ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΑΙΩΜΑΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

ΔΕΛΗΓΙΩΡΓΗ ΕΛΕΥΘΕΡΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΗ

ΜΠΑΖΙΑΝΑ ΠΕΡΙΣΤΕΡΑ
ΕΠΙΚΟΥΡΗ ΚΑΘΗΓΗΤΡΙΑ

Λαμία Ιούλιος έτος 2025

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΑΙΩΜΑΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

ΔΕΛΗΓΙΩΡΓΗ ΕΛΕΥΘΕΡΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΗ

ΜΠΑΖΙΑΝΑ ΠΕΡΙΣΤΕΡΑ
ΕΠΙΚΟΥΡΗ ΚΑΘΗΓΗΤΡΙΑ

Λαμία Ιούλιος έτος 2025

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

AUTOMATED DATA SUBJECT RIGHTS MANAGMENT

DELIGIORGI ELEFTHERIA

FINAL THESIS

ADVISOR

BAZIANA PERISTERA
ASSISTANT PROFESSOR

Lamia July year 2025

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 10/07/2025

Η Δηλ.

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία, εστιάζει στην εφαρμογή των δικαιωμάτων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), με ιδιαίτερη έμφαση στο δικαίωμα της πρόσβασης (Άρθρο 15). Παρότι ο Κανονισμός ορίζει ένα σαφές νομικό πλαίσιο για την προστασία των δικαιωμάτων των υποκειμένων, στην πράξη πολλοί οργανισμοί εξακολουθούν να μην υποστηρίζουν τεχνικά την ολοκληρωμένη εφαρμογή του. Η απουσία μιας πρακτικής λύσης για τη διαχείριση αυτών των δικαιωμάτων, αποτελεί ένα διαχρονικό πρόβλημα, τόσο για τους οργανισμούς όσο και για τους πολίτες. Επομένως, η δημιουργία ενός συστήματος που θα αυτοματοποιούσε τη διαχείριση των δικαιωμάτων των υποκειμένων, θα μπορούσε να διευκολύνει τόσο τα άτομα να έχουν έλεγχο επί των προσωπικών τους δεδομένων, όσο και τους οργανισμούς να συμμορφώνονται με τον Κανονισμό. Σε αυτό το πλαίσιο, σχεδιάστηκε και υλοποιήθηκε ένα σύστημα, που αποσκοπεί στην αυτοματοποίηση της διαχείρισης των δικαιωμάτων των υποκειμένων. Η ανάπτυξή του ακολούθησε τη μεθοδολογία του μοντέλου καταρράκτη, περιλαμβάνοντας την ανάλυση περιπτώσεων χρήσης και τις απαιτήσεις από την πλευρά των βασικών ρόλων του συστήματος, καθώς και το σχεδιασμό της αρχιτεκτονικής. Ακολούθησε η υλοποίησή του με χρήση σύγχρονων τεχνολογιών, ενώ η αξιολόγησή του πραγματοποιήθηκε με τη δημιουργία πέντε βασικών χρηστών, χρησιμοποιώντας συμβολικά δεδομένα ταυτοποίησης. Εν κατακλείδι, το προτεινόμενο σύστημα αποτελεί μια προσέγγιση για τη διαχείριση αιτημάτων βάσει του ΓΚΠΔ, ενώ παράλληλα δημιουργεί βάσεις για μελλοντική επέκταση και αξιοποίησή του σε πιο ολοκληρωμένα σενάρια χρήσης.

Λέξεις κλειδιά: Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), Άρθρο 15, Δικαίωμα Πρόσβασης, Υποκείμενα των Δεδομένων, Προσωπικά Δεδομένα, Αίτημα Πρόσβασης.

ABSTRACT

The subject of this thesis focuses on the implementation of the rights granted by the General Data Protection Regulation (GDPR), with particular emphasis on the right of access (Article 15). Although the Regulation establishes a clear legal framework for the protection of individuals' rights, in practice, many organizations still lack the technical infrastructure to fully support its implementation. The absence of a practical solution for managing these rights remains a longstanding challenge for both organizations and data subjects. Therefore, a system was designed and developed to automate the management of data subject rights, enhancing both individual control over personal data and organizational compliance with the Regulation. Its development followed the waterfall model, incorporating use case analysis and requirements specification, based on the system's primary actors, along with the architectural design. The implementation was carried out using modern technologies, and its evaluation took place using five primary users with basic identification data. In conclusion, the proposed system provides a viable solution for handling GDPR-related requests, while also laying the groundwork for future expansion and integration into more comprehensive use case scenarios.

Keywords: General Data Protection Regulation (GDPR), Article 15, Right of Access, Data Subjects, Personal Data, Access Request.

Table of Contents

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Η εξασφάλιση της ιδιωτικότητας αποτελεί έναν από τους σημαντικότερους προβληματισμούς της ψηφιακής εποχής, δεδομένης της αυξανόμενης ψηφιακής διακίνησης προσωπικών δεδομένων καθώς και του όγκου των προσωπικών δεδομένων που συλλέγονται και επεξεργάζονται καθημερινά. Ήδη από το 2002 η Ευρωπαϊκή Ένωση (ΕΕ) είχε προτείνει μεταρρυθμίσεις των κανόνων προστασίας των δεδομένων, με κύριο σκοπό την αύξηση του ελέγχου των δεδομένων των χρηστών.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), ο οποίος εφαρμόζεται από τον Μάιο του 2018, υιοθετήθηκε με σκοπό να κατοχυρώσει τα δικαιώματα των πολιτών και να διαμορφώσει ένα σταθερό πλαίσιο λογοδοσίας για όσους χειρίζονται προσωπικές πληροφορίες. Παρά τις αυξημένες υποχρεώσεις συμμόρφωσης που απορρέουν από τον Κανονισμό, πολλοί οργανισμοί εξακολουθούν να μην υποστηρίζουν τεχνικά την ολοκληρωμένη εφαρμογή του.

Μεταξύ άλλων διατάξεων, ο Κανονισμός, δίνει ιδιαίτερη έμφαση στα δικαιώματα των υποκειμένων των δεδομένων. Πιο συγκεκριμένα, ορίζει μια σειρά δικαιωμάτων τα οποία είναι τα εξής: δικαίωμα ενημέρωσης, δικαίωμα πρόσβασης, δικαίωμα διόρθωσης (ανακριβών δεδομένων), δικαίωμα διαγραφής («δικαίωμα στη λήθη»), δικαίωμα φορητότητας των δεδομένων, δικαίωμα εναντίωσης, δικαίωμα περιορισμού της επεξεργασίας, δικαίωμα μη υποβολής σε αυτοματοποιημένη λήψη αποφάσεων.

Το θέμα της παρούσας εργασίας προέκυψε από το ότι, στην πράξη, η υλοποίηση δικαιωμάτων συχνά γίνεται με χειροκίνητες διαδικασίες, που είναι χρονοβόρες, επιρρεπείς σε σφάλματα κ.α. Το γεγονός ότι πολλοί οργανισμοί είτε δεν διαθέτουν μηχανισμούς για τη διαχείριση αιτημάτων των υποκειμένων είτε τους διαχειρίζονται με μη αυτοματοποιημένες, αναποτελεσματικές μεθόδους, αποτελεί πρόβλημα τόσο για τα άτομα (υποκείμενα των δεδομένων), διότι δυσκολεύονται να ασκήσουν τα δικαιώματά τους, όσο και για τους υπεύθυνους επεξεργασίας, οργανισμούς, κτλ., που δεν μπορούν ή αποτυγχάνουν να αποδείξουν τη συμμόρφωση με τον Κανονισμό.

Στο πλαίσιο αυτό, υλοποιήθηκε ένα πληροφοριακό σύστημα, το οποίο διαχειρίζεται αιτήματα άσκησης του Δικαιώματος στην Πρόσβαση (Άρθρο 15 του ΓΚΠΔ) από τα υποκείμενα των

δεδομένων, προσφέροντας έτσι αυτοματισμούς, διαφάνεια και ευκολία παρακολούθησης των δεδομένων προσωπικού χαρακτήρα.

Η δομή της παρούσας εργασίας διαμορφώνεται ως εξής:

- Παρουσιάζεται το θεωρητικό υπόβαθρο και η νομική βάση του ΓΚΠΔ, δίνοντας έμφαση στο Δικαίωμα της Πρόσβασης.
- Ακολουθεί η αναλυτική σχεδίαση που έγινε για το σύστημα, με βάση τις απαιτήσεις και τις λειτουργικές ανάγκες.
- Περιγράφεται η υλοποίηση του συστήματος καθώς και το παράδειγμα χρήσης του.
- Τέλος, συνοψίζονται τα βασικά συμπεράσματα της εργασίας, καθώς και μελλοντικές προτεινόμενες εργασίες επέκτασης επί του θέματος.

ΚΕΦΑΛΑΙΟ 2 Γενικός Κανονισμός για την Προστασία Δεδομένων

2.1. Εισαγωγή στον ΓΚΠΔ

Στη σύγχρονη κοινωνία, τα προσωπικά δεδομένα συλλέγονται και υπόκεινται σε επεξεργασία τόσο από δημόσιους όσο και από ιδιωτικούς φορείς, για διάφορους σκοπούς και με διαφορετικά μέσα. Όμως, τα άτομα βρίσκονται κυρίως σε μια μειονεκτική θέση ως προς την κατανόηση του τρόπου επεξεργασίας των προσωπικών τους δεδομένων, καθώς και της τεχνολογίας που χρησιμοποιείται σε κάθε περίπτωση.

Προκειμένου να διασφαλίζεται η προστασία δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων, ο ΓΚΠΔ (*Γενικός Κανονισμός για την Προστασία Δεδομένων ή εν συντομία* ΓΚΠΔ) δημιούργησε ένα συνεκτικό και ισχυρό πλαίσιο, αυστηρότερο του προηγούμενου νομοθετικού πλαισίου (Οδηγία 95/46/ΕΚ και Ν. 2472/1997) και ικανό να εφαρμόζεται γενικότερα με τους διάφορους τύπους επεξεργασίας, συμπεριλαμβανομένων ειδικών διατάξεων που αφορούν τα δικαιώματα των υποκειμένων των δεδομένων.

Ειδικότερα, ο ΓΚΠΔ απαιτεί από τους οργανισμούς να συμμορφώνονται πλήρως με το νομικό πλαίσιο που ορίζει, τοποθετώντας έτσι τα δικαιώματα των φυσικών προσώπων στο επίκεντρο [1], με απώτερο στόχο την αύξηση του ελέγχου που έχουν οι πολίτες της Ευρωπαϊκής Ένωσης (ΕΕ) και του Ευρωπαϊκού Οικονομικού Χώρου, σχετικά με τα προσωπικά τους δεδομένα, την ενίσχυση της προστασίας της ιδιωτικής ζωής μέσω της «ιδιωτικότητας εκ σχεδιασμού» (*Privacy by Design*) και τη δημιουργία μιας κοινής νομοθετικής βάσης για την προστασία των δεδομένων και της ιδιωτικής ζωής [2].

Προκύπτει, πως με τον Κανονισμό προσφέρεται στα υποκείμενα των δεδομένων η δυνατότητα άσκησης πληθώρας δικαιωμάτων σε σχέση με την επεξεργασία των προσωπικών δεδομένων που τα αφορούν. Πριν γίνει ανάλυση των σημαντικότερων εκ τούτων, αξίζει να αναφερθεί η ορολογία τόσο για τους διάφορους ρόλους/φορείς που χρησιμοποιούνται στον ΓΚΠΔ — και θα αναφερθούν και στην παρούσα εργασία — όσο και για το ποια θεωρούνται προσωπικά δεδομένα.

2.1.α. Ορισμοί

Υποκείμενα των δεδομένων (ΥΔ - DS): τα φυσικά πρόσωπα στα οποία αναφέρονται και συλλέγονται τα προσωπικά δεδομένα.

Υπεύθυνος Επεξεργασίας (ΥΕ - DC): οργανισμός ή φορέας που καθορίζει τον/τους σκοπό/σκοπούς της επεξεργασίας των δεδομένων καθώς και τη συλλογή τους.

Εκτελών Επεξεργασίας (ΕΕ - DP): φορείς που συλλέγουν, επεξεργάζονται ή/και διαβιβάζουν τα δεδομένα εκ μέρους του υπεύθυνου επεξεργασίας.

Προσωπικά Δεδομένα: στο το Άρθρο 4 (1)(13)(14)(15) του ΓΚΠΔ [5] ορίζονται τρείς κύριες κατηγορίες: γενετικά δεδομένα, βιομετρικά δεδομένα, ιατρικά δεδομένα. Επιπρόσθετα, το Άρθρο 9 επεκτείνει τις κατηγορίες αυτές σε πιο ειδικές: φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές και φιλοσοφικές πεποιθήσεις, γενετήσιος προσανατολισμός και περιορίζει την επεξεργασία αυτών των ειδικών κατηγοριών.

