UNIVERSITY OF THE AEGEAN

DEPT. OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

Diploma Thesis

Analysis, Design and Implementation of an Open-Source Web-Based System for GDPR Compliance Assessment

Giannis Konstantinidis

UNIVERSITY OF THE AEGEAN

DEPT. OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

Diploma Thesis

Analysis, Design and Implementation of an Open-Source Web-Based System for GDPR Compliance Assessment

Ανάλυση, Σχεδιασμός και Υλοποίηση ενός Ανοικτού Κώδικα Συστήματος Ιστού για την Εκτίμηση Συμμόρφωσης με τον ΓΚΠΔ

Author:	Giannis Konstantinidis
Supervisor:	Prof. Dr. Spyros Kokolakis
Submission Date:	February 2019

I confirm that this thesis is my own work and I have documented all sources and material used.

Samos, February 2019 Giannis Konstantinidis

Acknowledgements

Personal

First and foremost, I would like to thank my family for their continuous support throughout my whole life and for encouraging me amidst my academic and professional endeavours.

I would also like to give a shout-out to my friends, classmates, and colleagues for the unforgettable moments we have shared the last few years as university students.

Institutional

I wish to thank Prof. Dr. Spyros Kokolakis for his consistent guidance throughout the conducting of this thesis and his valuable input and leading expertise. More importantly, I thank him for inspiring me throughout his teachings and for motivating me to become involved with the privacy and data protection domain.

Executive Summary

Background

The European Union (EU) has recently introduced the General Data Protection Regulation (GDPR) with the aim of giving residents additional control over their personal data. Consequently, data controllers and data processors are required to achieve and demonstrate continuous compliance with the regulation. While the regulation thoroughly describes the rights of the data subjects and the obligations of data controllers and processors, it does not offer any means of determining the compliance level and suggesting improvements if needed.

Problem Statement

Large organisations can afford high-quality consulting services, extensive evaluations, and effective revisions and adjustments to their business processes. However, this is presumably not the case with everyone else. The software market features sophisticated products with remarkable features to help determine the alignment of an entity with the regulation and propose resolutions, but such products are usually expensive to acquire and maintain. In the meantime, there are also solutions provided free-of-charge which however lack essential features and fail to produce comprehensive assessments. There is currently an important need for appropriate solutions, directed towards individuals and Small and Medium-Sized Enterprises (SMEs), which are available free of charge and offer satisfactory quality.

Purpose

The purpose of this diploma thesis is to analyse, design and implement an open-source web-based system for GDPR compliance assessment. The system's intended users can submit the processing activities their organisation performs, evaluate the alignment of their organisation with the GDPR, and also conduct Data Protection Impact Assessments (DPIAs) which the regulation expects under certain conditions. Besides the developed system, this diploma thesis additionally proposes an elementary model for GDPR compliance assessment and meanwhile provides extensive documentation that explains the entire process.

Methodology

The conceptualisation of the evaluation model and the subsequent development of the system is challenging. The proposed model considers articles that exist within the regulation's chapters one to four. These articles are considered to be applicable in most traditional data processing scenarios performed by individuals and SMEs. For an adequate alignment with the regulation, this thesis proposes a 2+1 step process. The intended user of the system first submits the processing activities their organisation performs and then answers questions regarding the readiness of their organisation. The system checks the answers of the user, examines the previously submitted processing activities and determines the compliance based on a predefined set of rules. If the DPIA considered necessary, the user performs that assessment manually while being assisted by the system.

Implementation

The resulting system utilises up-to-date open web technologies to achieve the expected functionality and showcases a modern user interface that works across multiple devices, screen resolutions and operating systems. Moreover, particular security mechanisms and controls exist within the system and contribute to its planned production-ready status. The system features its unique brand identity, includes end-user and technical documentation, and is available under the GNU AGPL v3 free and open-source software license.

Evaluation

To evaluate the appropriateness and effectiveness of the implemented system, the author of this thesis invited experts with a diverse set of skills to offer their feedback. The experts confirmed the system serves its intended purpose, noted down minor issues and recommended improvements to consider in future updates. The proposed system does not directly oppose advanced business solutions offered by professional software companies and consulting firm but exhibits satisfactory evaluations directed towards the majority of individuals and SMEs that are coping with compliance.

Additional Thoughts

There seem to be significant challenges within the global privacy and data protection field, as even prevailing companies are discovered not to be fully complying with the regulation. It is not only necessary to highlight the significance of privacy and increase awareness around data protection matters, but also to inform people of the potential risks related to the treatment of personal data as well as of the available controls and obligations that now apply.

