριμένου εργαλείου, αυτό που γίνεται αντιληπτό είναι ότι η κατάσταση δεν έχει αλλάξει προς το θετικό, για την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ.

Μέτρα άρσης κινδύνου και μετριασμού – Απόρρητο

Εάν το σύστημά σας περιλαμβάνει τη χρήση προσωπικών πληροφοριών, θα αναλάβετε ή έχετε πραγματοποιήσει μια εκτίμηση επιπτώσεων στο απόρρητο ή θα ενημερώσετε μια υπάρχουσα;

Ναι.

Θα σχεδιάσετε και θα δημιουργήσετε ασφάλεια και απόρρητο στα συστήματά σας από το στάδιο της ιδέας του έργου;

Σε καμία περίπτωση, και λαμβάνοντας υπόψιν την εκτίμηση επιπτώσεων που διενεργήθηκε με το οδηγό της ENISA, δεν διαφαίνεται να υπάρχει η υλικοτεχνική υποδομή που να εξασφαλίζει την ασφάλεια και το απόρρητο.

Θα χρησιμοποιηθούν πληροφορίες σε ένα κλειστό σύστημα (δηλαδή χωρίς συνδέσεις με το Διαδίκτυο, το Intranet ή οποιοδήποτε άλλο σύστημα);

Όχι, με βάση το σενάριό μας θα χρησιμοποιηθούν υπολογιστικά συστήματα με διασύνδεση είτε το Διαδίκτυο είτε το Intranet.

Εάν πρόκειται για κοινή χρήση προσωπικών πληροφοριών, έχει συναφθεί συμφωνία ή συμφωνία με τις κατάλληλες διασφαλίσεις;

Ναι, αφού στην βάση του GDPR θα πρέπει να διασφαλίζονται:

Ο σκοπός για τον οποίο θα χρησιμοποιηθούν τα προσωπικά στοιχεία,

Το είδος των προσωπικών πληροφοριών που θα κοινοποιηθούν,

Τα μέρη που εμπλέκονται στην ανταλλαγή των πληροφοριών,

Η νομική βάση για την ανταλλαγή των πληροφοριών,

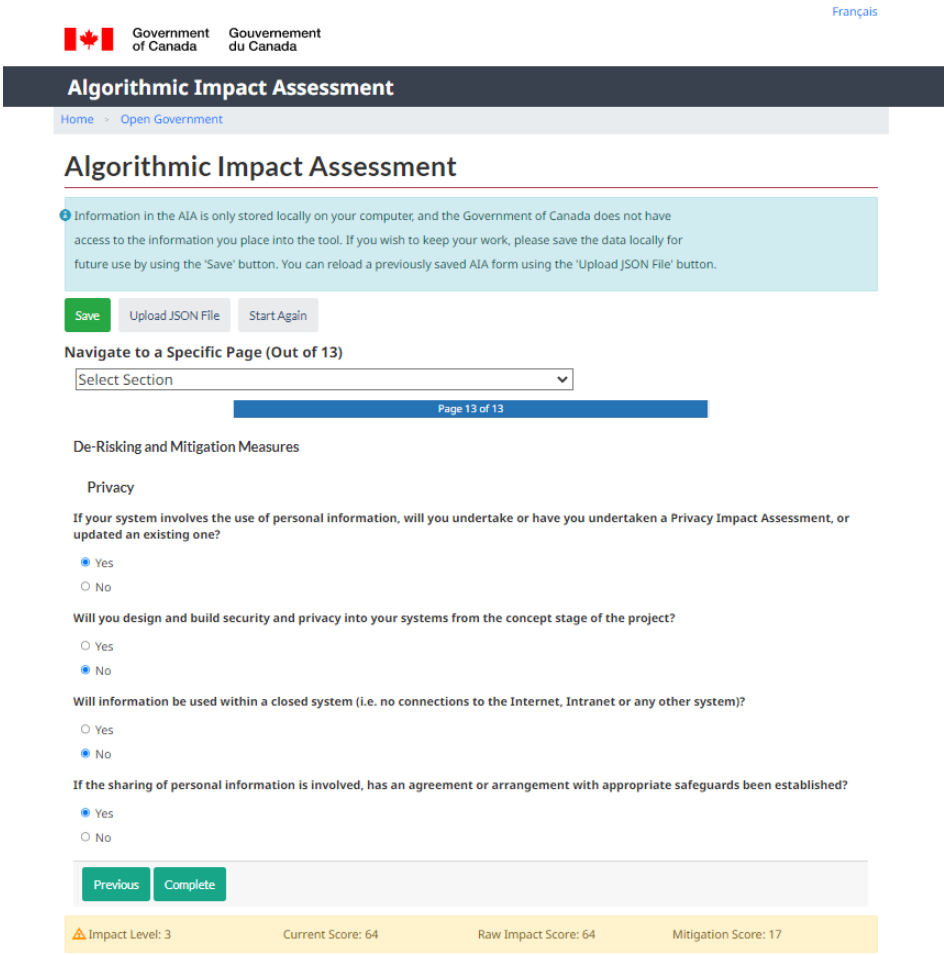
Τα μέτρα ασφαλείας που θα εφαρμοστούν για την προστασία των πληροφοριών,

Η διάρκεια της συμφωνίας κοινής χρήσης,

Οι διαδικασίες για τον χειρισμό τυχόν παραβιάσεων ή περιστατικών που αφορούν τις πληροφορίες,

Τα δικαιώματα των ατόμων των οποίων οι προσωπικές πληροφορίες κοινοποιούνται, συμπεριλαμβανομένου του δικαιώματός τους να έχουν πρόσβαση και να διορθώνουν τις πληροφορίες τους.

Έχοντας ολοκληρώσει και τις 3 ενότητες των αντίμετρων για την επίπτωση από την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, όπως διαφαίνεται και παρακάτω (εικόνα 6.8),



Εικόνα 6.8: Ενότητα 13 με το συνολικό σκορ επίπτωσης αλλά και το συνολικό σκορ των αντίμετρων

το mitigation score έχει λάβει ένα σκορ 17, δηλαδή με βάση τον πίνακα (αριθμός) που δείχνει το μέγιστο score που μπορεί να λάβει 45, γίνεται αντιληπτό ότι δεν φθάνει ούτε το 50% αυτού, και συγκεκριμένα είναι 37,77% ένα πολύ χαμηλό σκορ.