Να σημειωθεί πως ο όρος “Υπεύθυνος Επεξεργασίας” πολλές φορές, για ευκολία ανάγνωσης, χρησιμοποιείται ενιαία για να περιγράψει τόσο τους Υπεύθυνους όσο και τους Εκτελούντες Επεξεργασίας [2].

2.2. Δικαιώματα Γενικά

Αφού δόθηκαν σύντομοι ορισμοί στους βασικούς όρους, μπορούμε να επιστρέψουμε στην ανάλυση των σημαντικότερων δικαιωμάτων, σύμφωνα με το άρθρο [2], τα οποία είναι τα εξής:

- Ο διαχειριστής των δεδομένων οφείλει να μεταβιβάζει πληροφορίες στα υποκείμενα των δεδομένων με εύκολα κατανοητό και διαφανή τρόπο (Άρθρο 12).
- Το Δικαίωμα Πρόσβασης, που επιτρέπει στο υποκείμενο των δεδομένων να ζητήσει τόσο πρόσβαση στα προσωπικά του δεδομένα όσο και επιβεβαίωση για το εάν αυτά υπόκεινται σε επεξεργασία, καθώς επίσης, εάν αυτό συμβαίνει, να λάβει πληροφορίες καθώς και αντίγραφο των δεδομένων που υφίστανται επεξεργασία, εφόσον δεν παραβιάζονται δικαιώματα τρίτων (Άρθρο 15).

- Το Δικαίωμα Διόρθωσης, επιτρέπει στο υποκείμενο των δεδομένων να ζητήσει τη διόρθωση ανακριβών δεδομένων ή/και τη συμπλήρωση αυτών, εάν είναι ελλιπή (Άρθρο 16).

- Το Δικαίωμα Διαγραφής, το οποίο επιτρέπει στο υποκείμενο των δεδομένων να ζητήσει τη διαγραφή όλων των προσωπικών δεδομένων που το αφορούν. Το συγκεκριμένο δικαίωμα ισχύει με περιορισμούς και προϋποθέσεις και δεν είναι κάτι απόλυτο (Άρθρο 17).

- Το Δικαίωμα Φορητότητας των δεδομένων, το οποίο επιτρέπει στο υποκείμενο των δεδομένων να ζητήσει ένα πλήρες αντίγραφο των προσωπικών δεδομένων που έχει παράσχει, από έναν υπεύθυνο επεξεργασίας. Σκοπός αυτού, είναι η διευκόλυνση του υποκειμένου σε ενέργειες όπως διακίνηση, μεταφορά, αντιγραφή των δεδομένων που το αφορούν και γενικώς επαναχρησιμοποίηση των δεδομένων του σε άλλους οργανισμούς και φορείς με την προϋπόθεση πως τα δεδομένα θα είναι σε δομημένη, κοινώς χρησιμοποιούμενη, και μηχανικά αναγνώσιμη μορφή (Άρθρο 20).

- Το Δικαίωμα Περιορισμού της Επεξεργασίας (Άρθρο 18) και το Δικαίωμα Εναντίωσης στην Επεξεργασία για σκοπούς εμπορικής προώθησης ή για επεξεργασία που δεν είναι αναγκαία για την παρεχόμενη υπηρεσία (Άρθρο 21).

Είναι σημαντικό να σημειωθεί, ότι ο ίδιος ο Κανονισμός δεν ορίζει συγκεκριμένο τρόπο εφαρμογής των άρθρων του. Η Ομάδα Εργασίας του Άρθρου 29 [4] είχε εκδώσει κατευθυντήριες γραμμές για την ερμηνεία και προσαρμογή ορισμένων πτυχών του ΓΚΠΔ, ωστόσο, οι κατευθυντήριες αυτές δεν καλύπτουν το σύνολο του κανονιστικού πλαισίου. Έκτοτε, η Ομάδα αυτή έχει αντικατασταθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB), το οποίο έχει υιοθετήσει όλες τις προγενέστερες κατευθυντήριες γραμμές που σχετίζονται με τον ΓΚΠΔ [2].

2.3. Δικαίωμα Πρόσβασης

Το δικαίωμα πρόσβασης στα προσωπικά δεδομένα, αποτελεί ένα από τα δικαιώματα των υποκειμένων των δεδομένων που προβλέπει το Κεφάλαιο ΙΙΙ του ΓΚΠΔ - κάποια από αυτά αναφέρθηκαν επιγραμματικά παραπάνω. Η νομική βάση του δικαιώματος πρόσβασης, προκύπτει τόσο από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης όσο και από το Άρθρο 15 του ΓΚΠΔ. Αποτελεί έναν από τους θεμελιώδεις μηχανισμούς διαφάνειας

και λογοδοσίας στον ΓΚΠΔ, καθώς επιτρέπει στα φυσικά πρόσωπα να γνωρίζουν αν και πώς επεξεργάζονται τα προσωπικά τους δεδομένα, καθώς και να λαμβάνουν αντίγραφο αυτών [1].

Η άσκηση του δικαιώματος αυτού, εντάσσεται όχι μόνο στο πλαίσιο της εφαρμογής του δικαίου προστασίας δεδομένων, αλλά και στον ευρύτερο σκοπό του Κανονισμού – όπως διατυπώνεται στο Άρθρο 1(2) του ΓΚΠΔ "την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, με έμφαση την ιδιωτικότητα και την προστασία των προσωπικών δεδομένων".

Σύμφωνα με τη νομοθεσία για την προστασία δεδομένων [5], το δικαίωμα της πρόσβασης πρέπει να είναι διακριτό από άλλα παρόμοια δικαιώματα τα οποία έχουν διαφορετικούς προσανατολισμούς, για παράδειγμα το δικαίωμα της πρόσβασης σε δημόσια έγγραφα, του οποίου στόχος είναι η εξασφάλιση διαφάνειας κατά τη λήψη αποφάσεων των δημόσιων αρχών αλλά και της εύρυθμης διοικητικής πρακτικής [1].

2.3.α. Στόχοι του Δικαιώματος Πρόσβασης

Στόχος του δικαιώματος πρόσβασης είναι τα άτομα να έχουν επίγνωση της επεξεργασίας των προσωπικών τους δεδομένων και παράλληλα να έχουν τη δυνατότητα να επαληθεύσουν τη νομιμότητα της επεξεργασίας αυτής αλλά και την ορθότητα των επεξεργασμένων δεδομένων. Αυτό μπορεί να επιτευχθεί όταν παρέχονται στα υποκείμενα των δεδομένων πληροφορίες οι οποίες είναι επαρκείς, σαφείς και εύκολα προσβάσιμες. Επιπλέον, κατ' αυτόν τον τρόπο τα άτομα μπορούν ευκολότερα να ασκήσουν και άλλα δικαιώματα όπως το δικαίωμα της διαγραφής, της διόρθωσης κ.α..

Αναλυτικότερα, το EDPB στο Guidelines 01/2022 παραθέτει πως βάσει του ΓΚΠΔ, οι κύριες συνιστώσες του δικαιώματος της πρόσβασης είναι τρείς. Αρχικά, γνωστοποίηση σχετικά με το εάν τα προσωπικά δεδομένα του υποκειμένου υπόκεινται σε επεξεργασία ή όχι. Έπειτα, πρόσβαση στα επεξεργασμένα αυτά δεδομένα και τέλος, ενημέρωση και περεταίρω πληροφορίες για την ίδια την επεξεργασία. Πληροφορίες όπως ο σκοπός και η διάρκεια που γίνεται η επεξεργασία, ποια δεδομένα χρησιμοποιούνται και ποιοι είναι οι αποδέκτες αυτών, τι δικαιώματα έχουν τα υποκείμενα πάνω σε αυτά, καθώς επίσης και ποιες είναι οι ανάλογες δικλίδες ασφαλείας όταν τα δεδομένα αυτά διαβιβάζονται σε τρίτες χώρες. Επίσης, το υποκείμενο των δεδομένων, έχει τη δυνατότητα να ζητήσει αντίγραφο των επεξεργασμένων

προσωπικών του δεδομένων, χωρίς αυτό να πρόκειται για πρόσθετο δικαίωμα καθώς η δυνατότητα αυτή εμπεριέχεται στους τρόπους παροχής πρόσβασης στα δεδομένα [1].

Με βάση τα παραπάνω, το δικαίωμα της πρόσβασης μπορεί να ερμηνευθεί τόσο ως το δικαίωμα των υποκειμένων των δεδομένων να έχουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που διαχειρίζονται οι υπεύθυνοι επεξεργασίας και οι εκτελούντες της επεξεργασίας [2] αλλά και ως η δυνατότητα πρόσβασης και επαλήθευσης των δεδομένων αυτών [1].

Επίσης, το υποκείμενο των δεδομένων δεν οφείλει να αιτιολογήσει το αίτημά του και δεν είναι αρμοδιότητα του υπευθύνου επεξεργασίας να αναλύσει το κατά πόσον η απάντηση που θα παρέχει στο αίτημα πρόσβασης θα βοηθήσει όντως το άτομο να ελέγξει τη νομιμότητα και ό,τι άλλο έχει προαναφερθεί. Επιπλέον, ο υπεύθυνος της επεξεργασίας είναι αρμόδιος στο να εξετάσει το αίτημα, για το εάν αυτό εμπίπτει στα πλαίσια του δικαιώματος της πρόσβασης και δεν υποβάλλεται βάσει άλλων κανόνων, εκτός των κανόνων προστασίας δεδομένων [1].

2.3.β. Ανάλυση της Δομής του Δικαιώματος Πρόσβασης

Όπως αναφέρθηκε παραπάνω, το EDPB διαχώρισε το δικαίωμα πρόσβασης σε τρεις επιμέρους συνιστώσες. Κάθε μία από αυτές εξετάστηκε αναλυτικά, με στόχο την αποσαφήνιση όλων των πτυχών του άρθρου και τη διασφάλιση της πλήρους κατανόησης και κάλυψής του. Η προσέγγιση αυτή συμβάλλει στην καλύτερη κατανόηση της πολυπλοκότητας του Άρθρου 15, τόσο από την πλευρά του υποκειμένου των δεδομένων όσο και από τους υπεύθυνους επεξεργασίας. Παράλληλα, παρέχει καθοδήγηση στους τελευταίους σχετικά με το τι ακριβώς πρέπει να παρέχουν στο υποκείμενο, πώς να διαχειρίζονται κάθε αίτημα πρόσβασης, καθώς και ποιοι περιορισμοί ισχύουν.

Το Άρθρο 15 λοιπόν, μπορεί να διαχωρίστηκε σε: Άρθ. 15(1), Άρθ. 15(2) όπου μαζί αυτά τα δυο ορίζουν το περιεχόμενο του δικαιώματος πρόσβασης, Άρθ. 15(3) το οποίο αφορά τις λεπτομέρειες πρόσβασης και τέλος Άρθ. 15(4) όπου εστιάζει στα δικαιώματα και τις ελευθερίες των άλλων, στο πλαίσιο της πρόσβασης.

Πιο συγκεκριμένα, το Άρθ. 15(1) και (2) περιλαμβάνει τη γνωστοποίηση για το εάν τα δεδομένα του αιτούμενου ατόμου υπόκεινται σε επεξεργασία, πρόσβαση σε αυτά εφόσον όντως επεξεργάζονται και τέλος πληροφορίες σχετικά με την επεξεργασία. Οι πληροφορίες μπορεί να περιλαμβάνουν: τον/τους σκοπό/σκοπούς της επεξεργασίας, τους παραλήπτες των

επεξεργασμένων δεδομένων, την προβλεπόμενη διάρκεια της επεξεργασίας, τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα, την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων / κατάρτισης προφίλ, πιθανές πληροφορίες για δεδομένα που δεν έχουν συλλεχθεί από το ίδιο το υποκείμενο των δεδομένων, το δικαίωμα υποβολής καταγγελίας στις αρμόδιες εποπτικές αρχές και την ύπαρξη των δικαιωμάτων διόρθωσης, διαγραφής, εναντίωσης και περιορισμού της επεξεργασίας. Για τις περιπτώσεις όπου ο υπεύθυνος επεξεργασίας δεν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που αφορούν το αιτούμενο άτομο, οι μόνες πληροφορίες που οφείλει να παρέχει είναι απλώς η γνωστοποίηση ότι δεν υφίσταται επεξεργασία των δεδομένων του.