Επιτελική Σύνοψη

Πλαίσιο

Η Ευρωπαϊκή Ένωση (ΕΕ) πρόσφατα εισήγαγε τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) με σκοπό να δώσει στους πολίτες επιπρόσθετο έλεγχο των προσωπικών τους δεδομένων. Ως συνέπεια, οι υπέυθυνοι επεξεργασίας δεδομένων και οι εκτελούντες την επεξεργασία δεδομένων υποχρεούνται να επιτύχουν και να αποδεικνύουν διαρκώς τη συμμόρφωση τους με τον κανονισμό. Ενώ ο κανονισμός περιγράφει αναλυτικά τα δικαιώματα των υποκειμένων των δεδομένων και τις υποχρεώσεις των υπευθύνων και εκτελούντων επεξεργασίας δεδομένων, δεν προσφέρει κάποιο μέσο ώστε να προσδιοριστεί το επίπεδο συμμόρφωσης και να προταθούν προσαρμογές, εφόσον χρειάζονται.

Πρόβλημα

Οι μεγάλοι οργανισμοί έχουν την οικονομική δυνατότητα για συμβουλευτικές υπηρεσίες υψηλής ποιότητας, εκτενείς αξιολογήσεις και τροποποιήσεις στις επιχειρηματικές τους διαδικασίες. Ωστόσο, αυτό πιθανώς δε συμβαίνει στις υπόλοιπες περιπτώσεις. Η αγορά λογισμικού διαθέτει εκλεπτυσμένα προϊόντα με εξαιρετικά χαρακτηριστικά που βοηθούν στην εκτίμηση της συμμόρφω–σης μιας οντότητας με τον κανονισμό και προτείνουν αποφάσεις. Αλλά, τέτοια προϊόντα είναι συνήθως ακριβά στην προμήθεια και συντήρηση τους. Εν τω μεταξύ, υπάρχουν επίσης λύσεις που διατίθενται δωρεάν ωστόσο στερούνται βασικών χαρακτηριστικών και αδυνατούν να παράγουν περιεκτικές αξιολογήσεις. Υπάρχει επί του παρόντος μια σημαντική ανάγκη για κατάλληλες λύσεις, που απευθύνονται σε μεμονωμένα άτομα και μικρομεσαίους οργανισμούς, που διατίθενται δωρεάν και προσφέρουν ικανοποιητική ποιότητα.

Σκοπός

Σκοπός αυτής της διπλωματικής εργασίας είναι να αναλύσει, να σχεδιάσει και να υλοποιήσει ένα ανοικτού κώδικα σύστημα ιστού για την εκτίμηση συμμόρφωσης με τον ΓΚΠΔ. Οι προοριζόμενοι χρήστες του συστήματος μπορούν να υποβάλλουν τις δραστηριότητες επεξεργασίας που εκτελεί ο οργανισμός τους, να αξιολογήσουν την ευθυγράμμιση του οργανισμού τους με τον ΓΚΠΔ και να διεξάγουν Εκτιμήσεις Αντικτύπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ) που ο κανονισμός απαιτεί κάτω από συγκεκριμένες προϋποθέσεις. Εκτός από το υλοποιημένο σύστημα, αυτή η διπλωματική εργασία προτείνει επιπροσθέτως ένα στοιχειώδες μοντέλο εκτίμησης της συμμόρφωσης με τον ΓΚΠΔ και παράλληλα παρέχει εκτεταμένη τεκμηρίωση που περιγράφει τη συνολική διαδικασία.

Μεθοδολογία

Η σύλληψη του μοντέλου αξιολόγησης και η ακόλουθη ανάπτυξη του συστήματος είναι απαιτητική. Το προτεινόμενο μοντέλο λαμβάνει υπόψη τα άρθρα που βρίσκονται μεταξύ των κεφαλαίων ένα έως τέσσερα του κανονισμού. Τα άρθρα αυτά θεωρούνται ότι εφαρμόζονται στις περισσότερες συνήθεις περιπτώσεις επεξεργασίας δεδομένων που πραγματοποιούνται από μεμονομένα άτομα και μικρομεσαίους οργανισμούς. Για την ικανοποιητική ευθυγράμμιση με το κανονισμό, αυτή η διπλωματική προτείνει μία διαδικασία 2+1 βημάτων. Ο προοριζόμενος χρήστης του συστήματος πρώτα υποβάλλει τις δραστηριότητες επεξεργασίας που πραγματοποιεί ο οργανισμός του και έπειτα απαντάει σε ερωτήσεις σχετικά με την ετοιμότητα του οργανισμού του. Το σύστημα ελέγχει τις απαντήσεις του χρήστη, εξετάζει τις δραστηριότητες επεξεργασίας και καθορίζει το επίπεδο συμμόρφωσης βασισμένο σε ένα προκαθορισμένο σύνολο κανόνων. Εάν η ΕΑΠΔ θεωρείται απαραίτητη, ο χρήστης πραγματοποιεί την εκτίμηση χειροκίνητα υποβοηθούμενος από το σύστημα.