6.4.2.3. Συνολικά αποτελέσματα της AIA

Έχοντας ολοκληρώσει και τις 13 ενότητες του συγκεκριμένου εργαλείου για την εκπόνηση της AIA, μπορεί να φανεί συνολικά και το «σκορ» που λαμβάνει η επίπτωση αλλά και το «σκορ» που λαμβάνουν τα προτεινόμενα αντίμετρα, όπως φαίνεται και παρακάτω (εικόνες 6.9 και 6.10),

Section 1: Impact Level : 3

Current Score : 64

Raw Impact Score: 64

Risk Area	No. of Questions	Project Score	Maximum Score
Risk Profile	4	13	13
Project Authority	1	2	2
About the Algorithm	2	3	6
About the Decision	1	4	6
Impact Assessment	10	22	36
About the Data - A. Data Source	11	20	38
About the Data - B. Type of Data	2	0	6
RAW IMPACT SCORE	31	64	107

Εικόνα 6.9: Συνολικό σκορ που λαμβάνει η επίπτωση αλλά και το επίπεδο αυτής, από την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων

Mitigation Score: 17

Mitigation Area	No. of Questions	Project Score	Maximum Score
Consultations	4	0	2

Mitigation Area	No. of Questions	Project Score	Maximum Score
De-Risking and Mitigation Measures - Data Quality	10	3	14
De-Risking and Mitigation Measures - Procedural Fairness	17	12	25
De-Risking and Mitigation Measures - Privacy	4	2	4
MITIGATION SCORE	35	17	45

Εικόνα 6.10: Συνολικό σκορ που λαμβάνουν τα αντίμετρα

έχουμε ένα αποτέλεσμα που λαμβάνει ένα μεγάλο σκορ επίπτωσης 64 με μέγιστο το 107, και επίσης στα μέτρα Απαλλαγής Κινδύνων και Μετριασμού λαμβάνει ένα χαμηλό σκορ 17 με μέγιστο το 45.

Ύστερα από τα παραπάνω και χωρίς να έχει διενεργηθεί ακόμα μια DPIA, γίνεται αντιληπτό ότι η χρήση του συγκεκριμένου αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ, τουλάχιστον μέχρι να ληφθούν όλα τα απαραίτητα μέτρα για τον μετριασμό αλλά και όσον τον δυνατόν την εξάλειψη μιας τόσο μεγάλης επίπτωσης από την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων και δημιουργίας προφίλ δεν είναι δυνατή.

Έχοντας ολοκληρώσει και την AIA, και έχοντας λάβει μια σχεδόν σφαιρική εικόνα για την επίπτωση με βάση των οδηγό της ENISA, που ως προς τα υλοποιημένα συνολικά μέτρα ασφάλειας λήφθηκε υπόψη στην AIA, το επόμενο βήμα είναι η εκπόνηση μιας DPIA χρησιμοποιώντας το εργαλείο της Γαλλικής Υπηρεσίας Προστασίας Δεδομένων CNIL (βιβλιογραφία 11), που σαν σκοπό έχει να εντοπίζει τους κινδύνους που προκύπτουν από την επεξεργασία προσωπικών δεδομένων και να ελαχιστοποιεί αυτούς τους κινδύνους όσο το δυνατόν γρηγορότερα. Τα DPIA είναι σημαντικά εργαλεία για τον εντοπισμό του κινδύνου και για την απόδειξη της συμμόρφωσης με τον GDPR.

Το σημαντικό που θα πρέπει να αναφερθεί εδώ, είναι ότι έχοντας ολοκληρώσει την εκτίμηση επιπτώσεων ως προς την Ακεραιότητα, την Διαθεσιμότητα και την Εμπιστευτικότητα με την χρήση του οδηγού της ENISA και την εκτίμηση επιπτώσεων με την χρήση της AIA, έχει δημιουργηθεί πολύτιμη πληροφορία, που θα αποτελέσει τροφοδότηση του εργαλείου της Γαλλικής Υπηρεσίας Προστασίας Δεδομένων CNIL**[11]**, που θα έχει σαν αποτέλεσμα η εκτίμηση των επιπτώσεων με το συγκεκριμένο εργαλείο να εκπονηθεί πολύ πιο γρήγορα και εύκολα.

6.5. Εκπόνηση DPIA

Για την εκπόνηση της AIA θα χρησιμοποιηθεί το εργαλείο PIA της CNIL (Commission Nationale Informatique & Libertés) είναι η Αρχή Προστασίας Δεδομένων της Γαλλίας και πρωταρχικό της ρόλος είναι να προστατεύει τα δικαιώματα απορρήτου των ατόμων διασφαλίζοντας ότι τα προσωπικά δεδομένα συλλέγονται, αποθηκεύονται και χρησιμοποιούνται με νόμιμο και υπεύθυνο τρόπο.

Είναι υπεύθυνη για την επιβολή της νομοθεσίας περί προστασίας δεδομένων στη Γαλλία, συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και του Γαλλικού Νόμου για την Προστασία Δεδομένων (Loi Informatique et Libertés). Ο οργανισμός

παρέχει καθοδήγηση και συμβουλές σε επιχειρήσεις και οργανισμούς για θέματα προστασίας δεδομένων και έχει την εξουσία να ερευνά και να επιβάλλει κυρώσεις σε όσους δεν συμμορφώνονται με τους νόμους περί προστασίας δεδομένων.

Ένας από τους κύριους λόγους για τη χρήση του εργαλείου που παρέχεται από την CNIL για Εκτιμήσεις Επιπτώσεων Προστασίας Δεδομένων (DPIA) είναι η εκτεταμένη εμπειρία και η τεχνογνωσία στον τομέα της προστασίας δεδομένων και της ιδιωτικής ζωής. Η CNIL έχει συμμετάσχει ενεργά στη συμμόρφωση με τον GDPR και έχει βαθιά κατανόηση των απαιτήσεων και των βέλτιστων πρακτικών για τη διενέργεια ΕΑΠ.

Επιπλέον, είναι ένα ολοκληρωμένο εργαλείο για διενέργεια DPIA, το οποίο περιλαμβάνει έναν οδηγό βήμα προς βήμα και πρότυπα για να βοηθήσει τους οργανισμούς να αξιολογήσουν τους κινδύνους που σχετίζονται με τις δραστηριότητες επεξεργασίας δεδομένων τους. Το εργαλείο CNIL DPIA περιλαμβάνει επίσης ένα ερωτηματολόγιο που βοηθά στον εντοπισμό και την αξιολόγηση του αντίκτυπου των δραστηριοτήτων επεξεργασίας δεδομένων στα δικαιώματα και τις ελευθερίες των ατόμων, καθώς και καθοδήγηση σχετικά με τον μετριασμό των εντοπισμένων κινδύνων.

Επίσης, το CNIL προσφέρει υποστήριξη και καθοδήγηση σε οργανισμούς που χρειάζονται βοήθεια με το DPIA τους, συμπεριλαμβανομένων διαβουλεύσεων με ειδικούς προστασίας δεδομένων, εκπαιδευτικών συνεδριών και εργαστηρίων.