Το Άρθρο 15(3) επικεντρώνεται στην υποχρέωση του υπευθύνου επεξεργασίας να παρέχει στο υποκείμενο των δεδομένων αντίγραφο των προσωπικών του δεδομένων που υφίστανται επεξεργασία. Η υποχρέωση αυτή, δεν συνιστά αυτοτελές δικαίωμα, αλλά αποτελεί μέσο άσκησης του δικαιώματος πρόσβασης, όπως αυτό ορίζεται στο Άρθρο 15(1). Διευκρινίζεται ότι η πρόσβαση στα δεδομένα συνεπάγεται πλήρη ενημέρωση επί αυτών και όχι απλώς μία σύνοψη ή γενική περιγραφή. Η παροχή αντιγράφου είναι απαραίτητη για την εκπλήρωση των σκοπών του δικαιώματος πρόσβασης, όπως η ενημέρωση του υποκειμένου και η δυνατότητα να ελέγξει αν η επεξεργασία των προσωπικών του δεδομένων είναι νόμιμη. Προφανώς, για να επιτευχθούν αυτοί οι σκοποί, το ΥΔ χρειάζεται χρόνο για να μελετήσει τις πληροφορίες που θα του παρέχει ο διαχειριστής και δεν θα ήταν αρκετό να είχε πρόσβαση σε αυτές μόνο προσωρινά. Αυτός είναι και ο λόγος που η αποστολή αντιγράφου των δεδομένων θεωρείται αναγκαία.

Ο υπεύθυνος επεξεργασίας οφείλει να παρέχει δωρεάν το αρχικό αντίγραφο των δεδομένων προσωπικού χαρακτήρα που σχετίζεται της επεξεργασίας. Όταν όμως το ΥΔ κάνει εκ νέου αίτηση για αντίγραφο τίθενται κάποια ερωτήματα όπως το εάν αυτό θα πρέπει να θεωρηθεί ως νέο αίτημα ή εάν θέλει επιπλέον αντίγραφο. Ο διαχωρισμός αυτών, κρίνεται από το αν το αίτημα αφορά το ίδιο σύνολο δεδομένων, όπου εκεί θεωρείται ως επιπλέον αντίγραφο, παρόλα αυτά εάν: θέλει απλώς επιπλέον πληροφορίες / σχετίζεται με διαφορετικό εύρος δεδομένων απ' ότι το αρχικό αίτημα / η απάντηση που έλαβε στο αρχικό αίτημά του ήταν ελλιπής, τότε θεωρείται ως ένα νέο αίτημα.

Για κάθε πρόσθετο αντίγραφο που ζητείται, ο υπεύθυνος επεξεργασίας έχει το δικαίωμα να ζητήσει ένα εύλογο αντίτιμο, το οποίο προκύπτει από τα ανάλογα διοικητικά έξοδα. Σε αυτές τις περιπτώσεις θα πρέπει αφού καθοριστεί το ποσό αυτό να ενημερώσει το ΥΔ για τους λόγους

που κατέληξε σε αυτή την πράξη και με τη σειρά του το ΥΔ να αποφασίσει εάν θα συνεχίσει στην ολοκλήρωση του αιτήματος. ια τα αιτήματα που χαρακτηρίζονται ως νέα, το δικαίωμα λήψης δωρεάν αντιγράφου ισχύει κανονικά, όπως προβλέπεται ρητά από τον Κανονισμό.

Επιπλέον, όταν το υποκείμενο των δεδομένων υποβάλλει αίτημα πρόσβασης μέσω ηλεκτρονικών μέσων, ο υπεύθυνος επεξεργασίας υποχρεούται να παρέχει όλες τις πληροφορίες που προβλέπονται στο Άρθρο 15(1) και (2) σε ευρέως χρησιμοποιούμενη ηλεκτρονική μορφή, εκτός εάν το υποκείμενο ζητήσει διαφορετικό τρόπο παροχής αυτών. Προφανώς για να σταλούν προσωπικές πληροφορίες δεδομένων, θα πρέπει να εξασφαλιστούν τα κατάλληλα μέτρα ασφάλειας.

Τέλος, το Άρθ.15(4), περιορίζει το δικαίωμα λήψης αντιγράφου δεδομένων προσωπικού χαρακτήρα όταν αυτό μπορεί να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες άλλων (π.χ. ιδιωτική ζωή, εμπορικά μυστικά, πνευματική ιδιοκτησία). Κάτι το οποίο αφορά μόνο το δικαίωμα λήψης αντιγράφου και όχι το γενικότερο δικαίωμα της πρόσβασης που αναλύεται από το Αρθ.15(1). Ο περιορισμός αυτός, δεν ισοδυναμεί με την πλήρη άρνηση της πρόσβασης, καθώς ο διαχειριστής θα πρέπει αρχικά να προβεί σε αναδιατύπωση ή ανωνυμοποίηση των δεδομένων τρίτων. Ωστόσο, εάν ούτε έτσι επιλυθεί η πιθανότητα να γνωστοποιηθούν πληροφορίες τρίτων, ο διαχειριστής μπορεί να προβεί στην πλήρη άρνηση πρόσβασης, εάν είναι αδύνατο να βρεθεί λύση συμβιβασμού. Στις περιπτώσεις αυτές, θα πρέπει το ΥΔ να ενημερωθεί για την απόφαση της άρνησης ολοκλήρωσης του αιτήματος, και να λάβει μια εξήγηση για τους λόγους που ο διαχειριστής κατέληξε στην απόφαση αυτή.

Σημαντικό είναι επίσης, το τι θεωρείται ως πληροφορία που μπορεί να παραβιάσει τα δικαιώματα και τις ελευθερίες των άλλων. Για παράδειγμα, τα οικονομικά συμφέροντα μιας εταιρίας, δεν ανήκουν σε αυτή την κατηγορία και σίγουρα δεν θα πρέπει να είναι παράγοντας άρνησης ολοκλήρωσης του αιτήματος.

ΚΕΦΑΛΑΙΟ 3 Σχεδιασμός

3.1. Περιπτώσεις Χρήσης

Για το σύστημα, προηγήθηκε μια εκτενής μελέτη των Περιπτώσεων Χρήσης (Use Cases), με όσο το δυνατόν καλύτερη σαφήνεια για το πως αλληλεπιδρούν με το σύστημα οι βασικοί ρόλοι αυτού.

3.1.α. Σκοπός και Βασικοί Ρόλοι

Οι περιπτώσεις χρήσης, απεικονίζουν τις ενέργειες που μπορεί να εκτελέσει ο κάθε εξωτερικός παράγοντας του συστήματος και τις ανάλογες αποκρίσεις του συστήματος. Εξωτερικός παράγοντας ή αλλιώς Βασικός Ρόλος (actor) του συστήματος θεωρείται όποιος αλληλεπιδράει με το σύστημα – στην προκειμένη έχουμε δυο βασικούς ρόλους του συστήματος, το υποκείμενο των δεδομένων (Data Subject) και τον υπεύθυνο της επεξεργασίας (Controller).

3.1.β. Επεξήγηση των Περιπτώσεων Χρήσης

Οι Περιπτώσεις Χρήσης του συστήματος παρουσιάζονται σχηματικά στην Εικόνα 1. Ακολουθεί μια σύντομη περιγραφή για τις κυριότερες από αυτές.

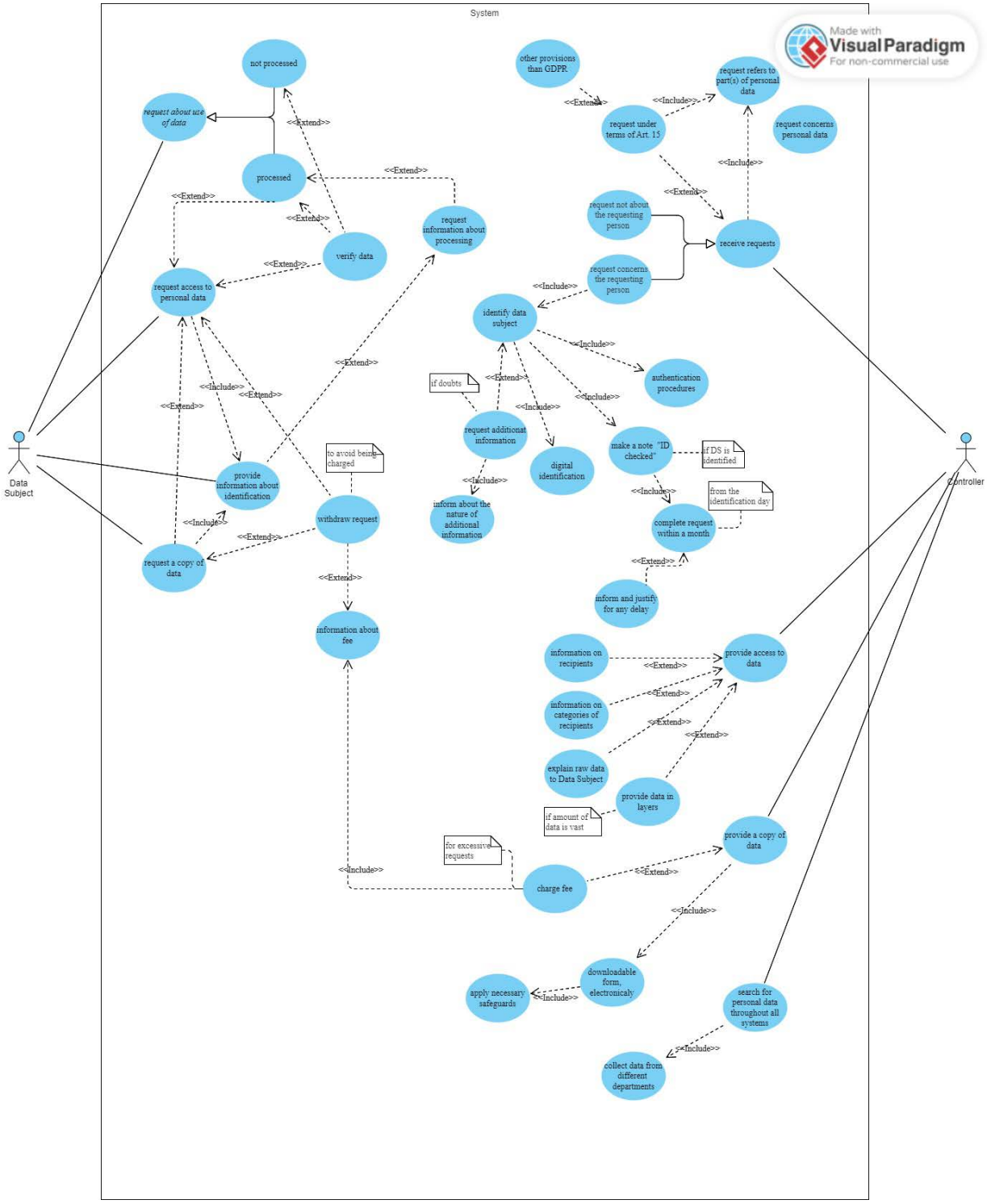
Από την πλευρά του υποκειμένου των δεδομένων – ΥΔ (Data Subject – DS) έχουμε:

- **Αίτημα ενημέρωσης χρήσης δεδομένων** (Request about use of data): Το ΥΔ υποβάλλει αίτημα για να ενημερωθεί σχετικά με το πώς και γιατί χρησιμοποιούνται τα προσωπικά του δεδομένα.
- **Αίτημα πρόσβασης σε προσωπικά δεδομένα** (Request access to personal data): Το ΥΔ αιτείται πρόσβαση στα προσωπικά δεδομένα του.
- **Αίτημα για αντίγραφο δεδομένων** (Request a copy of data): Το ΥΔ αιτείται αντίγραφο των προσωπικών του δεδομένων σε αναγνώσιμη μορφή.

- **Παροχή πληροφοριών ταυτοποίησης** (Provide information about identification): το ΥΔ υποβάλλει στοιχεία που επιβεβαιώνουν την ταυτότητά του, ώστε να μπορέσει να υποβάλλει αιτήσεις.
- **Αίτημα ενημέρωσης για την επεξεργασία** (Request information about processing): το ΥΔ ζητά λεπτομέρειες για την επεξεργασία που υπόκεινται τα δεδομένα του.
- **Επαλήθευση δεδομένων** (Verify data): δυνατότητα να επαληθεύσει τα δεδομένα που υπάρχουν στην απάντηση του αιτήματος πρόσβασης.
- **Ακύρωση/Ανάκληση αιτήματος** (Withdraw request): το ΥΔ μπορεί να ακυρώσει ή να ανακαλέσει ένα αίτημα που έχει υποβάλει.