Υλοποίηση

Το επακόλουθο σύστημα χρησιμοποιεί επίκαιρες ανοικτές τεχνολογίες ιστού για να επιτύχει την αναμενόμενη λειτουργικότητα και διαθέτει μία μοντέρνα διεπαφή χρήστη που λειτουργεί σε διαφορετικές συσκευές, αναλύσεις οθόνης και λειτουργικά συστήματα. Επιπλέον, συγκεκριμένοι μηχανισμοί ασφάλειας και έλεγχοι βρίσκονται εντός του συστήματος και συνεισφέρουν στην προγραμματισμένη πλήρως λειτουργική κατάσταση του. Το σύστημα χαρακτηρίζεται από μία μοναδική σχεδιαστική ταυτότητα, περιλαμβάνει τεκμηρίωση για τελικούς χρήστες και επαγγελματίες της τεχνολογίας, και διατίθεται κάτω από την άδεια ελεύθερου και ανοικτού λογισμικού GNU AGPL v3.

Αξιολόγηση

Για την αξιολόγηση της καταλληλότητας και αποτελεσματικότητας του υλοποιημένου συστήματος, ο συγγραφέας αυτής της διπλωματικής προσκάλεσε ειδικούς με ένα ευρύ σύνολο δεξιοτήτων για να αποτυπώσουν τη γνώμη τους. Οι ειδικοί επιβεβαίωσαν ότι το σύστημα εξυπηρετεί τον προβλεπόμενο σκοπό του, σημείωσαν μικρά ζητήματα και πρότειναν βελτιώσεις για να ληφθούν υπ' όψιν σε μελλοντικές ενημερώσεις. Το προτεινόμενο σύστημα δεν έρχεται άμεσα αντιμέτωπο με προηγμένες εταιρικές λύσεις που προσφέρονται από εξειδικευμένος εταιρείες ανάπτυξης λογισμικού και συμβουλευτικές εταιρείες, ωστόσο παρουσιάζει ικανοποιητικές αξιολογήσεις που απευθύνονται στην πλειοψηφία των ιδιωτών και των μικρομεσαίων επιχειρήσεων που αντιμετωπίζουν προβλήματα συμμόρφωσης.

Επιπρόσθετες Σκέψεις

Φαίνεται ότι υπάρχουν σημαντικές προκλήσεις στον διεθνή χώρο της ιδιωτικότητας και προστασίας δεδομένων, καθώς ακόμη και οι επικρατέστερες εταιρείες ανακαλύπτονται να μη συμμορφώνονται πλήρως με τον κανονισμό. Είναι απαραίτητο να δοθεί έμφαση στην αξία της ιδιωτικότητας, να υπάρξει κατάλληλη ενημερότητα γύρω από θέματα προστασίας δεδομένων και να ενημερωθούν οι πολίτες για τους πιθανούς κινδύνους που σχετίζονται με τη μεταχείριση των προσωπικών τους δεδομένων και παράλληλα τους διαθέσιμους ελέγχους και υποχρεώσεις που πλέον βρίσκονται σε ισχύ.

Contents

List of Figures

List of Tables

List of Acronyms

Art.	Article
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
ERD	Entity–Relationship Diagram
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
ID	Identity Document
MVC	Model-View-Controller
ORM	Object–Relational Mapping
Par.	Paragraph
PIA	Privacy Impact Assessment
SME	Small and Medium–Sized Enterprise
SSO	Single Sign–On
WCAG	Web Content Accessibility Guidelines

1. Introduction

1.1. Background

The EU General Data Protection Regulation (GDPR), also known as Regulation (EU) 2016/679, provides EU residents with additional control over their personal data. The regulation was first published in April 2016 and came into force on May 25, 2018. It repeals the former Directive 95/46/EC which was adopted in 1995 and remained valid until May 24, 2018.

An EU regulation implies a binding legislative act that applies across all EU member states (Folsom, Lake, & Nanda, 1996). On the contrary, an EU directive merely establishes objectives that EU members must accomplish and, for that purpose, the latter formulate their discrete laws (Steiner, Woods, & Twigg-Flesner, 2006). Since the GDPR is an EU regulation, rather than an EU directive, it appears the legislators desired the harmonisation of data protection laws across the EU.

During the last twenty to thirty years, the Information and Communications Technology (ICT) industry has evolved and grown remarkably. Nowadays, computer networks transmit vast volumes of data across continents within seconds. The amount of data, relating to citizens, that organisations are collecting and processing is enormous. Hence, the demand for contemporary data protection legislation became apparent.

The regulation thoroughly describes data subjects rights and the obligations of data controllers and processors but appears not to support data controllers and data processors with achieving and demonstrating compliance. To put it another way, it tells data controllers and data processors what to do but not how (Garber, 2018).