Συνολικά, η χρήση του CNIL για το DPIA μπορεί να παρέχει στους οργανισμούς την απαραίτητη τεχνογνωσία και πόρους για τη διεξαγωγή συνολικής και αποτελεσματικής αξιολόγησης των κινδύνων που σχετίζονται με τις δραστηριότητές τους επεξεργασίας δεδομένων, διασφαλίζοντας τη συμμόρφωση με τους κανονισμούς GDPR και προστατεύοντας τα προσωπικά δεδομένα.

6.5.1. Γενικό πλαίσιο

Ποια είναι η υπό εξέταση επεξεργασία;

Το Υπουργείο Μετανάστευσης και Ασύλου στα πλαίσια μια πρώτης αξιολόγησης για την επίσπευση των διαδικασιών των αιτούντων άσυλο, θέλει να χρησιμοποιήσει ένα Αυτοματοποιημένο Εργαλείο Λήψης Αποφάσεων και Δημιουργίας προφίλ, το οποίο θα μπορεί να λάβει αποφάσεις όπως εάν ο αιτών ή η αιτούσα θα περάσει από συνέντευξη για την παροχή ασύλου ή όχι, εάν ανήκει σε κάποια ευπαθή ομάδα, και μελλοντικά με χρήση του AI και του ML, να

μπορεί να πάρει και άλλες αποφάσεις με βελτιώσεις και νέες εκδόσεις του συγκεκριμένου εργαλείου.

Τα δεδομένα τα οποία θα χρησιμοποιηθούν για την λήψη των αποφάσεων, είναι προσωπικά και ευαίσθητα προσωπικά δεδομένα, όπως ηλικία, φύλο, θρησκευτικές πεποιθήσεις, οικογενειακή κατάσταση κτλ.

Ποιες είναι οι ευθύνες που συνδέονται με την επεξεργασία;

Οι διάφορες αποφάσεις που θα χορηγούνται από την Υπηρεσία Ασύλου, δηλαδή απόφαση ασύλου, εάν ο αιτών ανήκει σε ευάλωτη ομάδα κτλ, σύμφωνα με τον παρακάτω νόμο ((ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4939 ΦΕΚ Α 111/10.6.2022).

Υπάρχουν πρότυπα που ισχύουν για την επεξεργασία;

Όχι δεν υπάρχουν κάποια πρότυπα.

Ποια προσωπικά δεδομένα υφίστανται επεξεργασία;

Τα προσωπικά στοιχεία των αιτούντων άσυλο, και συγκεκριμένα:

- Όνομα
- Επίθετο
- Ηλικία
- Τηλέφωνο
- Email
- Δεδομένα Υγείας
- Θρησκευτικές Πεποιθήσεις
- Φύλο
- Βιομετρικά Στοιχεία

Πώς λειτουργεί ο κύκλος ζωής των δεδομένων και των διαδικασιών;

Τα προσωπικά δεδομένα θα συλλέγονται από τα κατά τόπους Γραφεία Πρώτης Υποδοχής αλλά και τα Περιφερειακά Γραφεία Ασύλου, τα οποία θα τροφοδοτούν το Αυτοματοποιημένο Εργαλείο Λήψης Αποφάσεων και Δημιουργίας προφίλ, για την λήψη αποφάσεων.

Θα υπάρχουν και σε ψηφιακή μορφή (στα υπολογιστικά συστήματα του περιφερειακών γραφείων αλλά και στα κεντρικά υπολογιστικά συστήματα του Υπουργείου μέσω της διασύνδεσης που θα υπάρχει), αλλά και σε φυσικό αρχείο.

Υπάλληλοι θα χρησιμοποιούν αυτά τα δεδομένα, τα οποία θα τροφοδοτούν το Αυτοματοποιημένο Εργαλείο Λήψης Αποφάσεων και Δημιουργίας προφίλ για την λήψη της απόφασης.

Υπάρχει η σκέψη το αυτοματοποιημένο εργαλείο να συνδεθεί με βάση δεδομένων για την αποθήκευση των αποφάσεων, θα γνωστοποιείται στους αιτούντες άσυλου, και θα ακολουθείτε η ανάλογη πορεία για την έκδοση απόφασης ασύλου ή όχι με βάση της απόφασης που θα λαμβάνεται από το Αυτοματοποιημένο Εργαλείο Λήψης Αποφάσεων και Δημιουργίας Προφίλ.

Ποια είναι τα στοιχεία που υποστηρίζουν τα δεδομένα;

Εδώ μπορούν να αναφερθούν τα εξής:

- Υπάρχον εξοπλισμός όπως υπολογιστές (επιτραπέζιοι και laptops) με λειτουργικό που δεν υποστηρίζονται από τις εταιρείες πλέον, όπως για παράδειγμα Windows XP και 7.
- Free εφαρμογές
- Διακομιστές
- Δικτυακός εξοπλισμός (router, switches, Access Points)

6.5.2. Θεμελιώδες Αρχές

Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;

Ναι είναι, στην βάση του GDPR αφού η σαφήνεια και η διαφάνεια σχετικά με τους σκοπούς της επεξεργασίας δεδομένων είναι ουσιαστικής σημασίας για να διασφαλιστεί ότι τα άτομα κατανοούν πώς χρησιμοποιούνται τα δεδομένα τους και μπορούν να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την κοινοποίηση των προσωπικών τους στοιχείων.

Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;

Από τις νομικές βάσεις του άρθρου 6 του GPDR, στη συγκεκριμένη περίπτωση έχει εφαρμογή η εξής νομική βάση:

«ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,»

αφού η εξέταση αιτήσεων ασύλου προβλέπεται σε νόμο και έχει ανατεθεί ως δημόσιο καθήκον, σε μία συγκεκριμένη Υπηρεσία.

Τα προσωπικά δεδομένα που συλλέγονται είναι επαρκή, συναφή και περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»);

Ναι είναι. Όλα τα ζητούμενα δεδομένα προβλέπονται από τη συναφή νομοθεσία.

Τα δεδομένα είναι ακριβή και ενημερωμένα;

Ναι, εκτός τις περιπτώσεις όπου ένας αιτών ή αιτούσα άσυλο δηλώνει ψευδή στοιχεία.

Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

Τα δεδομένα αποθηκεύονται μόνιμα και σε μορφή φυσικού αρχείου αλλά και σε πλατφόρμες cloud όπως για παράδειγμα SharePoint. Για τους χρόνους διαγραφής τους ισχύουν τα όσα αναφέρει το συναφές νομικό πλαίσιο.

Πώς ενημερώνονται τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία;

Η ενημέρωση των αιτούντων άσυλο γίνεται από τα κατά τόπους περιφερειακά γραφεία ασύλου, αλλά και αυτοτελή κλιμάκια.