Ενώ από την πλευρά του υπεύθυνου επεξεργασίας – ΥΕ έχουμε:

- **Λήψη αιτημάτων πρόσβασης** (Receive Requests): ο ΥΕ λαμβάνει τα αιτήματα που υποβάλλονται από τα ΥΔ.
- **Παροχή πρόσβασης στα δεδομένα** (Provide access to data): αφού επαληθεύσει την ταυτότητα του ΥΔ, παρέχει τη δυνατότητα προβολής των δεδομένων που το αφορούν.
- **Παροχή αντίγραφου δεδομένων** (Provide a copy of data): ο ΥΕ διανέμει αντίγραφα των προσωπικών δεδομένων σε μορφή που είναι ευανάγνωστη και κατανοητή από το ΥΔ.
- **Αναζήτηση δεδομένων προσωπικού χαρακτήρα σε όλα τα συστήματα** (Search for personal data throughout all systems): ο ΥΕ διεξάγει αναζήτηση σε όλα τα συστήματα και τις ΒΔ για την εύρεση όλων των προσωπικών δεδομένων του αιτούμενου ατόμου.
- **Ταυτοποίηση υποκειμένου των δεδομένων** (Identify data subject): ο ΥΕ επαληθεύει την ταυτότητα του αιτούμενου ατόμου, διασφαλίζοντας την εγκυρότητα πρόσβασης.
- **Ολοκλήρωση του αιτήματος εντός μηνός** (Complete request within a month): διασφαλίζει την ολοκλήρωση των αιτημάτων εντός της προθεσμίας ενός μήνα, όπως ορίζεται από τον ΓΚΠΔ.



Εικόνα 1: Use Cases

3.2. Απαιτήσεις

Σε αυτή την Ενότητα παρουσιάζονται οι απαιτήσεις λογισμικού οι οποίες απορρέουν από όσα έχουν αναφερθεί έως τώρα. Οι απαιτήσεις θα αναλυθούν ξεχωριστά ως προς τους δυο

βασικούς τύπους χρηστών – υποκείμενο των δεδομένων και διαχειριστής – καθένας εκ των οποίων έχει διαφορετικές ανάγκες και δυνατότητες αλληλεπίδρασης με το σύστημα.

3.2.α. Απαιτήσεις Υποκειμένων των Δεδομένων

Ας ξεκινήσουμε με τις απαιτήσεις από την πλευρά του υποκειμένου των δεδομένων. Αρχικά, θα πρέπει να μπορεί, με εύκολο και απλό τρόπο, να υποβάλει αίτηση για: πρόσβαση στα προσωπικά του δεδομένα, απόκτηση αντιγράφου των προσωπικών του δεδομένων και πληροφορίες για την χρήση τους. Σχετικά με το τελευταίο, η απάντηση που πρέπει να λάβει αφορά το εάν τα δεδομένα του υπόκεινται σε επεξεργασία ή όχι. Στην πρώτη περίπτωση, να μπορεί να ζητήσει επιπλέον πληροφορίες για τη διαδικασία της επεξεργασίας καθώς και τη χρήση τους. Για όλες τις περιπτώσεις αιτήσεων, αφού λάβει την απάντηση από τον διαχειριστή, το άτομο πρέπει να έχει τη δυνατότητα να επιβεβαιώσει τα δεδομένα αυτά ως προς την εγκυρότητά τους.

Για την υποβολή των αιτήσεων, είναι προφανές πως το άτομο οφείλει να έχει γνωστοποιήσει πληροφορίες ταυτοποίησης στον διαχειριστή. Βέβαια, υπάρχουν περιπτώσεις που οι πληροφορίες αυτές μπορεί να μην επαρκούν και να ζητηθούν, έπειτα από την υποβολή κάποιας αίτησης, επιπρόσθετες πληροφορίες. Σε αυτή την περίπτωση, εάν το άτομο θέλει να συνεχίσει με το αίτημά του, οφείλει να διαβιβάσει τις πληροφορίες αυτές στον διαχειριστή εάν και εφόσον ο τελευταίος, από την πλευρά του, έχει επεξηγήσει το/τους λόγο/λόγους που τις ζητάει. Σε κάθε άλλη περίπτωση, το άτομο μπορεί να αρνηθεί τη γνωστοποίηση των επιπλέον πληροφοριών.

3.2.β. Απαιτήσεις Διαχειριστή

Ολοκληρώνοντας με τις απαιτήσεις από την πλευρά του υποκειμένου των δεδομένων, μπορούμε να περάσουμε στις απαιτήσεις που αφορούν τον διαχειριστή. Πρώτα απ’ όλα θα πρέπει να λαμβάνει όλα τα αιτήματα των υποκειμένων των δεδομένων και έπειτα να πραγματοποιεί ανάλυση του εκάστοτε αιτήματος. Από την ανάλυση αυτή, πρέπει να μπορεί να αναγνωρίζει εάν αρχικά το αίτημα είναι σχετικό με το Άρθρο 15 του ΓΚΠΔ, έπειτα για το εάν απαιτούνται άλλες διατάξεις και τέλος εάν αφορά τα προσωπικά δεδομένα του ίδιου του

αιτούμενου ατόμου καθώς επίσης να διακρίνει αν αυτό αναφέρεται στο σύνολο ή σε επιμέρους τμήματά τους. Στις περιπτώσεις που το αίτημα αφορά όντως το αιτούμενο άτομο, ξεκινάει η διαδικασία της ταυτοποίησης.

Προκειμένου να ολοκληρωθεί αυτή η διαδικασία, ο διαχειριστής οφείλει να εφαρμόσει κατάλληλες διαδικασίες αυθεντικοποίησης και ψηφιακής ταυτοποίησης. Επιπλέον, στις περιπτώσεις που το αιτούμενο άτομο δεν μπορεί να ταυτοποιηθεί με τις όσες πληροφορίες έχει ως τότε γνωστοποιήσει στον διαχειριστή, θα πρέπει να ζητηθούν επιπλέον πληροφορίες οι οποίες όμως θα φέρουν κατάλληλη αιτιολόγηση ως προς τον λόγο που ζητούνται και που θα εξυπηρετήσουν. Τέλος, καλή πρακτική στο τέλος αυτού του σταδίου, θα ήταν να γίνεται μια σημείωση για το άτομο αυτό πως έχει επιτυχώς επαληθευτεί, ώστε μελλοντικά σε κάποια άλλη αίτηση να μην χρειάζεται επανάληψη της όλης διαδικασίας.

Στη συνέχεια, πρέπει να ορίζεται η ημερομηνία από την οποία ξεκινάει το διάστημα του ενός μήνα που οφείλει ο διαχειριστής να τηρήσει και να έχει έτοιμη την απάντηση στο εκάστοτε αίτημα. Παρ' όλα αυτά, εάν ο διαχειριστής κρίνει πως το διάστημα αυτό δεν επαρκεί για να προετοιμάσει την απάντηση του αιτήματος, πρέπει να ενημερώσει το αιτούμενο άτομο, όσο πιο άμεσα γίνεται, ότι θα υπάρξει μια επιμήκυνση του χρόνου απόκρισης, και να ανανεώσει την καταλυτική ημερομηνία απάντησης, την οποία θα πρέπει αυστηρώς να τηρήσει.

Έπειτα, ο διαχειριστής πρέπει να ανταποκριθεί κατάλληλα, ανάλογα με το είδος του αιτήματος. Για παράδειγμα, στην περίπτωση που το αίτημα είναι αντίγραφο των δεδομένων, θα πρέπει αρχικά για την αποστολή των δεδομένων αυτών, να εφαρμοστούν κατάλληλοι μηχανισμοί ασφάλειας και επίσης τα δεδομένα αυτά να είναι σε μορφή διαθέσιμη τόσο προς λήψη όσο και προς ανάγνωση από το αιτούμενο άτομο. Επίσης, ο διαχειριστής οφείλει να εξηγήσει ή/και να προσαρμόσει κάποιες φορές τα δεδομένα που θα αποστείλει εάν κρίνεται πως αυτά είναι σε δυσνόητη προς το άτομο μορφή. Συμπληρωματικά με αυτό και σε πιο σπάνιες περιπτώσεις, όπου ο όγκος των δεδομένων είναι τεράστιος, θα πρέπει με κάποιον μηχανισμό, η πληροφορία των δεδομένων να παρέχεται σε επίπεδα (layers) ώστε να μπορεί το άτομο να περιηγείται και να μην χάσει σημαντικές πληροφορίες.

Τέλος, θα πρέπει να υπάρχει μια αναλυτική αναφορά, στην οποία θα καταγράφονται οι αιτήσεις που έχει πραγματοποιήσει το κάθε υποκείμενο καθώς και το πότε έχει γίνει κάθε αίτηση. Η αναφορά αυτή κρίνεται σημαντική, καθώς με αυτό τον τρόπο ο διαχειριστής θα μπορεί να γνωρίζει τι διάστημα έχει μεσολαβήσει από προηγούμενα αιτήματα ώστε να αποφεύγονται αλόγιστα αιτήματα σε μικρά χρονικά διαστήματα και χωρίς σημαντικό σκοπό.

Μάλιστα, σε περιπτώσεις που κριθεί περιττό κάποιο αίτημα ή δεν έχει περάσει ένα διάστημα μεγαλύτερο του ενός μήνα, ο διαχειριστής μπορεί να κοστολογήσει την ανταπόκρισή του. Η απόφαση αυτή θα πρέπει να αποσταλεί στο άτομο, ειδοποιώντας το για τους λόγους κοστολόγησης και το αντίτιμο που θα χρειαστεί να καταβάλει εάν θέλει ακόμα και έτσι να συνεχίσει στην ολοκλήρωση του αιτήματός του. Η αρνητική απάντηση για την κατάθεση αντίτιμου από το άτομο τερματίζει τη διαδικασία ολοκλήρωσης του αιτήματος, απαλλάσσοντας το άτομο από την όποια χρέωση και τον διαχειριστή από την όποια περεταίρω υποχρέωση.

3.2.γ. Διαμόρφωση Απαιτήσεων

Αφού λοιπόν αναλύθηκαν με σαφήνεια οι απαιτήσεις και από τις δυο πλευρές, σε αυτή την υποενότητα παρουσιάζονται με τρόπο συνεκτικό και προς απευθείας χρήση τους:

Υποκείμενο των δεδομένων:

- Να μπορεί με εύκολο τρόπο να υποβάλει αίτηση για:
    - πρόσβαση στα προσωπικά του δεδομένα,
    - απόκτηση αντιγράφου των προσωπικών του δεδομένων,
    - πληροφορίες για τη χρήση των δεδομένων του.
- Εάν τα δεδομένα του υπόκεινται σε επεξεργασία, να μπορεί να ζητήσει επιπλέον πληροφορίες για την διαδικασία της επεξεργασίας – το τι επεξεργασία υπόκεινται.
- Σε όλες τις περιπτώσεις αίτησής του, μετά την απάντηση από τον διαχειριστή, το άτομο θα έχει τη δυνατότητα να επιβεβαιώσει τα δεδομένα αυτά ως προς την εγκυρότητά τους.
- Οφείλει να παρέχει πληροφορίες ταυτοποίησης στον διαχειριστή.
- Εάν ο διαχειριστής ζητήσει επιπλέον πληροφορίες ταυτοποίησής, αιτιολογώντας το/τους λόγο/λόγους που ζητάει τις παραπάνω αυτές πληροφορίες, θα πρέπει να τις παρέχει εάν θέλει να συνεχίσει με το αίτημά του.

Υπεύθυνος Επεξεργασίας:

- Λαμβάνει όλα τα αιτήματα των υποκειμένων των δεδομένων.
- Πραγματοποιεί ανάλυση του εκάστοτε αιτήματος που λαμβάνει.

- Από την ανάλυση να μπορεί να εξάγει πληροφορίες για:
    - το εάν το αίτημα είναι σχετικό με το Άρθρο 15 του ΓΚΠΔ,
    - εάν απαιτούνται άλλες διατάξεις πέραν αυτού,
    - να διακρίνει εάν το αίτημα αναφέρεται σε μέρη/μέρος των προσωπικών δεδομένων του αιτούμενου ατόμου και
    - το εάν το αίτημα αφορά τα δεδομένα του ίδιου του ατόμου ή όχι.
- Εάν το αίτημα αφορά το ίδιο το αιτούμενο άτομο, ξεκινάει τη διαδικασία της ταυτοποίησης.
- Όταν το αίτημα δεν αφορά το αιτούμενο άτομο, πρέπει να ενημερώνει κατάλληλα το άτομο για το εάν η διαδικασία μπορεί να συνεχιστεί ή όχι.
- Χρήση κατάλληλων διαδικασιών αυθεντικοποίησης και ψηφιακής ταυτοποίησης ώστε να πραγματοποιεί την ταυτοποίηση ατόμων.
- Εάν οι διαθέσιμες πληροφορίες που παρέχει το άτομο δεν επαρκούν για το παραπάνω, πρέπει να ζητούνται παραπάνω πληροφορίες ώστε να ολοκληρωθεί η ταυτοποίηση.
- Η αίτηση για παραπάνω πληροφορίες πρέπει να συμπεριλαμβάνει και την κατάλληλη αιτιολόγηση ως προς τον λόγο που ζητούνται.
- Η επιτυχής ταυτοποίηση θα πρέπει να ακολουθείται από μια σημείωση ότι το άτομο επαληθεύτηκε, ώστε να αποφεύγεται μελλοντικά η ίδια διαδικασία.
- Μόλις ολοκληρωθούν τα παραπάνω, ο διαχειριστής ορίζει ημερομηνία έναρξης του διαστήματος επεξεργασίας του αιτήματος.
- Οφείλει να ολοκληρώσει το αίτημα σε διάστημα ενός μήνα.
- Εάν κριθεί πως το διάστημα αυτό δεν επαρκεί, πρέπει να ενημερωθεί το υποκείμενο των δεδομένων, όσο πιο άμεσα γίνεται, ότι θα υπάρξει μια επιμήκυνση του χρόνου απόκρισης και να ανανεωθεί η καταλυτική ημερομηνία ολοκλήρωσης του αιτήματος.
- Σε περιπτώσεις που τα δεδομένα είναι σε μορφή που δεν θα καταλάβει το άτομο, οφείλει να τα εξηγήσει ή/και να τα προσαρμόσει ώστε να είναι πλήρως κατανοητό το περιεχόμενό τους.
- Σε περιπτώσεις που ο όγκος των δεδομένων είναι ιδιαίτερα μεγάλος, θα πρέπει να προβλέπεται ένας κατάλληλος μηχανισμός παρουσίασης, ο οποίος να οργανώνει τις

πληροφορίες σε επίπεδα (layers), προκειμένου το υποκείμενο των δεδομένων να μπορεί να περιηγηθεί αποτελεσματικά σε αυτές, χωρίς να χάνεται το νόημα μέσα στην υπερβολική πληροφορία.