Every natural or legal person handling data that refer to EU residents must comply with the regulation. Failure to do so may result in significant fines as high as 20 million Euros or 4% of the annual worldwide turnover. The EU may commonly impose draconian penalties on perpetrators.

Unarguably, the GDPR makes outstanding arrangements to the privacy and data protection domain worldwide. Since the regulation came into effect a few months ago, it seems to be quite early to predict what is going to happen next. Everybody who processes personal data must nevertheless show considerable attention.

1.2. Problem Statement

The regulation creates new opportunities for the harmonisation of data protection practices not only across the EU but generally worldwide. Nevertheless, it does not make mattering distinctions based on the size of entities or the amount of personal data that individuals or organisation process. In essence, everybody who processes personal data must conform to the provisions of the GDPR one way or another. Miglicco (2018) considers that many of the regulation's requirements are not well understood by those affected. This new data protection regime results into inequalities. Individuals not unaffiliated with large organisations, plus SMEs are conceivably subject to grapple with compliance.

While gigantic and prevailing organisations can afford high-quality consulting services, extensive evaluations, and effective revisions and adjustments to their business processes, this is presumably not the case with the rest of the world. Scantier entities risk decisive regulatory response if found to be non-compliant. More importantly, they may be overwhelmed with the loss of their customer's trust and likely lose competitive advantage on the market as a consequence.

Software vendors, consulting agencies, organisations and also individuals have published tools and solutions to help determine the alignment of an entity with the regulation and propose resolutions. Sophisticated products offer remarkable features but tend to be proprietary, i.e., closed-source software with austere licensing preferences and the lack of customisation, and very expensive to acquire and sustain. Elseways, complimentary software of this kind may help improve awareness around compliance matters but are typically incapable of leading to comprehensive assessments. Hence the necessity for solutions, directed towards individuals and SMEs, which are available free of charge and offer central characteristics of satisfactory quality.

1.3. Scope and Objectives

The scope of this diploma thesis is to analyse, design and implement an open-source web-based system for GDPR compliance assessment, as the title suggests.

Free and open-source software allows anyone to inspect, modify, and enhance the software. Furthermore, a modern web-based system, i.e., a system that utilises web technologies, does not make any distinctions concerning hardware or software; anyone may use the system regardless of their device or operating system. These two aspects can potentially play an indispensable role in the development and adoptability of the system.

The objectives that relate to the scope of this diploma thesis begin with the extensive study of the essential articles of the regulation relating to compliance. They additionally include the study and consultation of existing literature, although there appears that a plethora of academic work is currently nonexistent considering the relatively recent introduction and implementation of the regulation. Following the study and review of both the legal text and relevant work, this diploma thesis continues with the design of an uncomplicated model for an elementary GDPR compliance assessment. More importantly, this thesis concerns the requirements analysis and use-case specifications that the concluding implementation relies upon. Last but not least, standard end-user documentation accompanies the implemented system and intends for actual user adoption.

Therefore, in order to summarise, this diploma thesis incorporates the following deliverables:

- An elementary model for GDPR compliance assessment;
- An essential system analysis and design, including use-case specification and requirements analyse;
- An open-source web-based system for GDPR compliance assessment; and
- The end-user documentation accompanying the system.

1.4. Assumptions and Limitations

Privacy, data protection, and ICT professionals, among others, argue that the GDPR is one of the most complex pieces of regulation the EU has ever bestowed. It does include 99 articles, which span across 88 pages of text, and 173 recitals.

The composer of this thesis does not possess a solid legal background but concentrates on information and communication systems engineering instead. Therefore, this thesis does not analyse the regulation in-depth neither does it intend to produce some sophisticated assessment model and its corresponding perfected web-based system.

This diploma thesis analyses most common and prevailing articles included in the regulation, notably from chapters one (1) to four (4). It does not consider articles that exist between chapters five (5) and eleven (11). The initial four chapters incorporate articles that should be applicable in most traditional data processing scenarios performed by individuals and SMEs. On the contrary, the succeeding seven chapters describe more complicated scenarios several of which are regulatory.

As aforementioned, the regulation came into the whole effect from May 25th, 2018. Although there are ongoing legal cases based on complaints, that individuals and digital rights organisations have submitted, it is considerably early to consider court rulings. Likewise, very few scientific journals, papers, and textbooks do exist. The current situation significantly limits the review of engaged literature.

The proposed compliance assessment model and corresponding open–source web–based system strive to be as straightforward and easy–to–use as possible, having individuals and traditional SMEs in mind. However, it is safe to assume that the prospective users of the open–source web–based system need to maintain some foundational knowledge around the regulation, privacy, and data protection matters before claiming the maximum benefit.

1.5. Thesis Structure

This chapter presents an overview of this thesis and its purposes. It provides concise background information about the regulation, indicates the need for supporting organisations become and remain compliant with the GDPR, and reveals the assumptions and limitations that apply to this thesis.