Η ενημέρωση γίνεται πάντα με την παρουσία μεταφραστών, και για να διασφαλιστεί ότι η ενημέρωση θα γίνει σωστά οι αιτούντες πάντα θα ερωτηθούν εάν καταλαβαίνουν το μεταφραστή.

Εάν ισχύει, πώς επιτυγχάνεται η συγκατάθεση των υποκειμένων των δεδομένων;

Αν και η νομική βάση για την επεξεργασία δεν είναι η συγκατάθεση αλλά η εκπλήρωση δημόσιου καθήκοντος, οι αιτούντες άσυλο ενημερώνονται για την όλη διαδικασία κατά την φάση της πρώτης καταγραφής.

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους πρόσβασης και φορητότητας προσωπικών δεδομένων;

Το δικαίωμα φορητότητας δεν έχει εφαρμογή στην περίπτωση αυτή, το δικαίωμα πρόσβασης σαφώς ικανοποιείται, αφού υπάρχουν διαδικασίες για την άσκηση αυτού.

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους διόρθωσης και διαγραφής;

Υπάρχουν διαδικασίες για την άσκηση του δικαιώματος διόρθωσης, και όταν ξεκινήσει η επεξεργασία με την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων θα γίνει προσαρμογή των διαδικασιών/πολιτικών.

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους περιορισμού και εναντίωσης;

Υπάρχουν διαδικασίες για την άσκηση του δικαιώματος περιορισμού και εναντίωσης, και όταν ξεκινήσει η επεξεργασία με την χρήση του αυτοματοποιημένου εργαλείου λήψης αποφάσεων θα γίνει προσαρμογή των διαδικασιών/πολιτικών.

Οι υποχρεώσεις των εκτελούντων την επεξεργασία προσδιορίζονται σαφώς και διέπονται από σύμβαση;

Ναι – θα υπάρξουν σαφείς υποχρεώσεις, βάσει των όσων προβλέπονται στο άρθρο 28 του GDPR.

Σε περίπτωση μεταφοράς δεδομένων εκτός της Ευρωπαϊκής Ένωσης, τα προσωπικά δεδομένα προστατεύονται επαρκώς;

Δεν υπάρχει περίπτωση μεταφοράς δεδομένων εκτός ΕΕ.

6.5.3. Προγραμματισμένα Ή Υπάρχοντα Μέτρα για αντιμετώπιση κινδύνων

Καταστολή κακόβουλου λογισμικού

Δεν ακολουθείται κάποιο πρότυπο για την ασφάλεια πληροφοριών, απλά υπάρχει λογισμικό αντιμετώπισης ιών, που σε κάποιες περιπτώσεις είναι απλά μια free έκδοση του, με περιορισμένες δυνατότητες.

Λαμβάνοντας υπόψιν, και τον τρέχων υλικό-τεχνικό εξοπλισμό που χρησιμοποιείται, και την κατάσταση αυτού, βάση την εκτίμηση επιπτώσεων με τον οδηγό της ENISA, σε καμία περίπτωση δεν μπορεί να εξασφαλιστεί ότι θα παρέχει ένα ικανοποιητικό επίπεδο ασφάλειας.

Απλά αναφέρεται ως μέτρο γιατί υπάρχει έστω και με αυτόν το τρόπο.

Κρυπτογράφηση

Η κρυπτογράφηση αναφέρεται μόνο σε περιπτώσεις VPN, και συγκεκριμένα με την χρήση IPSec ή OpenVPN.

Στην περίπτωση της χρήσης του OpenVPN υπάρουν μια πληθώρα από critical flaws εάν γίνει μια έρευνα στο διαδίκτυο, όπως για παράδειγμα το CVE-2022-0547 με ένα σκορ 9,8.

Και στην συγκεκριμένη περίπτωση, απλά αναφέρονται ως μέτρα γιατί υπάρχουν, αλλά σε καμία περίπτωση από μονά τους δεν εξασφαλίζουν ένα ικανοποιητικό βαθμό ασφάλειας. Εξάλλου, το εργαλείο αυτοματοποιημένης λήψης αποφάσεων αναπόφευκτα δεν θα χειρίζεται κρυπτογραφημένα δεδομένα.

Ανωνυμοποίηση

Θα γίνεται ανωνυμοποίηση των δεδομένων που θα λάβει ο Ανάδοχος που θα υλοποιήσει τον αλγόριθμο μηχανικής μάθησης, αναφορικά με το training set.

Συμβάσεις επεξεργασίας

Θα προβλέπεται ρητά στη σύμβαση ότι η ανάδοχος εταιρεία θα αποκτήσει πρόσβαση σε ανώνυμα δεδομένα καθώς επίσης και ότι ποτέ δεν θα αποκτήσει πρόσβαση στα αρχικά δεδομένα.

6.5.4. Κίνδυνοι - Αθέμιτη Πρόσβαση Στα Δεδομένα

Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα δεδομένων αν επέρχονταν ο κίνδυνος;

Έκθεση των αιτούντων σε κίνδυνο,

Μείωση της εμπιστοσύνης,

Ενόχληση των αιτούντων άσυλο,

Ψυχολογικό στρες

εδώ μπορεί να γίνει αντιληπτό η επαλήθευση των παραπάνω με τα όσα έχουν αναφερθεί στο Risk Analysis - ενότητα Δίκτυο Και Τεχνικοί Πόροι - αλλά και στην AIA - ενότητα 3

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

Παράνομη πρόσβαση,

Ανθρώπινο λάθος,

Κακόβουλο λογισμικό

Ποιες είναι οι πηγές κινδύνου;

Χρήστες (κακόβουλοι ή μη),

Κυβερνοεπιθέσεις,

Τα δεδομένα του training set του αλγορίθμου θα είναι γνωστά στην εταιρεία που θα υλοποιήσει τον αλγόριθμο (και άρα θα έχουν τη δυνατότητα να το χρησιμοποιήσουν για άλλο σκοπό).

Ποια από τα εντοπισμένα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

Μερικώς μπορεί να αντιμετωπιστούν από τα μετρά που έχουν αναφερθεί, με βάση αυτά που έχουν προαναφερθεί.

Καταστολή κακόβουλου λογισμικού,

Κρυπτογράφηση,

Ανωνυμοποίηση των δεδομένων που θα λάβει ο ανάδοχος για το training set.