- Όταν η αίτηση του αιτούμενου ατόμου είναι αντίγραφο των δεδομένων του, πρέπει να εφαρμόσει κατάλληλους μηχανισμούς ασφάλειας για την αποστολή τους.
- Θα πρέπει τα δεδομένα αυτά να είναι σε μορφή διαθέσιμη τόσο προς λήψη όσο και προς ανάγνωση.
- Θα υπάρχει ένα αρχείο στο οποίο θα καταγράφονται οι αιτήσεις που έχει πραγματοποιήσει κάθε άτομο και το διάστημα που έχει περάσει από το κάθε αίτημα.
- Με τη βοήθεια του παραπάνω, στις περιπτώσεις που κάποιο άτομο έχει ζητήσει αλόγιστες φορές – χωρίς σημαντικό σκοπό, σε μικρό χρονικό διάστημα – πληροφορίες για τα δεδομένα του, θα έχει την επιλογή να κοστολογήσει την απάντηση του αιτήματος.
- Για την κοστολόγηση του αιτήματος, πρέπει να στείλει μια ειδοποίηση σχετική με τους λόγους αυτής της πράξης του, καθώς και το αντίτιμο που θα χρειαστεί να καταβάλλει το αιτούμενο άτομο εάν θελήσει να συνεχίσει στην ολοκλήρωση του αιτήματος.
- Η διαδικασία ολοκλήρωσης του αιτήματος ακυρώνεται εάν:
    - το αιτούμενο άτομο αρνηθεί την ολοκλήρωση του αιτήματος ή
    - δεν καταβάλλει το αντίστοιχο ποσό του αντίτιμου.

3.3. Αρχιτεκτονική

Με βάση τα παραπάνω προκύπτει και η αρχιτεκτονική του συστήματος, η οποία απεικονίζεται σχηματικά παρακάτω (

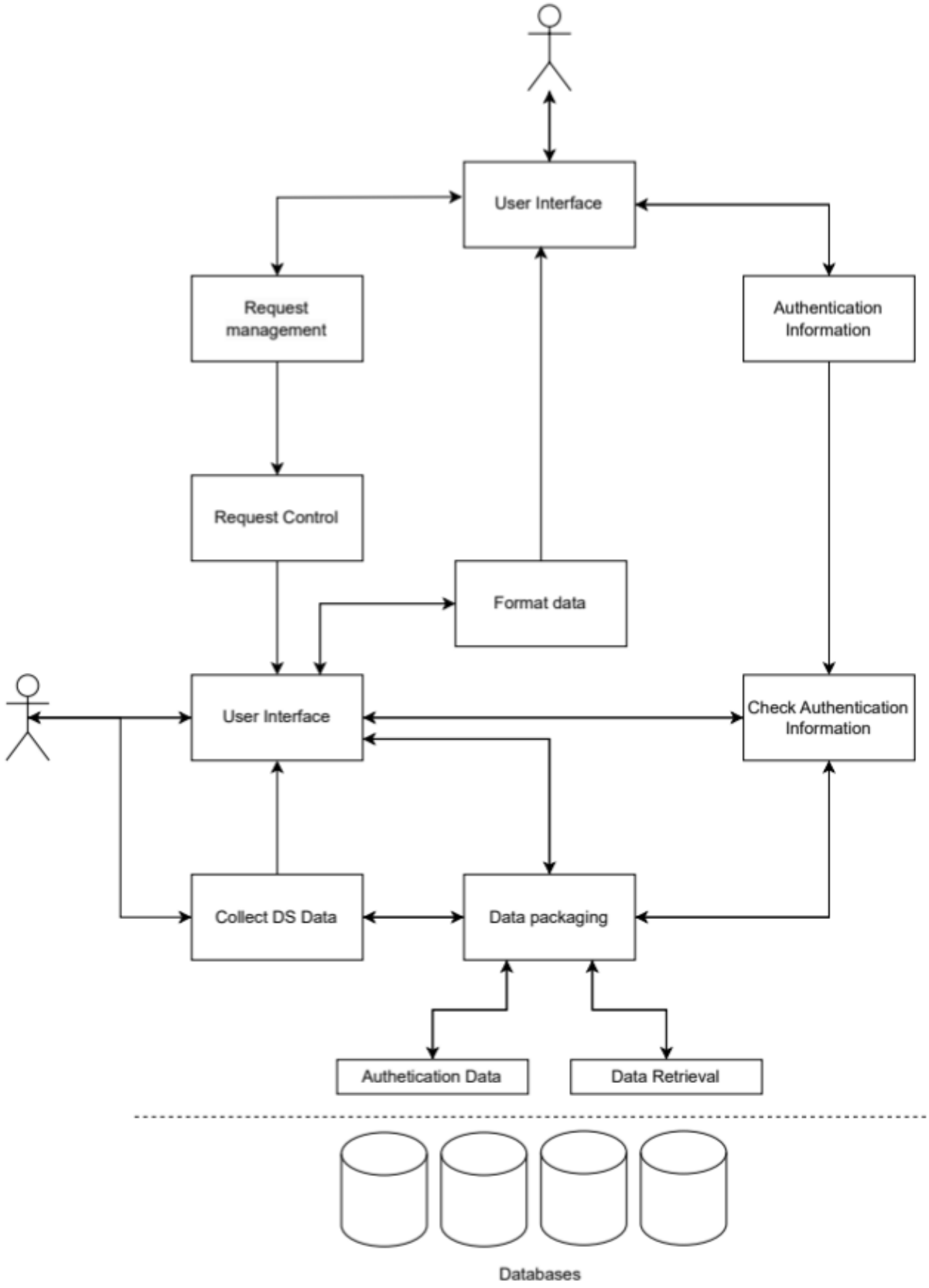
Εικόνα 2). Αρχικά έχουμε τους δυο κύριους ρόλους (actors) του συστήματος: τον χρήστη (υποκείμενο των δεδομένων), που απεικονίζεται πάνω, και τον διαχειριστή του συστήματος (controller), που απεικονίζεται αριστερά. Οι δυο αυτοί ρόλοι, αλληλεπιδρούν με διαφορετικό τρόπο με το σύστημα, ώστε να υλοποιήσουν τις ανάγκες/λειτουργίες τους και αυτό φαίνεται σχηματικά από τις δυο ξεχωριστές διεπαφές (User Interfaces – UI) που υπάρχουν.

Ο χρήστης εισέρχεται στο σύστημα μέσω της διεπαφής, από την οποία μπορεί να εκκινήσει τη διαδικασία για ένα αίτημα πρόσβασης (Request Managment). Στο στάδιο Διαχείρισης Αιτημάτων (Request Managment) ο χρήστης μπορεί να υποβάλει ένα αίτημα πρόσβασης που να αφορά τα δεδομένα του (Request Control) εάν ισχύουν κάποιες προϋποθέσεις, τις οποίες αναλύσαμε σε προηγούμενα κεφάλαια. Τα αιτήματα αυτά διαχειρίζονται από τη διεπαφή του διαχειριστή. Επίσης, η λειτουργία «Πληροφορίες Αυθεντικοποίησης» (Authentication Information), αντιπροσωπεύει τόσο τη δυνατότητα του χρήστη να επαληθεύσει τα δεδομένα του, όσο και τη διαδικασία παροχής δεδομένων αυθεντικοποίησής του προς τον διαχειριστή.

Αφού λοιπόν ο χρήστης εκκινήσει μέσω της διεπαφής του ένα αίτημα πρόσβασης, ο διαχειριστής του συστήματος, μέσω της δικής του διεπαφής με το σύστημα, διαχειρίζεται τα ληφθέντα αιτήματα πρόσβασης του χρήστη, για τα οποία πρέπει να εκτελέσει κάποιες διαδικασίες ώστε να διαμορφώσει την απάντηση αιτήματος κατάλληλα. Αρχικά θα πρέπει να ελέγξει τις πληροφορίες αυθεντικοποίησης του χρήστη (Check Authentication Information), τις οποίες έχει ήδη παράσχει ο χρήστης και οι οποίες με τη βοήθεια του Data Packaging είχαν προωθηθεί καταλλήλως στις συναφείς ΒΔ.

Έπειτα, μπορεί να ξεκινήσει τη διαδικασία συλλογής δεδομένων (Collect DS Data), για την οποία πρέπει να συλλεχθούν/συγκεντρωθούν, από διαφορετικές ΒΔ, ετερογενή δεδομένα. Σχηματικά αυτό απεικονίζεται μέσω της μονάδας που είναι υπεύθυνη για να ανακτά τις απαραίτητες πληροφορίες (Data Packaging), ώστε να τις προωθήσει είτε απευθείας στη διεπαφή του διαχειριστή είτε στην λειτουργική διαδικασία της συλλογής.

Τέλος, το σύνολο των δεδομένων που έχουν συλλεχθεί και αφορούν το αίτημα πρόσβασης, μορφοποιούνται σε συγκεκριμένο πρότυπο (Format data), που θα είναι αναγνώσιμο και κατανοητό από τον χρήστη ώστε να αποσταλούν στη διεπαφή του και να ολοκληρωθεί η διαδικασία του αιτήματος πρόσβασης.



Εικόνα 2: Αρχιτεκτονική

ΚΕΦΑΛΑΙΟ 4 ΥΛΟΠΟΙΗΣΗ ΣΥΣΤΗΜΑΤΟΣ

4.1. Πληροφορίες Υλοποίησης

Ο ΓΚΠΔ όπως αναφέρθηκε, ορίζει το νομικό πλαίσιο για τα δικαιώματα των υποκειμένων, παρόλα αυτά, η πρακτική εφαρμογή του Κανονισμού δεν τηρείται από όλους τους οργανισμούς όπως θα έπρεπε. Συγκεκριμένα, η μη συμμόρφωση με τον Κανονισμό επιφέρει πρόστιμα στους οργανισμούς και μάλιστα, κατά το πρώτο έτος εφαρμογής του, το Άρθρο 15 ήταν ένα από τα άρθρα που μέτρησε τις περισσότερες παραβάσεις με εξαιρετικά υψηλά πρόστιμα.

Το να υπάρξει ένα σύστημα το οποίο θα μπορούσε να αυτοματοποιήσει τη διαχείριση δικαιωμάτων των υποκειμένων θα ήταν μια καλή λύση που θα ωφελούσε τόσο τους οργανισμούς όσο και κάθε υποκείμενο των δεδομένων. Στο κεφάλαιο αυτό, περιλαμβάνονται οι απαραίτητες πληροφορίες για το προτεινόμενο σύστημα που έγινε σε αυτό το πλαίσιο. Για την υλοποίησή χρησιμοποιήθηκαν οι εξής τεχνολογίες: Python, TypeScript, HTML5, SCSS, MongoDB, Neo4j (AuraDB) και PostgreSQL.

4.1.α. Δεδομένα

Για το σύστημα, θεωρήθηκε πως:

- Οι ΒΔ είναι διακριτά συστήματα,
- Είναι όλες συνδεδεμένες στο ίντερνετ, αλλά δεν επικοινωνούν μεταξύ τους,
- Ο έλεγχος ταυτότητας του χρήστη και η σύνδεσή του έχουν γίνει σε προηγούμενα στάδια.

Συνεπάγεται ότι ο χρήστης δεν έχει ένα κοινό αναγνωριστικό ανάμεσα στις ΒΔ, καθώς λόγω του ότι είναι διακριτά συστήματα δεν γνωρίζουν τη δομή και το περιεχόμενο των υπολοίπων, κάτι το οποίο δυσκολεύει την αναζήτηση σε όλα τα συστήματα για δεδομένα.