The second chapter illustrates some of the critical aspects of the regulation, including organisational requirements, processing requirements and data subject rights, and meanwhile attempts to highlight the importance of achieving sufficient data protection mechanisms.

The third chapter describes the methodology this thesis reflects. Furthermore, it analyses, designs and describes the implementation of an open–source web–based system for GDPR compliance assessment.

Finally, the fourth and final chapter summarises the outcomes of this thesis, provides an overview of its critical elements and concludes with providing further recommendations for the enhancement of its outcomes.

2. Fundamental Aspects

2.1. Terminology and Scope

This section covers the essential terminology and application scope of the regulation. The final legal text encompasses several additional terms and discusses the scope of the GDPR with higher detail. This segment focuses instead on the most relevant parts for the scope of this thesis.

2.1.1. Essential Terminology

The regulation consolidates several terms, some of which already existed in the now-repealed Directive. This subsection acquaints the reader with the most prevailing, and relevant to the purposes of this thesis, expressions.

2.1.1.1. Personal Data

Personal data comprises any information associated with an *identified or identifiable natural person* (Art. 4 Par. 1 GDPR). Examples of information that may constitute personal data include:

- Name;
- Identification Numbers (e.g., an ID or passport number);
- Home Address;
- Phone Number;
- E-mail Address;
- IP Address;
- Location Data (e.g., a mobile phone that sends GPS coordinates).

According to Rec. 27 GDPR, the regulation *does not apply to the personal data of deceased persons*. Nonetheless, Rec. 27 GDPR advises that EU member states may produce individual controls concerning the processing of personal data of deceased persons.

2.1.1.2. Special Categories of Personal Data

Art. 9 GDPR reveals that personal data indicating *racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation* are considered special categories of personal data. The same article prohibits the processing of special categories of personal data unless one or more specific conditions apply.

2.1.1.3. Processing

Processing indicates any *operation or set of operations performed on personal data or on sets of personal data.* These operations may include the *collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination [...], alignment or combination, restriction, erasure or destruction* of personal data (Art. 4 Par. 2 GDPR).

Voigt and von dem Bussche (2017) suggest that any treatment of data can be acknowledged as processing. Some cases that may involve the processing of personal data follow below:

- Payroll Management;
- Newsletter Management (e.g., maintaining lists of newsletter subscribers);
- Video Surveillance (e.g., operating CCTV systems);
- Security Audit Logging (e.g., storing IP addresses in security logs).

Last but not least, the regulation does not make any distinction between automated and non-automated processing (Art. 4 Par. 2 GDPR).

2.1.1.4. Data Subject

The data subject is the person to whom personal data refer. According to Art. 4 Par. 1 GDPR, the data subject *is an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier [...] or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

2.1.1.5. Controller

The controller *determines the purposes and means of data processing* (Art. 4 Par. 7 GDPR). The processor may be a natural or legal person, public authority, agency or other body.

2.1.1.6. Processor

The processor is responsible for processing *personal data on behalf of the data controller* (Art. 4 Par. 8 GDPR). Similarly to the controller, any natural or legal person, public authority, agency or other body may assume the role of the processor.

2.1.1.7. Joint Controllers

The legislator was aiming for an explicit allocation of responsibilities and therefore introduced the concept of joint controllers (Voigt & von dem Bussche, 2017). If two or more controllers *jointly determine the purposes and means of processing*, they are called joint controllers.

According to Art. 26 Par. 1 GDPR, joint controllers are required *to determine their respective responsibilities for compliance with the obligations* under the regulation. Joint controllers need to arrange the exercising of the rights of data subjects and fulfil their respective duties to provide the information to the data subjects as described in Art. 13 GDPR and Art. 14 GDPR.

2.1.2. Application Scope

Art. 3 GDPR defines the territorial scope of the regulation. If the controller or processor have established their presence and conduct their associated activities within the EU, the regulation applies notwithstanding where the processing takes place (Art. 3 Par. 1 GDPR). The GDPR can likewise apply to organizations outside of the EU, under distinct conditions (Houser, 2018). Indeed, Art. 3 Par. 2 indicates two certain conditions which this subsection is not going to analyse further.

Besides the territorial scope, the regulation involves the material scope. Art. 2 Par. 1 GDPR tells that the regulation applies to data processing *wholly or partly by automated means*, or even without automated means as long as personal data form, or intend to form, *part of a filing system*.

2.2. Organisational Requirements

The GDPR introduces a risk-based approach that makes the rules and principles of data protection law work better (Leenes, van Brakel, Gutwirth, & Hert, 2017). While the controller is primarily responsible for compliance with the regulation, the processor can no longer hide behind the respective data controller if regulatory action arises (Gregg Latchams Solicitors, 2017).

The following subsections present some of the most critical organisational requirements for achieving and demonstrating compliance.