Πώς υπολογίζετε τη σοβαρότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Η σοβαρότητα του κινδύνου ορίζεται στο μέγιστο και αυτό γιατί έχει αναφερθεί ότι:

Τα δεδομένα τα οποία θα χρησιμοποιηθούν προς επεξεργασία, περιέχουν και ευαίσθητα προσωπικά δεδομένα, όπως για παράδειγμα φύλο, θρησκευτικές πεποιθήσεις κτλ, τα οποία σε

περίπτωση διαρροής θα έχουν σαν αποτέλεσμα να βάλουν ακόμα και σε κίνδυνο την ανθρώπινη ζωή των αιτούντων άσυλο.

Και επίσης τα μέτρα προστασίας τα οποία υπάρχουν, σε καμία περίπτωση δεν προσφέρουν την επιθυμητή προστασία, για τους λόγους που έχουν προαναφερθεί.

Πώς υπολογίζετε την πιθανότητα του κινδύνου, ειδικά ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Η πιθανότητα κινδύνου ορίζεται στο μέγιστο αφού τα μέτρα τα οποία είναι σε εφαρμογή, σε καμία περίπτωση δεν μπορούν έστω να μετριάσουν τους κινδύνους που έχουν προαναφερθεί.

6.5.5. Κίνδυνοι - Ανεπιθύμητη Τροποποίηση Των Δεδομένων

Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα των δεδομένων σε περίπτωση επέλευσης του κινδύνου;

Ψυχολογικό στρες από μια λανθασμένη απόφαση της αίτησης τους για άσυλο,

Περιορισμός συνταγματικά κατοχυρωμένων ελευθεριών,

Ενδεχόμενο αυτοκτονίας που πολλές φορές έχει συμβεί στο παρελθόν,

Ενδεχόμενο εξέγερσης των αιτούντων άσυλο.

και εδώ μπορεί να γίνει αντιληπτό η επαλήθευση των παραπάνω με τα όσα έχουν αναφερθεί στο Risk Analysis - ενότητες Δίκτυο Και Τεχνικοί Πόροι και Διαδικασίες/διεργασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων - αλλά και στην AIA - ενότητες 3 και 7.

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

Ανθρώπινο λάθος ή δόλος,

Παράνομη πρόσβαση,

Κακόβουλο λογισμικό,

Λάθος απόφαση του αλγορίθμου

Ποιες είναι οι πηγές κινδύνου;

Εξουσιοδοτημένος Χρήστης,

Εισβολέας,

Κυβερνοεπίθεση

Μη σωστές παράμετροι στον αλγόριθμο – μη ικανοποιητικός αλγόριθμος

Ποια από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

Μερικώς μπορεί να αντιμετωπιστούν από τα μετρά που έχουν αναφερθεί, με βάση αυτά που έχουν προαναφερθεί.

Καταστολή κακόβουλου λογισμικού

Κρυπτογράφηση

Ανθρώπινος παράγοντας για την τελική λήψη απόφασης αναφορικά με αίτημα ασύλου – τεκμηρίωση της απόφασής του, η οποία δεν θα πρέπει να βασίζεται αποκλειστικά στο αυτοματοποιημένο εργαλείο.

Πώς εκτιμάτε τη σοβαρότητα του κινδύνου, ιδίως ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Η σοβαρότητα του κινδύνου τίθεται στο μέγιστο και αυτό λαμβάνοντας υπόψιν ότι η απώλεια της ακεραιότητας έχει σημαντικές συνέπειες, αφού σε περίπτωση μιας τροποποίησης των δεδομένων μπορεί να οδηγήσει σε μη αναστρέψιμες συνέπειες όπως για παράδειγμα το να προβεί κάποιος από τους αιτούντες σε αυτοκτονία.

Τα μέτρα τα οποία έχουν ληφθεί δεν μπορούν να καλύψουν ενδεχόμενο ανθρώπινο δόλο, αλλά και φυσικά και κυβερνοεπιθέσεις αφού δεν είναι μια πλήρη σειρά μέτρων που μπορούν να αποτρέψουν κάτι τέτοιο.

Πώς εκτιμάτε την πιθανότητα του κινδύνου, ιδίως σε σχέση με τις απειλές, τις πηγές κινδύνου και τα προγραμματισμένα μέτρα;

Η πιθανότητα κινδύνου επίσης τίθεται σε μέγιστο, και αυτό λαμβάνοντας υπόψιν ότι τα μέτρα τα οποία έχουν ληφθεί δεν μπορούν να καλύψουν ενδεχόμενο ανθρώπινο δόλο, αλλά και φυσικά και

κυβερνοεπιθέσεις αφού δεν είναι μια πλήρη σειρά μέτρων που μπορούν να αποτρέψουν κάτι τέτοιο. Επίσης, αν και υπάρχει σαφής πρόβλεψη για ανωνυμοποίηση των δεδομένων που θα χρησιμοποιηθούν από τον ανάδοχο, δεν υπάρχει πρόβλεψη για τον έλεγχο της αποτελεσματικότητας της ανωνυμοποίησης (πώς αυτή θα γίνεται, γιατί θα κρίνεται επαρκής κτλ.)

6.5.6. Κίνδυνοι - Εξαφάνιση Δεδομένων

Ποιες θα μπορούσαν να είναι οι κύριες επιπτώσεις στα υποκείμενα των δεδομένων σε περίπτωση επέλευσης του κινδύνου;

Σημαντικές, αφού σε μια τέτοια περίπτωση θα χρειάζεται να γίνει επανασυλλογή όλων των στοιχείων με ότι συνεπάγεται αυτό σε χρονική καθυστέρηση για την λήψη τελικής απόφασης,

Ψυχολογικό στρες,

Αυτοκτονικές τάσεις

Ποιες είναι οι κύριες απειλές που θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου;

Ανθρώπινο λάθος,

Κακόβουλο λογισμικό,

Δολιοφθορά,

Φυσική καταστροφή,

Κυβερνοεπίθεση

Ποιες είναι οι πηγές κινδύνου;

Φυσικές καταστροφές,

Εξουσιοδοτημένος χρήστης,

Κυβερνοεπίθεση,

Κακόβουλο λογισμικό

Ποια από τα προσδιορισθέντα μέτρα συμβάλλουν στην αντιμετώπιση του κινδύνου;

Στην συγκεκριμένη περίπτωση κανένα από τα εφαρμοζόμενα μέτρα δεν μπορούν να εξασφαλίσουν η τουλάχιστον να μετριάσουν την μη διαθεσιμότητα των δεδομένων, και αυτό αποτελεί έναν σημαντικό ανασταλτικό παράγοντα εάν λάβουμε υπόψιν και τις εκτιμήσεις επιπτώσεων που διενεργήθηκαν και με την βοήθεια του οδηγού της ENISA, αλλά και της AIA.