4.1.β. Βάσεις Δεδομένων

Αρχικά χρησιμοποιήθηκαν τρεις τύποι Βάσεων Δεδομένων (ΒΔ): SQL, NoSQL (MongoDB), και Graph (Neo4j).

- Η SQL ΒΔ αφορά εγγραφές ιδιοκτησίας σπιτιών.
- Η Neo4j Graph ΒΔ απεικονίζει τις σχέσεις μεταξύ ιδιοκτητών αυτοκινήτων (ένα αυτοκίνητο μπορεί να ανήκει σε πολλούς ανθρώπους, η ΒΔ γραφημάτων μπορεί να δείξει αυτή τη σχέση).
- Η NoSQL ΒΔ περιέχει εγγραφές ιατρικών προσωπικών δεδομένων.
- Επιπλέον, χρησιμοποιήθηκε μια κεντρική MongoDB, η οποία περιέχει το ιστορικό των αιτήσεων για κάθε χρήστη.
    - Σκοπός αυτού είναι να αποφεύγεται η εκ νέου εκτέλεση αιτημάτων σε διάστημα μικρότερο του ενός μήνα.

Να σημειωθεί πως η κάθε βάση έχει γνώση για τη δομή και το σχήμα (schema) της ίδιας, και δεν γνωρίζει τα αντίστοιχα για τις υπόλοιπες βάσεις του συστήματος. Το μόνο που έχουν προς αναζήτηση είναι τα δεδομένα χρηστών.

4.1.γ. Χρήστες

Παρακάτω φαίνονται οι χρήστες που δημιουργήθηκαν με γενικά δεδομένα και 7 κύρια αναγνωριστικά που είναι διαδεδομένα στην Ελλάδα. Αυτά είναι τα εξής: όνομα, επώνυμο, πατρώνυμο, μητρώνυμο, ημερομηνία γέννησης, αριθμός ταυτότητας, ΑΜΚΑ, ΑΦΜ, ΑΜΑ, κινητό τηλέφωνο, email. Προφανώς, για να αποφευχθεί η πιθανότητα τα στοιχεία αυτά να είναι πραγματικά δεδομένα, δόθηκαν “τυχαίες” τιμές οι οποίες είναι προσαρμοσμένες στη σωστή μορφή του κάθε αναγνωριστικού. Οι ακόλουθοι χρήστες δημιουργήθηκαν ως δοκιμαστικοί χρήστες:

1. { "name": "Johny", "surname": "Doe", "father_name": "Michael", "mother_name": "Sarah", "date_of_birth": "1980-01-01", "amka_id": "12345678901", "afm_id": "987654321", "email": "john.doe@example.com", "mobile_phone": "1234567890", "citizen_id": "CIT12345" }

2. { "name": "Jane", "surname": "Smith", "father_name": "Robert", "mother_name": "Emily", "date_of_birth": "1985-02-02", "amka_id": "23456789012", "afm_id": "876543210", "email": "jane.smith@example.com", "mobile_phone": "2345678901", "citizen_id": "CIT23456" }
3. { "name": "Alice", "surname": "Johnson", "father_name": "David", "mother_name": "Laura", "date_of_birth": "1990-03-03", "amka_id": "34567890123", "afm_id": "765432109", "email": "alice.johnson@example.com", "mobile_phone": "3456789012", "citizen_id": "CIT34567" }
4. { "name": "Bob", "surname": "Brown", "father_name": "James", "mother_name": "Linda", "date_of_birth": "1995-04-04", "amka_id": "45678901234", "afm_id": "654321098", "email": "bob.brown@example.com", "mobile_phone": "4567890123", "citizen_id": "CIT45678" }
5. { "name": "Charlie", "surname": "Davis", "father_name": "William", "mother_name": "Barbara", "date_of_birth": "2000-05-05", "amka_id": "56789012345", "afm_id": "543210987", "email": "charlie.davis@example.com", "mobile_phone": "5678901234", "citizen_id": "CIT56789" }

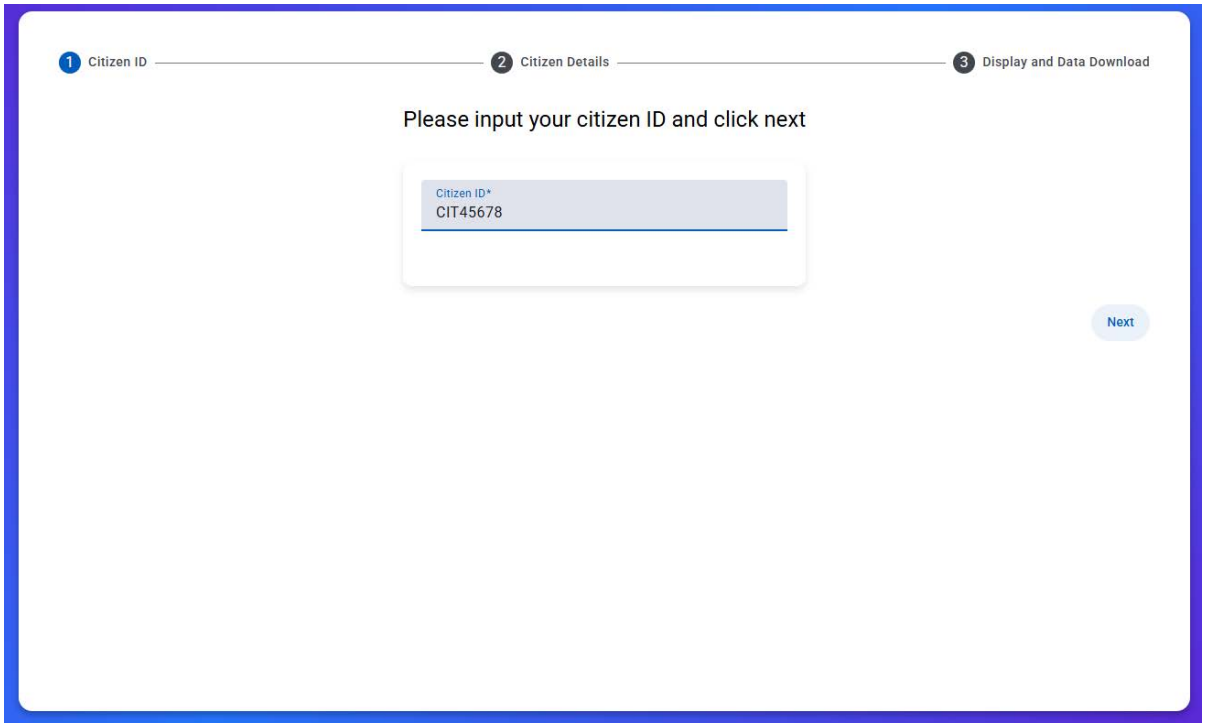
4.2. Παράδειγμα Εκτέλεσης

Στο κεφάλαιο αυτό παρουσιάζεται η λειτουργία του συστήματος από την πλευρά του χρήστη, μέσω της διεπαφής του. Περιλαμβάνεται η περιγραφή των βασικών βημάτων πλοήγησης, οι κύριες λειτουργίες του συστήματος καθώς και η ροή των ενεργειών για την υποβολή και διαχείριση αιτημάτων.

Η αρχική σελίδα του συστήματος φαίνεται παρακάτω, στην Εικόνα 3, όπου ο χρήστης προτρέπεται να εισάγει τον αριθμό ταυτότητας του για να προχωρήσει στο επόμενο βήμα.

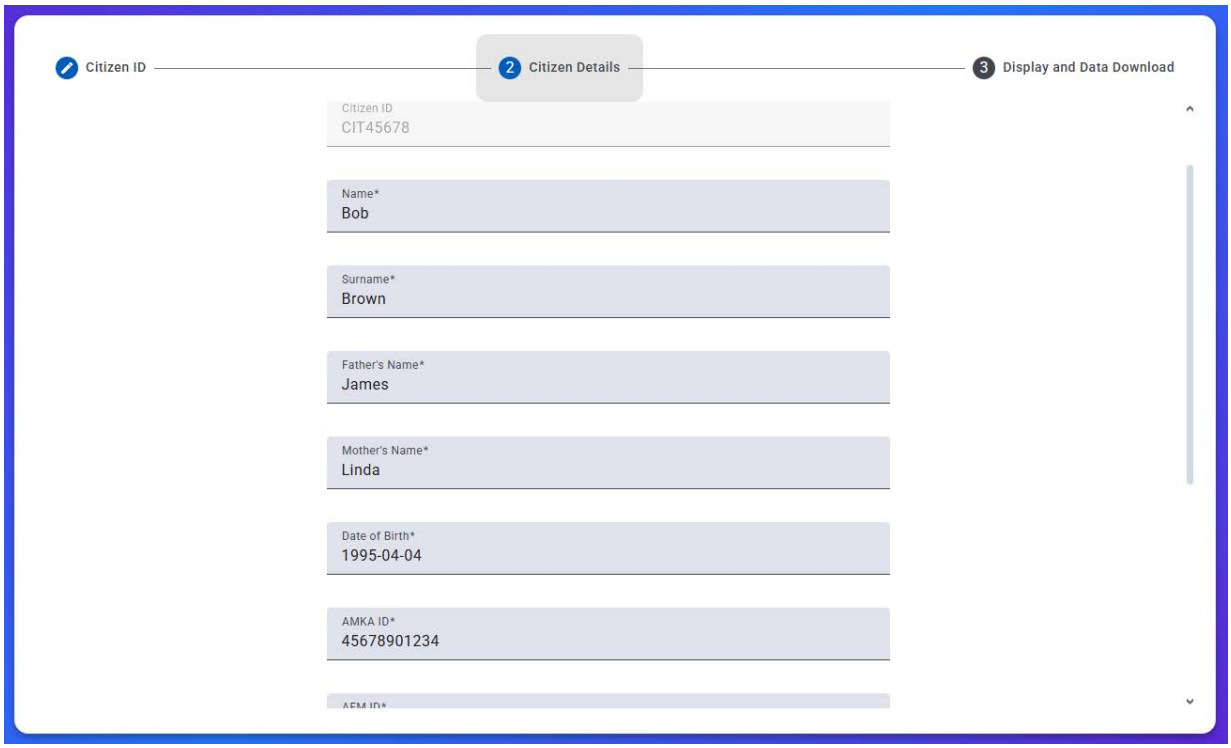
Εικόνα 3:Εικόνα 3 Κεντρική Σελίδα – Προτροπή χρήστη να εισάγει ID

Παρακάτω, πληκτρολογούμε έναν αριθμό ταυτότητας από τους ήδη υπάρχοντες χρήστες που έχουμε δημιουργήσει (Εικόνα 4):

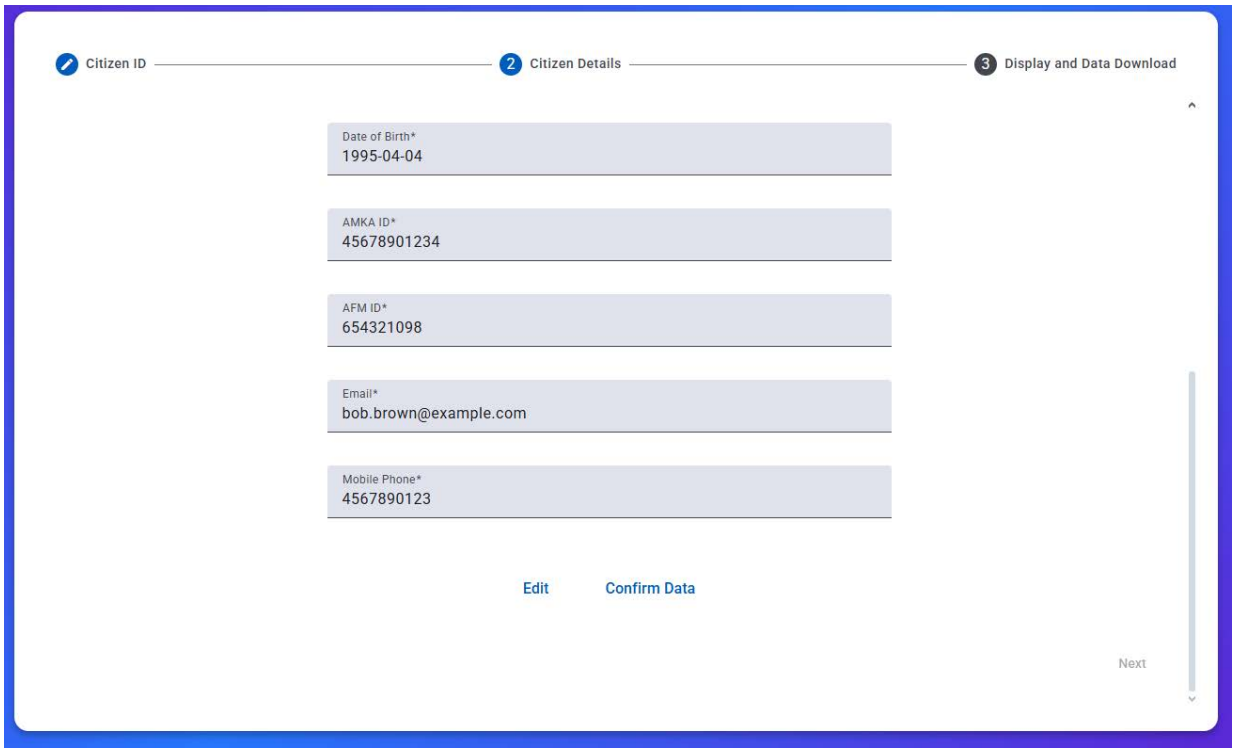


Εικόνα 4: Εισαγωγή Αρ. ταυτότητας χρήστη

Έπειτα, μεταφερόμαστε στο επόμενο στάδιο, που είναι το «Citizen Details», στο οποίο εμφανίζονται τα κύρια αναγνωριστικά του χρήστη (Εικόνα 5, Εικόνα 6).