2.2.1. Data Protection by Design and by Default

The regulation expects controllers to utilise all necessary measures from the very beginning to safeguard personal data and meanwhile process personal data while thoroughly complying with fundamental data protection principles.

The controller should implement *appropriate technical and organisational measures* and integrate necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects (Art. 25 Par. 1 GDPR). In regards to data protection by design, the controller *shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed* (Art. 25 Par. 2 GDPR).

Data protection by design and by default is also reflected in Rec. 78 GDPR which notes that the controller *should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default*. Rec. 78 GDPR also highlights few essential practices:

- Performing data minimisation;
- Performing data pseudonymisation;
- Demonstrating transparency while handling personal data;
- Enabling data subjects to monitor the processing of their personal data;
- Appending and enhancing security mechanisms for guarding personal data.

2.2.2. Records of Processing Activities

Art 30 Par. 1 GDPR stresses the necessity of maintaining records of processing activities. Every controller must maintain such records which incorporate information such as the name and contact details of the controller(s) and corresponding Data Protection Officers (DPOs), the purposes behind the processing, the categories of recipients who receive the personal data, and a general description of implemented technical and organisational measures.

Records of processing activities is not an obligation limited exclusively to controllers. As stated in Art. 30 Par. 2 GDPR, each processor should maintain records for all processing activities *carried out on behalf of a controller*.

2.2.3. Technical and Organisational Measures

Controllers and processors are expected to implement technical and organisational measures to ensure the continuous protection of personal data. According to Art. 32 Par. 1 GDPR, they need to *ensure a level of security appropriate to the risk* and meanwhile consider these following paradigms:

- Peudonymising and encrypting personal data;
- Ensuring the constant *confidentiality, integrity, availability and resilience* of processing systems and services;
- Restoring *the availability and access to personal data*, without further delay, in case a physical or technical incident takes place;
- Regularly *testing, assessing and evaluating the effectiveness* of technical and organisational measures to guarantee the security of the processing.

2.2.4. Personal Data Breaches

Personal data breach implies an unauthorised system access which results into *the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of [...] personal data transmitted, stored or otherwise processed*.

2.2.5. Data Protection Impact Assessment

The Data Protection Impact Assessment works as an assistive mechanism that controllers can practice to conform to the legal obligations of the GDPR and mitigate risks related to the rights and freedoms of data subjects (Hansen, Kosta, Nai-Fovino, & Fischer-Hübner, 2018). Art. 35 Par. 3 GDPR sets three conditions that require the processor to conduct a DPIA:

- *A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
- *Processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
- *A systematic monitoring of a publicly accessible area on a large scale.*

The DPIA further expands the already-known Privacy Impact Assessment (PIA) but, in contrast to the latter, does not explicitly focus on privacy (Quelle, 2015). According to Art. 35 Par. 7 GDPR, every DPIA should include at least the following:

- *A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- *An assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- *An assessment of the risks to the rights and freedoms of data subjects; and*

- *The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure theprotection of personal data and to demonstrate compliance with the regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

2.2.6. Data Protection Officer

The Data Protection Officer is an individual tasked with ensuring the compliance of the controller with the regulation and providing knowledge and advise on data protection matters (P. Lambert, 2016). Organisations may appoint an existing employee as DPO, who is well-informed about data protection, or hire one externally. That person must nevertheless be able to act autonomously and communicate straight with upper management (Information Commissioner's Office, 2018a).

Art. 37 Par. 1 GDPR depicts three distinct situations under which the controller and processor must designate a DPO:

- A *public authority or body* carries out the processing, except for courts operating in their *judicial capacity*;
- The controller or the processor performs processing activities demanding the *regular and systematic monitoring of data subjects on a large scale*; or
- The controller or the processor performs processing activities involving a large number of special categories of personal data and personal data *relating to criminal convictions and offences*.

2.3. Processing Requirements

Compliance, in the context of the GPDR, comprises a continuous process. Apart from organisation-wide requirements, each processing activity must adhere to added requirements.

Moore (2018) opines that the regulation imposes harsh penalties to organisations that fail to comply. Admittedly, infringements of several provisions can be subject to administrative fines up to 20,000,000 EUR or up to 4% of the total worldwide annual turnover of the preceding financial year according to Art. 83 Par. 5 and Art. 83 Par. 6 GDPR. Controllers and processors

2.3.1. Processing Principles

Art. 5 Par. 1 GDPR introduces six distinct principles that adhere to every data processing operation. Art. 5 Par. 2 GDPR presents the term of accountability, which makes every controller responsible for reaching and demonstrating compliance with the six principles established within the first paragraph.