Πώς εκτιμάτε τη σοβαρότητα του κινδύνου, ιδίως ανάλογα με τις πιθανές επιπτώσεις και τα προγραμματισμένα μέτρα;

Με βάση και την προηγούμενη απάντηση, τίθεται στο μέγιστο αφού ενδεικτικά μπορεί να αναφερθεί ότι οι αιτούντες άσυλο στην περίπτωση μιας απώλειας της διαθεσιμότητας, θα βρεθούν κάτω από έντονο ψυχολογικό στρες, και όταν η απώλεια αυτή δεν είναι αναστρέψιμη μπορεί να οδηγήσει ακόμα και σε αυτοκτονία.

Πώς εκτιμάτε την πιθανότητα του κινδύνου, ιδίως σε σχέση με τις απειλές, τις πηγές κινδύνου και τα προγραμματισμένα μέτρα;

Η πιθανότητα του κινδύνου τίθεται στο μέγιστο, λαμβάνοντας υπόψιν ότι δεν υπάρχει καμία πολιτική (έχει αναφερθεί και σε προηγούμενες εκτιμήσεις επιπτώσεων), αλλά και ούτε κάποια οδηγία για την ύπαρξη μηχανισμού εφεδρικών αντιγραφών, αλλά και στην μη ύπαρξη προγραμματισμένων μέτρων, γίνεται αντιληπτό ότι δεν μπορεί να αντιμετωπιστεί μια απώλεια διαθεσιμότητας.

Μετά και την ολοκλήρωση της DPIA, φαίνονται οι σχέσεις των Πιθανών επιπτώσεων, των Απειλών, των Πηγών και των Μέτρων (εικόνα 6.11) σε σχέση με:

- Αθέμιτη Πρόσβαση Στα Δεδομένα
- Ανεπιθύμητη Τροποποίηση Των Δεδομένων
- Εξαφάνιση Δεδομένων

Εικόνα 6.11: Επισκόπηση κινδύνων

Και στην (εικόνα 6.12) την καταγραφή των παραγόντων που επηρεάζουν την πιθανότητα εμφάνισης κινδύνων κατά την διάρκεια της επεξεργασίας, καθώς και την εκτίμηση για το εύρος των επιπτώσεων που θα έχει η εμφάνιση των κινδύνων.

Εικόνα 6.12: Χαρτογράφηση κινδύνων

Επομένως λαμβάνοντας υπόψιν:

- την Risk analysis
- την AIA
- και τέλος ότι τα προγραμματισμένα ή υπάρχοντα μέτρα δεν μπορούν έστω να μετριάσουν τους κινδύνους και τις απειλές,

η συγκεκριμένη επεξεργασία, δεν μπορεί να διεξαχθεί ως έχει: χρειάζονται πρόσθετα μέτρα και προηγούμενη διαβούλευση με την Αρχή Προστασίας Δεδομένων, σύμφωνα με το άρθρο 36 του GDPR.

Κεφάλαιο 7 –

Επίλογος

Η παρούσα μεταπτυχιακή διατριβή επικεντρώνεται στη διαχείριση των κινδύνων προστασίας προσωπικών δεδομένων που σχετίζονται με την επεξεργασία μεγάλου όγκου προσωπικών δεδομένων με την χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων τα οποία βασίζονται σε αλγορίθμους μηχανικής μάθησης, με γνώμονα την διερεύνηση των συσχετίσεων διαφόρων εργαλείων λογοδοσίας όπως η διαχείριση κινδύνων ασφάλειας, η εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα (DPIA) αλλά και η αλγοριθμική εκτίμηση αντικτύπου (AIA). .

Με βάση το παραπάνω, καταρχήν αναλύεται το υπάρχον νομικό πλαίσιο που αφορά την προστασία των προσωπικών δεδομένων γενικότερα στη βάση του GDPR, και επίσης στη συνέχεια, στο πλαίσιο της ως άνω διερεύνησης, μελετάται μία συγκεκριμένη μελέτη περίπτωσης, στο πλαίσιο της οποίας εκπονούνται εκτιμήσεις επιπτώσεων με διάφορα διαθέσιμα συναφή εργαλεία, και συγκεκριμένα:

- Ανάλυση κινδύνων ασφαλείας σύμφωνα με τον οδηγό του Ευρωπαικού Οργανισμού Κυβερνοασφάλειας «ENISA» **[21]**, αλλά επίσης και τον αντίκτυπο που έχει αυτήν η επεξεργασία στα προσωπικά και ευαίσθητα προσωπικά δεδομένα των αιτούντων άσυλο ως προς την Εμπιστευτικότητα, την Ακεραιότητα και την Διαθεσιμότητα

- Πραγματοποίησή AIA, με την βοήθεια του εργαλείου- ερωτηματολογίου του Υπουργείου Οικονομικών του Καναδά **[18]**

- Και τέλος, ΕΑΠΔ (Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων) στην βάση του GDPR, κάνοντας χρήση του εργαλείου PIA της Γαλλικής Αρχής Προστασίας Δεδομένων CNIL**[11]**

Μέσα από όλα τα παραπάνω γίνεται μια προσπάθεια να αναδειχθεί η σημαντικότητα της AIA σαν εργαλείο εκτίμησης επιπτώσεων όταν γίνεται χρήση αυτοματοποιημένων εργαλείων λήψης αποφάσεων αλλά και του συνδυασμού αυτής με άλλα εργαλεία εκτίμησης επιπτώσεων και την ανάπτυξη μιας ενιαίας μεθοδολογίας ελέγχου. Απώτερος σκοπός η ανάπτυξη ενός γενικότερου

μεθοδολογικού πλαισίου το οποίο μπορεί να αξιοποιείται από οποιονδήποτε υπεύθυνο επεξεργασίας, ανεξαρτήτως της υποκείμενης επεξεργασίας δεδομένων.

7.1 Συμπεράσματα

Καταρχήν θα μπορούσε να ειπωθεί ότι ο GDPR σαφώς και παρέχει ένα πλαίσιο προστασίας προσωπικών και ευαίσθητων προσωπικών δεδομένων, αλλά εκ των πραγμάτων όχι τόσο σε τεχνικό επίπεδο όσο σε νομικό επίπεδο, παρέχοντας ένα σύνολο άρθρων που έχουν σαν σκοπό την νομική προστασία των ατομικών δικαιωμάτων και ελευθεριών των πολιτών.

Το δεύτερο που μπορεί να ειπωθεί είναι ότι μπορεί να υπάρξουν εργαλεία, κανονισμοί και κατευθυντήριες γραμμές που δημιουργούν ένα γενικό πλαίσιο για τον έλεγχο των αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ.