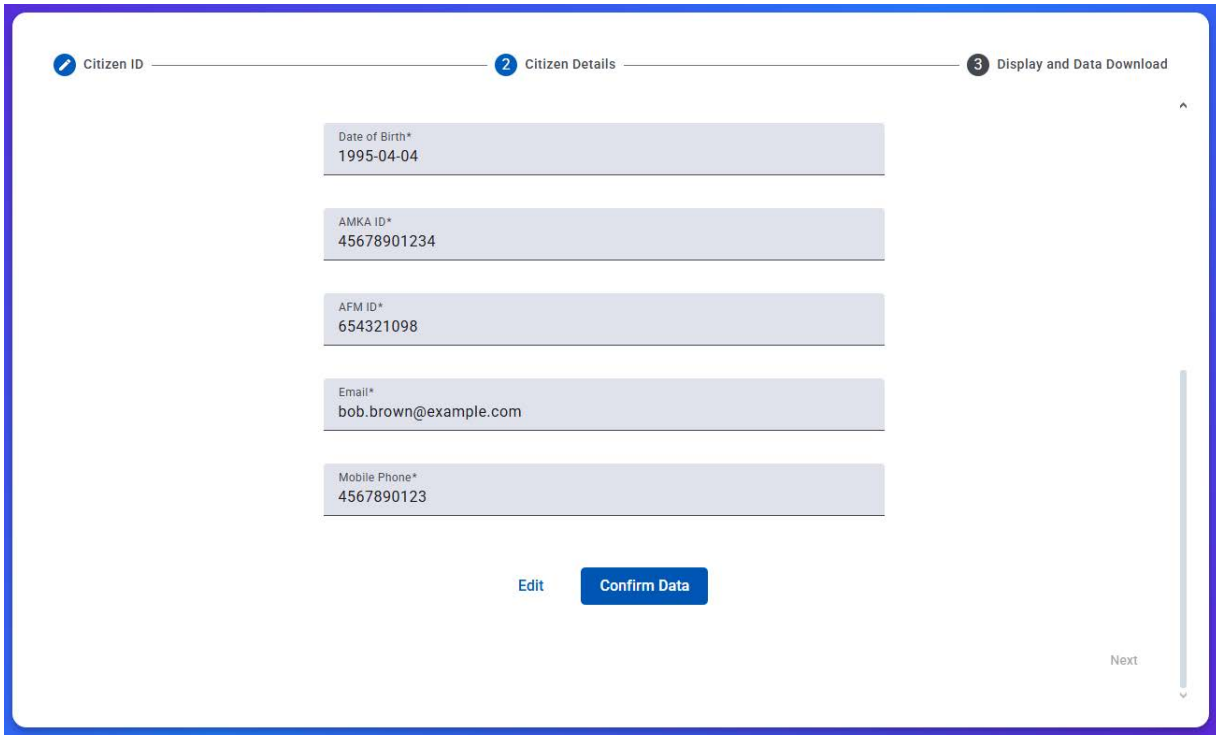


Εικόνα 5: Δεύτερο Στάδιο "Citizen Details"



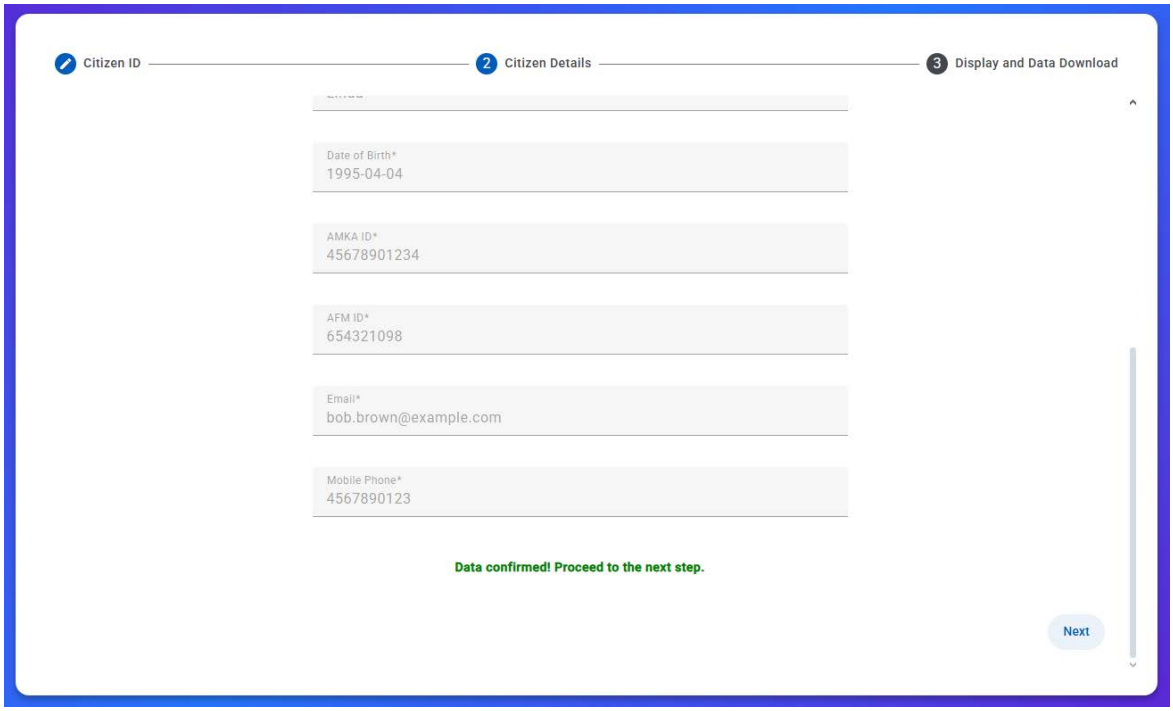
Εικόνα 6: Δεύτερο Στάδιο "Citizen Details"

Τα οποία μπορεί είτε να επαληθεύσει και να προχωρήσει παρακάτω, είτε να ζητήσει την επεξεργασία τους, σε περιπτώσεις που δεν ισχύει κάτι (Εικόνα 7). Προφανώς στο συγκεκριμένο παράδειγμα, η δυνατότητα της επεξεργασίας έχει νόημα μόνο στα πεδία αριθμός κινητού τηλεφώνου και email, καθώς σε όλα τα υπόλοιπα εάν δεν ίσχυε κάτι ή ήταν λανθασμένη εγγραφή, τα δεδομένα προς αλλαγή θα έπρεπε να πιστοποιηθούν από τις αρμόδιες αρχές και γενικώς να ακολουθηθεί μια πιο αυστηρή διαδικασία.



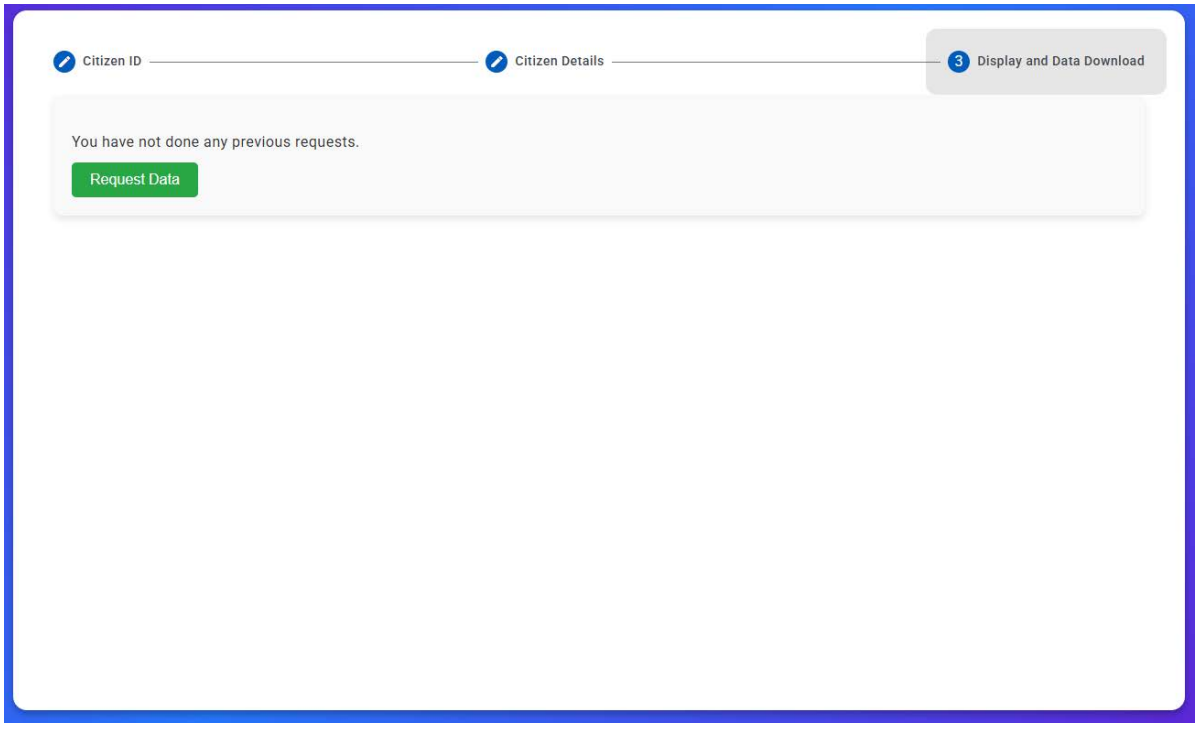
Εικόνα 7: Διαθέσιμες Επιλογές Χρήστη

Αφού λοιπόν επιβεβαιώσει τα δεδομένα, εμφανίζεται η ένδειξη να συνεχίσει στη διαδικασία (Εικόνα 8).



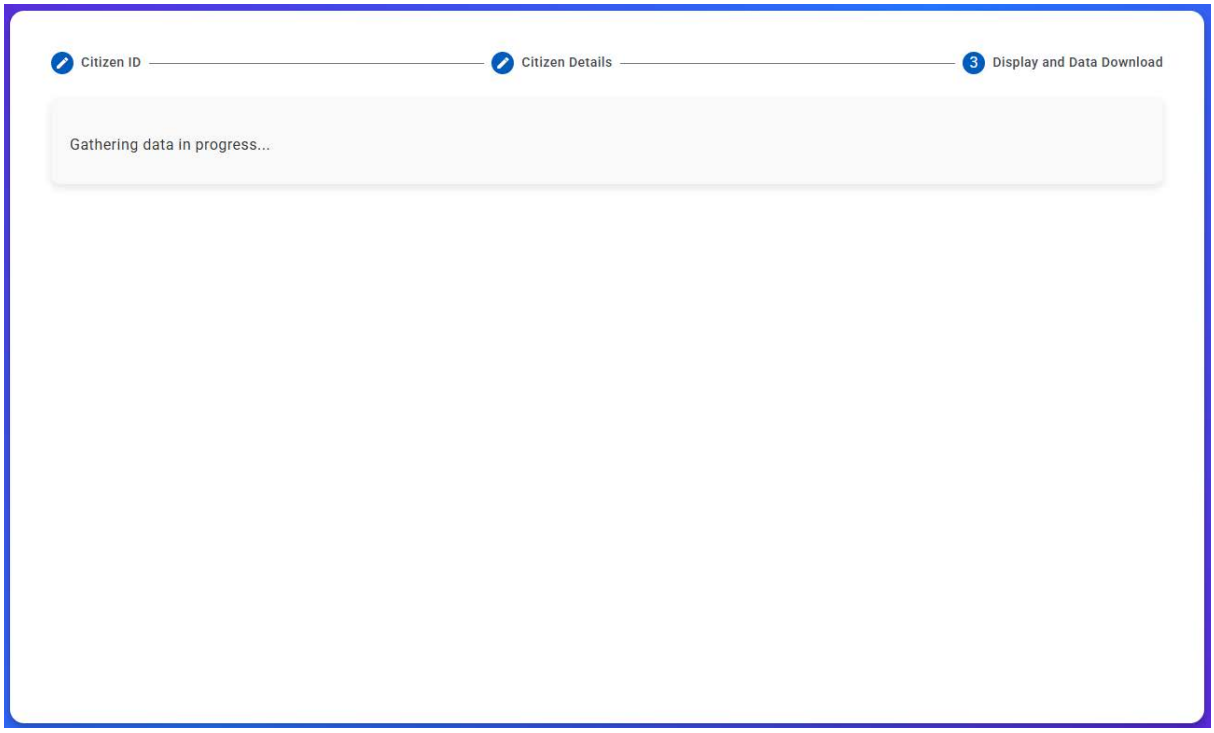
Εικόνα 8: Επιβεβαίωση στοιχείων - Τέλος Στάδιο 2

Στο τελευταίο βήμα «Display and Data Download» εάν δεν έχει ξανά κάνει κάποιο αίτημα πρόσβασης βρίσκεται σε αυτό το στάδιο, όπου του δίνεται η επιλογή να εκκινήσει τη διαδικασία αιτήματος (Εικόνα 9).