2.3.1.1. Lawfulness, Fairness and Transparency

Organisations should process personal data in lawful, fair and transparent conduct while actualising relevant security standards to guarantee integrity and confidentiality (Gkoulalas-Divanis & Bettini, 2018). The data protection directive had already rendered lawful and fair data processing; the GDPR extends these principles by expecting personal data processing in a transparent manner (Synodinou, Jougleux, Markou, & Prastitou, 2017).

Rec. 39 GDPR elaborates on those expectations further and requires organisations to provide *information to the data subjects on the identity of the controller and the purposes of the processing* and *further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed*.

2.3.1.2. Purpose Limitation

Purpose limitation is a substantive principle of the regulation which permits the processing of personal data for a distinct purpose (Hijmans, 2016). Personal data must be *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes* (Art. 5 Par. 1 GDPR).

2.3.1.3. Data Minimisation

Personal data need to be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* (Art. 5 Par. 1 GDPR). Data minimisation often relates to purpose limitation, as it necessitates that explicitly outlined purposes support the processing of personal data (Tamò-Larrieux, 2018).

2.3.1.4. Accuracy

Personal data must remain *accurate and, where necessary, kept up to date* (Art. 5 Par. 1 GDPR). Controllers are bound to erase or amend inaccurate personal data without delay. Precisely, the regulation declares that controllers must perform all reasonable efforts to *ensure that personal data that are inaccurate [...] are erased or rectified without delay*.

2.3.1.5. Storage Limitation

Personal data must be *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed* (Art. 5 Par. 1 GDPR). Politou, Michota, Alepis, Pocs, and Patsakis (2018) hence reason that modern systems which process and store personal data should guarantee they do not keep data in the backups for more than it is necessary.

2.3.1.6. Integrity and Confidentiality

Controllers are expected to develop appropriate safeguards and protect personal data against unlawful access, data breaches, data losses or leaks (Wachter, 2018). Likewise, Art. 5 Par. 1 GDPR mentions that personal data *should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*.

2.3.2. Legal Justifications

Art. 6 GDPR establishes six legal justifications for the processing of personal data. The next subsections present these justifications. The regulation renders the processing unlawful unless at least one of the six legal bases are applicable.

2.3.2.1. Consent

Art. 6 Par. 1 GDPR mentions data subjects may consent to the processing of their personal data for one or more specific purposes. Art. 7 Par. 1 GDPR adds that the controller shall be able to demonstrate that data subjects have provided their consent. Furthermore, Art. 7 Par. 3 GDPR declares that data subjects possess the right to withdraw their consent at any time and that the withdrawal should be as easy to as to give consent.

2.3.2.2. Contract

Processing is considered lawful if *necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract* (Art. 6 Par. 1 GDPR).

2.3.2.3. Legal Obligation

Processing is also allowed if *necessary for compliance with a legal obligation to which the controller is subject* (Art. 6 Par. 1 GDPR).

2.3.2.4. Vital Interests

Art. 6 Par. 1 GDPR additionally considers the processing lawful if *necessary in order to protect the vital interests of the data subject or of another natural person*.

2.3.2.5. Public Task

Furthermore, processing is permitted if *necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller* (Art. 6 Par. 1 GDPR).

2.3.2.6. Legitimate Interests

The Information Commissioner's Office (2018b) mentions that legitimate interests is the most flexible of the six legal justifications since it does not restrict its scope and can therefore allow controllers to rely on it under many different circumstances. If the law does not require the processing, but the latter is still beneficial for data subjects, the controller may rely upon this basis as long as the potential impacts on data subjects are limited and the controller does not process personal data for any further reason.

2.3.3. Rights of Data Subjects

The regulation establishes six exclusive rights that data subjects can exercise, namely the right to access, rectification, erasure, restriction of processing, data portability and object. Although this chapter does not make an extensive reference, Art. 22 GDPR challenges the practice of profiling and prohibits data controllers from making decisions concerning data subjects solely via automated means. Besides, controllers are responsible for communicating with the data subjects transparently and responding to the requests of the latter the earliest.

2.3.3.1. Transparent Information

Controllers should use *clear and plain language* and in a *concise, transparent, intelligible and easily accessible form* when communicating with data subjects (Art. 12 Par. 1 GDPR). Art. 12 Par. 2 GDPR delegates the controller to facilitate the requests of data subjects under Art. 15 GDPR to Art. 22 GDPR.

2.3.3.2. Right of Access

Wachter (2017) associates the right of access with the principle of transparency. The former lets data subjects request information regarding the processing of their personal data and also obtain a copy of their processed data.

Specifically, Art. 15 Par. 1 GDPR decrees that data subjects can *receive confirmation* as to whether or not the controller processes their personal data. If that is the case, they can request access to the personal data and the following information:

- The purposes behind the processing of personal data;
- The *categories of personal data* involved;
- The recipients of personal data, including recipients in *third countries or international organisations*;
- The estimated storage period or at least the criteria used to determine that period;
- The occurrence of the rights to rectification, erasure, restriction of processing, and object.
- The right to complain to the respective supervisory authority;
- If personal data are not collected from the data subject, any available information regarding their source;
- The existence, importance and expected influence of *automated decision-making* methods, including profiling.