Η μελέτη περίπτωσης που εκπονήθηκε έδειξε ότι τόσο η AIA όσο και η DPIA, δημιουργώντας ένα κοινό μεθοδολογικό πλαίσιο μπορούν να βοηθήσουν στον εντοπισμό και τον μετριασμό πιθανών κινδύνων που σχετίζονται με αυτές τις τεχνολογίες. Στο πλαίσιο της μεθοδολογίας που αναπτύξαμε, η AIA προηγήθηκε της DPIA έτσι ώστε κατά την εκπόνηση της DPIA να έχουν ήδη εξεταστεί τυχόν κιίνδυνοι που απορρέουν από αυτόν καθ' αυτόν τον αλγόριθμο μηχανικής μάθησης.

Επίσης κατευθυντήριες γραμμές και βέλτιστες πρακτικές μπορούν να αναπτυχθούν από επίσημα κυβερνητικά όργανα για να βοηθήσουν τις εταιρείες να αναπτύξουν και να εφαρμόσουν υπεύθυνες πολιτικές και πρακτικές για τη χρήση αυτών των τεχνολογιών.

Για παράδειγμα, η IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems έχει αναπτύξει μια σειρά κατευθυντήριων γραμμών για ηθικό και κοινωνικά υπεύθυνο σχεδιασμό και εφαρμογή AI.

Σε συνέχεια των ερευνητικών ερωτημάτων θα μπορούσε να ειπωθεί ότι σαφώς και μπορεί ένα αυτοματοποιημένο εργαλείο λήψης αποφάσεων και δημιουργίας προφίλ να ελεγχθεί κατά την φάση της ανάπτυξής του, έτσι ώστε να προβλεφθούν εγκαίρως παραβιάσεις στον τρόπο επεξεργασίας, μεταβίβασης δεδομένων και άλλοι κίνδυνοι προστασίας δεδομένων που απορρέουν από αυτό, και αυτό έγινε αντιληπτό από την εκπόνηση της AIA στην μελέτη περίπτωσης όπου η AIA κατέληξε σε υψηλούς κινδύνους – πιο εστιασμένους από ό,τι ενδεχομένως θα μπορούσε να επιτύχει η DPIA.

Συνεχίζοντας με τα ερευνητικά ερωτήματα, θα πρέπει να αναφερθεί ότι:

Η Εκτίμηση Επιπτώσεων Προστασίας Δεδομένων (DPIA) και η Αλγοριθμική Εκτίμηση Επιπτώσεων (AIA) είναι δύο ξεχωριστές αξιολογήσεις που μπορούν να χρησιμοποιηθούν για την αξιολόγηση των κινδύνων και των επιπτώσεων που σχετίζονται με την επεξεργασία προσωπικών δεδομένων και τη χρήση αλγορίθμων τεχνητής νοημοσύνης, αντίστοιχα.

- Η DPIA είναι μια διαδικασία που χρησιμοποιείται για τον εντοπισμό, την αξιολόγηση και τον μετριασμό των κινδύνων που σχετίζονται γενικά με την επεξεργασία προσωπικών δεδομένων.

- Η AIA, από την άλλη πλευρά, είναι μια διαδικασία που χρησιμοποιείται για την αξιολόγηση του πιθανού αντίκτυπου των συστημάτων τεχνητής νοημοσύνης στα άτομα και την κοινωνία.

Σε περιπτώσεις όπου τα δεδομένα υποβάλλονται σε επεξεργασία μέσω τεχνικών τεχνητής νοημοσύνης, ενδέχεται να απαιτείται τόσο η DPIA όσο και η AIA για την αξιολόγηση των κινδύνων και των επιπτώσεων που σχετίζονται με την επεξεργασία. Η DPIA θα επικεντρωνόταν στους κινδύνους που συνδέονται με την επεξεργασία προσωπικών δεδομένων, ενώ η AIA θα επικεντρωνόταν στους κινδύνους που σχετίζονται με τη χρήση αλγορίθμων AI. Ως εκ τούτου, είναι δυνατός και σκόπιμος ο συνδυασμός DPIA και ΔΑΑ για την παροχή συνολικής αξιολόγησης των κινδύνων και των επιπτώσεων που σχετίζονται με την επεξεργασία προσωπικών δεδομένων μέσω τεχνικών τεχνητής νοημοσύνης. Αντίστοιχα, σε αυτό το μεθοδολογικό πλαίσιο μπορεί να ενταχθεί και μία γενική διαχείριση κινδύνων ασφάλειας: στην προσέγγιση που ακολουθήσαμε η διαχείριση κινδύνων ασφάλειας προηγήθηκε χρονικά τόσο της AIA όσο και της DPIA, με το σκεπτικό ότι δύναται να εντοπίσει βασικά κενά ασφάλειας σε ένα αρχικό στάδιο και να τα αντιμετωπίσει.

Επίσης ως συμπέρασμα και ενδεχομένως ως πρόταση για μελλοντική έρευνα τα δύο εργαλεία λογοδοσίας AIA και DPIA να «επικοινωνούν»(ενδεχομένως σε ένα κοινό λογισμικό), έτσι ώστε στις ερωτήσεις της DPIA που σχετίζονται με το εργαλείο αυτό να «συμπληρώνονται» αυτόματα οι απαντήσεις από το AIA εργαλείο. Αυτό αποτελεί μία ιδιαίτερη πρόκληση, λαμβάνοντας υπόψη ότι για την AIA χρειάζεται ενεργή συμμετοχή και του κατασκευαστή του αλγορίθμου, ενώ για την DPIA η ευθύνη βαρύνει αποκλειστικά τον υπεύθυνο επεξεργασίας (δηλαδή τον χρήστη της τεχνολογίας που υλοποιεί τον αλγόριθμο).

Το πιο σημαντικό όμως είναι η ύπαρξη πολλών και διαφορετικών τομέων όπως η υγεία, τα κοινωνικά επιδόματα, τα οικονομικά και άλλοι μπορούν ενδεχομένως να επηρεάσουν τα ατομικά δικαιώματα και ελευθερίες των εμπλεκόμενων ατόμων. Ως εκ τούτου, είναι απαραίτητο να υπάρχει ένα κατάλληλο σύστημα ελέγχου για την προστασία των δικαιωμάτων και των ελευθεριών των ατόμων.

Ένα γενικό πλαίσιο για την προστασία των ατομικών δικαιωμάτων και ελευθεριών μπορεί να δημιουργηθεί μέσω νόμων και κανονισμών για την προστασία δεδομένων, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση, ο οποίος ισχύει για όλους τους τομείς που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Ο GDPR απαιτεί από τους οργανισμούς να διασφαλίζουν ότι οποιαδήποτε αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένου του προφίλ, είναι δίκαιη, διαφανής και βασίζεται σε νόμιμους σκοπούς, σε συνεργασία με άλλα εργαλεία όπως έχει ειπωθεί για παράδειγμα την AIA. Είναι σημαντικό εξάλλου ότι και η πρόταση Κανονισμού της ΕΕ για την τεχνητή νοημοσύνη, η οποία δημοσιεύτηκε το 2022 (δεν έχει ακόμα οριστικοποιηθεί/ψηφιστεί κατά τη στιγμή που γράφονται οι γραμμές αυτές) αναφέρει την ανάγκη ανάλυσης των επιπτώσεων του αλγορίθμου ως προς τα προσωπικά δεδομένα.