Εικόνα 9: Στάδιο 3 Αίτηση Δεδομένων

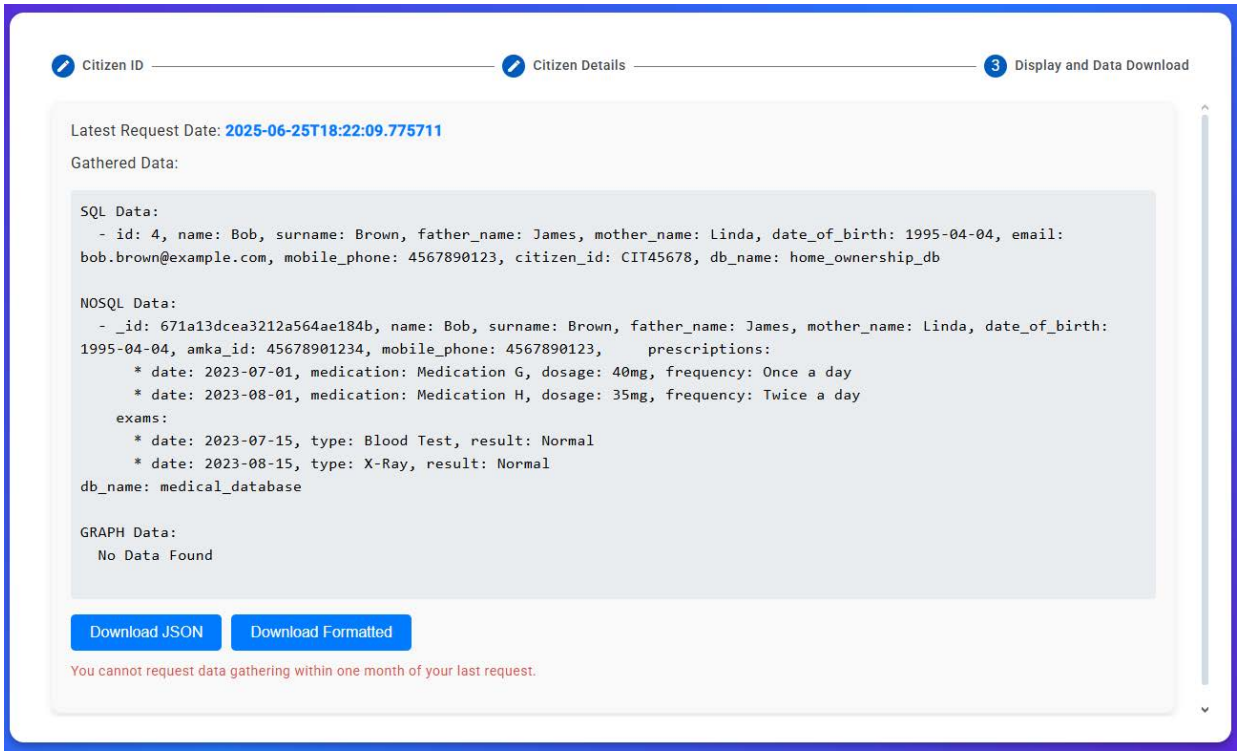
Και ενημερώνεται για την εξέλιξη του (Εικόνα 10).



Εικόνα 10: Αναμονή για τη συλλογή δεδομένων

Όταν ολοκληρωθεί η διαδικασία συλλογής των δεδομένων του, έχει την επιλογή να τα κατεβάσει είτε σε μορφή JSON είτε ως απλό αρχείο (Εικόνα 11). Επίσης, ενημερώνεται για το ότι δεν θα μπορεί να υλοποιήσει κάποιο νέο αίτημα σε διάστημα ενός μήνα.

Τέλος, στις περιπτώσεις που το διάστημα του ενός μήνα δεν έχει παρέλθει, μετά το στάδιο «Citizen Details» (Εικόνα 8) θα βρίσκεται απευθείας σε αυτό το σημείο (Εικόνα 11), χωρίς την επιλογή να κάνει εκ νέου αίτημα. Όλες οι προηγούμενες απαντήσεις στις αιτήσεις πρόσβασής του θα είναι διαθέσιμες προς ανάγνωση και αποθήκευση.



Εικόνα 11: Τελικό Στάδιο – Απάντηση στο αίτημα Πρόσβασης

ΚΕΦΑΛΑΙΟ 5 Συμπεράσματα και Μελλοντικές Επεκτάσεις

Η παρούσα πτυχιακή εργασία είχε ως βασικό στόχο τη μελέτη και την υλοποίηση ενός πληροφοριακού συστήματος που υποστηρίζει την εφαρμογή των δικαιωμάτων των υποκειμένων των δεδομένων, όπως αυτά ορίζονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ), εστιάζοντας στο δικαίωμα πρόσβασης (Άρθρο 15). Ακολουθώντας μια προσέγγιση καταρράκτη, μελετήθηκαν οι περιπτώσεις χρήσης, πραγματοποιήθηκε ανάλυση απαιτήσεων, σχεδιάστηκε μια προτεινόμενη αρχιτεκτονική και στη συνέχεια υλοποιήθηκε ένα λειτουργικό σύστημα το οποίο επιτρέπει την υποβολή και την αυτοματοποίηση της διαχείρισης αιτημάτων χρηστών. Η υλοποίηση βασίστηκε σε σύγχρονες τεχνολογίες, ενώ η αξιολόγησή του πραγματοποιήθηκε με τη χρήση εικονικών χρηστών και δεδομένων, τα οποία προσομοιάζουν πραγματικές περιπτώσεις, καταφέρνοντας έτσι να καλύψει τις βασικές απαιτήσεις ενός τέτοιου σεναρίου.

Η επιτυχής λειτουργία του συστήματος σε ελεγχόμενο περιβάλλον, επιβεβαιώνει ότι η προσέγγιση μπορεί να λειτουργήσει στην πράξη και θέτει τις βάσεις για τη δημιουργία μιας πιο ολοκληρωμένης και επεκτάσιμης λύσης, ικανής να ενσωματωθεί σε πραγματικά πληροφοριακά περιβάλλοντα οργανισμών, τόσο του δημοσίου όσο και του ιδιωτικού τομέα. Μολονότι το σύστημα καλύπτει τις βασικές λειτουργίες, παραμένουν ορισμένοι περιορισμοί, για τους οποίους προτείνονται μελλοντικές επεκτάσεις που θα μπορούσαν να ενισχύσουν το σύστημα.

Αρχικά, μια καλή πρακτική θα ήταν το σύστημα να μπορεί να υποστηρίξει και άλλα δικαιώματα του ΓΚΠΔ, πέραν της πρόσβασης, όπως η διόρθωση, η διαγραφή, ο περιορισμός της επεξεργασίας κτλ. Η δυνατότητα ενσωμάτωσης τέτοιων δυνατοτήτων, θα καθιστούσε το σύστημα πιο ολοκληρωμένο, προσφέροντας μια ευρύτερη και πιο ευέλικτη λύση τόσο για τους οργανισμούς όσο και για τα υποκείμενα των δεδομένων.

Μια ακόμη σημαντική επέκταση είναι η ενσωμάτωση ενός ολοκληρωμένου μηχανισμού ταυτοποίησης των χρηστών, με στόχο την ενίσχυση της εγκυρότητας και της ασφάλειας της συνολικής λειτουργίας του συστήματος. Με αυτό τον τρόπο, το σύστημα θα μπορούσε να καταστεί κατάλληλο για χρήση σε πραγματικά περιβάλλοντα οργανισμών, όπου οι απαιτήσεις ασφάλειας και αξιοπιστίας είναι αυξημένες.

Παράλληλα, η απάντηση που αποστέλλεται στο υποκείμενο των δεδομένων, θα μπορούσε να εξελιχθεί περεταίρω, περιλαμβάνοντας περισσότερες και πιο λεπτομερείς πληροφορίες. Ειδικότερα, πέρα από την απλή παροχή και πρόσβαση σε δεδομένα που αφορούν το υποκείμενο, θα μπορούσαν να περιλαμβάνονται στοιχεία όπως η αιτία συλλογής των δεδομένων, ο σκοπός και η νομική βάση της επεξεργασίας, οι κατηγορίες των προσωπικών δεδομένων, καθώς και πληροφορίες για τους αποδέκτες στους οποίους έχουν διαβιβαστεί ή πρόκειται να διαβιβαστούν τα δεδομένα ή μέρος αυτών. Εξίσου σημαντική είναι η παροχή πληροφοριών σχετικά με τη χρονική διάρκεια διατήρησης των προσωπικών δεδομένων και στις περιπτώσεις που δεν μπορεί να δοθεί ακριβής χρονική περίοδος, να αναφέρονται τα κριτήρια που συμβάλουν στον προσδιορισμό της διάρκειας αυτής.

Μια ακόμη προτεινόμενη επέκταση είναι η ενσωμάτωση των έμμεσων/παραγόμενων δεδομένων, όπως προφίλ που δημιουργούνται από αλγορίθμους ή από συνδυασμούς και αναλύσεις δεδομένων, τα οποία τις περισσότερες φορές επηρεάζουν άμεσα τα δικαιώματα και τις ελευθερίες των υποκειμένων. Η συμπερίληψη αυτών των πληροφοριών, συμβάλει στην ενίσχυση της διαφάνειας και επιτρέπει στο υποκείμενο των δεδομένων μια πιο σαφή και πλήρη εικόνα σχετικά με τον τρόπο που τα προσωπικά του δεδομένα χρησιμοποιούνται.

Συνοψίζοντας, η εργασία αυτή θέτει ένα θεμέλιο για την τεχνική υποστήριξη της αυτοματοποίησης της άσκησης των δικαιωμάτων των υποκειμένων. Οι προτεινόμενες επεκτάσεις ενισχύουν την περαιτέρω πρακτική αξία του συστήματος, και σε συνδυασμό με τη συνεχή προσαρμογή στις εξελισσόμενες απαιτήσεις του κανονιστικού πλαισίου, μπορούν να συμβάλουν ουσιαστικά στην άσκηση των δικαιωμάτων των υποκειμένων καθώς και στην συμμόρφωση των υπευθύνων επεξεργασίας με τον ΓΚΠΔ.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] European Data Protection Board (EDPB), *Guidelines 01/2022 on data subject rights – Right of access, Version 1.0*, Brussels: EDPB, 18 Ιανουαρίου 2022. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en

[2] M. Hansen και M. Jensen, *A Generic Data Model for Implementing Right of Access Requests*, στο Privacy Technologies and Policy: 10th Annual Privacy Forum, APF 2022, Βαρσοβία, Πολωνία, 23–24 Ιουνίου 2022, Πρακτικά. Berlin, Heidelberg: Springer-Verlag, 2022, σσ. 3–22. https://doi.org/10.1007/978-3-031-07315-1_1

[3] Φούντα Δ., *Διαδικασίες και πολιτικές για συμμόρφωση ανώτατων εκπαιδευτικών ιδρυμάτων με το ΓΚΠΔ*, Μεταπτυχιακή διπλωματική εργασία, Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων», Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς, Πειραιάς, Νοέμβριος 2018. https://dione.lib.unipi.gr/xmlui/handle/unipi/11672

[4] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs') – WP 243 rev.01*, Brussels: European Commission, 5 Απριλίου 2017. https://ec.europa.eu/newsroom/article29/items/612048

[5] European Parliament and Council, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Official Journal of the European Union, L 119, 27 Απριλίου 2016. http://data.europa.eu/eli/reg/2016/679/oj