Είναι σημαντικό όμως για τους οργανισμούς να λαμβάνουν υπόψη τους συγκεκριμένους κανονισμούς και κατευθυντήριες γραμμές που διέπουν τους αντίστοιχους τομείς τους κατά την εφαρμογή αυτοματοποιημένων εργαλείων λήψης αποφάσεων και δημιουργίας προφίλ. Θα πρέπει επίσης να δημιουργήσουν ένα κατάλληλο σύστημα ελέγχου που να διασφαλίζει τη συμμόρφωση με αυτούς τους κανονισμούς και τις κατευθυντήριες γραμμές, καθώς και την προστασία των ατομικών δικαιωμάτων και ελευθεριών. Αυτό περιλαμβάνει τη διεξαγωγή αξιολογήσεων επιπτώσεων, την εφαρμογή κατάλληλων διασφαλίσεων και την παροχή στα άτομα πρόσβασης στις πληροφορίες και της ικανότητας άσκησης των δικαιωμάτων τους.

Βιβλιογραφία

[01] Algorithmic Impact Assessment. (n.d.). Retrieved from Goverment of Canada: https://open.canada.ca/aia-eia-js/?lang=en

[02] Brunette, E. S., Flemmer, R., & Flemmer, C. (2009). A review of artificial intelligence. 4th International Conference on Autonomous Robots and Agents, ICARA (pp. 1-8). Wellington, New Zealand: IEEE. doi:10.1109/ICARA.2000.4804025

[03] Bygrave, L. (2019). Article 22 Automated individual decision-making, including profiling. In C. Kuner, The EU General Data Protection Regulation (GDPR) (pp. 522-540). Brussels: CPI Group . doi:10.1093/oso/9780198826491.003.0055

[04] canada-ca.github.io. (n.d.). Algorithmic Impact Assessment v0.9.1 . Retrieved from GitHub: https://github.com/canada-ca/aia-eia-js

[05] CNIL. (n.d.). The open source PIA software helps to carry out data protection impact assessment. Retrieved from https://www.cnil.fr/: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

[06] Dreyer, S., & Schulz, W. (2019, January). The General Data Protection Regulation and Automated Decision-making: Will it deliver? 1-48. doi:10.11586/2018018

[07] Groningen, U. o. (n.d.). *Starting with a DPIA methodology for human subject research*. Retrieved from University of Groningen: https://www.rug.nl/research/research-data-management/downloads/c2-dataprotection-dl/dpia_guidance_doc_v1_pub.pdf

[08] itgovernance. (n.d.). *DPIA Tool*. Retrieved from itgovernance: https://www.itgovernance.co.uk/shop/product/dpia-tool

[09] Ivanova, Y. (2020, January). The Data Protection Impact Assessment as a Tool. SSRN Electronic Journal , 1-20. doi:DOI: 10.2139/ssrn.3584219

[10] Mitchell, T., Buchanan, B., DeJong, G., Dietterich, T., Rosenbloom, P., & Waibel, A. (1990, 06 01). Machine Learning. *Annual Review of Computer Science*, pp. 417-433. doi:10.1146/annurev.cs.04.060190.002221

[11] Moss, E., Watkins, E. A., Singh, R., & Elish, M. C. (2021, July). Algorithmic Impact Assessments and Accountability. *SSRN Electronic Journal*, pp. 1-12. doi:10.2139/ssrn.3877437

[12] Parliament, E. (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. Official Journal of the European Communities.

[13] Programme, E. H. (2020). *Complete guide to GDPR compliance*. Retrieved from GDPR.EU: https://gdpr.eu/

[14] Programme, E. H. (2020). *Sample DPIA template*. Retrieved from GDPR.EU: https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

[15] Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018). ALGORITHMIC IMPACT ASSESSMENTS A PRACTICAL FRAMEWORK FOR PUBLIC AGENCY ACCOUNTABILITY. *AI Now Institute*, 1-22.

[16] Sartor, G. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.* European Parliamentary Research Service, Scientific Foresight Unit (STOA), Brussels. doi:10.2861/293

[17] Selbst, A. D. (2021, June 15). AN INSTITUTIONAL VIEW OF ALGORITHMIC IMPACT ASSESSMENTS. *Harvard Journal of Law & Technology, 35*, 1-75.

[18] SourceForge. (n.d.). *PrivIQ*. Retrieved from SourceForge: https://sourceforge.net/software/product/PrivIQ/

[19] Watkins, E. A., Metcalf, J., & Elish, M. C. (2020, January). Governing with Algorithmic Impact Assessments: Six Observations. *SSRN Electronic Journal* , 1-13. doi:DOI: 10.2139/ssrn.3584818

[20] *What is automated individual decision-making and profiling?* (n.d.). Retrieved from ico.Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/

[21] ENISA. (2018). *Handbook on Security of Personal Data Processing.* Athens: European Union Agency for Network and Information Security (ENISA). doi:10.2824/569768

[22] Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016, July-December). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1-21. doi://doi.org/10.1177/2053951716679679

[23] Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 389-399. doi:doi.org/10.1038/s42256-019-0088-2

[24] Diakopoulos, N. (2016). Accountability in Algorithmic Decision Making. *Communications of the ACM, 59*, 56-62. doi:10.1145/2844110

[25] Raji, I., & Buolamwini, J. (2019). Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products. *Conference on Artificial Intelligence, Ethics, and Society* (pp. 19-28). Honolulu HI USA: Association for Computing Machinery. doi:10.1145/3306618.3314244

[26] Kleek, M., Veale, M., Lyngs, U., Zhao, J., Shadbolt, N., & Binns, R. (2018). 'It's Reducing a Human Being to a Percentage': Perceptions of Justice in Algorithmic Decisions. *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-14). Montreal QC Canada: ACM . doi:10.1145/3173574.3173951

[27] Caliskan, A., Bryson, J. J., & Narayanan, A. (2017, April 14). Semantics derived automatically from language corpora contain human-like biases. *356*, pp. 183-186. doi:10.1126/science.aal4230

[28] Mittal, A., & Subramanyam, A. (2018, May 12). Automated Decision Making using Machine Learning Algorithms. Advanced Research in Computer Science, 9, pp. 213-218.

[29] Li, K. (2019). Machine Learning Algorithms in Automated Decision-Making. *International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-5). Coimbator, India: IEEE.