Art. 15 Par. 3 GDPR further mentions that the controller *shall provide a copy of the personal data undergoing processing*, therefore enabling data subjects to receive a copy of the processed data (Wachter, 2017).

2.3.3.3. Right to Rectification

Data subjects may request the immediate correction of inaccurate personal data concerning them. The right to rectification may amend or restrict adverse effects on the rights and freedoms of data subjects (Voigt & von dem Bussche, 2017). Art. 16 GDPR empowers data subjects with the right to have *incomplete personal data completed*, including by *means of providing a supplementary statement*.

2.3.3.4. Right to Erasure

Mittal (2017) says that many have debated the right to be forgotten because of the Google Spain decision. The regulation now incorporates this right as the right to erasure. Data subjects can request the erasure of personal data concerning them without excessive delay, and data controllers are required to fulfill this obligation if specific conditions apply (Art. 17 Par. 1 GDPR).

2.3.3.5. Right to Restriction of Processing

Art. 18 GDPR allows the data subject to request the restriction of processing of their personal data as long as relevant conditions, established within the same article, apply.

2.3.3.6. Right to Data Portability

Art. 20 GDPR grants data subjects with the right to receive their personal data in a *structured, commonly used and machine-readable format*. Moreover, they are entitled to transmit those personal data to another controller as they see fit. Hert, Papakonstantinou, Malgieri, Beslay, and Sanchez (2017) reason that the right to data portability is vital towards the empowerment of data subjects and suggest it supports the concept for granting data subjects the default ownership of their personal data.

2.3.3.7. Right to Object

Art. 21 GDPR sets three conditions for enabling data subjects to exercise their right to object. If any of the following circumstances is substantial, the controller must stop processing the personal data belonging to the respective data subject:

- On grounds relating to the *particular situation* of the data subject;
- Personal data are processed for *direct marketing purposes*; or
- Personal data are processed for *research or statistical purposes*.

2.4. Summary

This chapter highlights six essential data processing principles and another six legal bases that the regulation provides for making the processing lawful. The lawmakers expect controllers to provide data subjects with particular information, implement sufficient mechanisms to safeguard personal data right from the start and process personal data with the highest privacy protection and, where applicable, honor all six fundamental rights concerning data subjects. Furthermore, both controllers and processors must maintain records of processing activities under their responsibility and implement appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data. If a personal data breach takes place, the controller should notify the competent supervisory authority as soon as possible and, in certain circumstances, the data subjects. Last but not least, in some cases, the controller is expected to perform a DPIA and designate a DPO which both help ensure the alignment of processing activities with the regulation as well as the reinforced security of personal data.

The following table summarises the fundamental aspects of the regulation that this chapter briefly discusses. Moreover, it correlates the respective articles with their titles and short descriptions. The contents of the table are useful for the subsequent interpretation of the requirements concerning the assessment model and to-be-developed system.

Table 2.1.: Overview and Description of Examined GDPR Articles

Art.	Title	Description
5	Principles relating to processing of personal data	The regulation sets six essential principles that are associated with every processing activity.
6	Lawfulness of processing	The regulation establishes six legal bases for rendering the processing lawful.
13	Information to be provided where personal data are collected from the data subject	The regulation requires controllers to provide data subjects with particular information wherever they obtain personal data from the data subject or another source.
14	Information to be provided where personal data have not been obtained from the data subject	
15	Right of access by the data subject	The regulation empowers data subjects with six fundamental rights related to the processing of their personal data.
16	Right to rectification	
17	Right to erasure ('right to be forgotten')	
18	Right to restriction of processing	
20	Right to data portability	
21	Right to object	
25	Data protection by design and by default	The regulation expects controllers to implement technical and organisational measures to safeguard personal data right from the start and to process personal data with the highest privacy protection.
30	Records of processing activities	The regulation directs that controllers maintain records of processing activities under their responsibility.
32	Security of processing	The regulation demands that controllers and processors implement appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data.

33	Notification of a personal data breach to the supervisory authority	In the case of a personal data breach, the regulation expects controllers to notify the respective supervisory authority and, in certain circumstances, the data subjects.
34	Communication of a personal data breach to the data subject	
35	Data protection impact assessment	When processing endangers the rights and freedoms of data subjects, the regulation requires controllers to conduct an assessment.
37	Designation of the data protection officer	The regulation requires the controller and the processor to designate a data protection officer, in certain circumstances.

Figure 2.1 meanwhile provides an accessible breakdown of the examined organisational and processing requirements which derive from the articles as mentioned earlier. This visualised breakdown can be useful for the subsequent analysis of and design of the envisioned system.

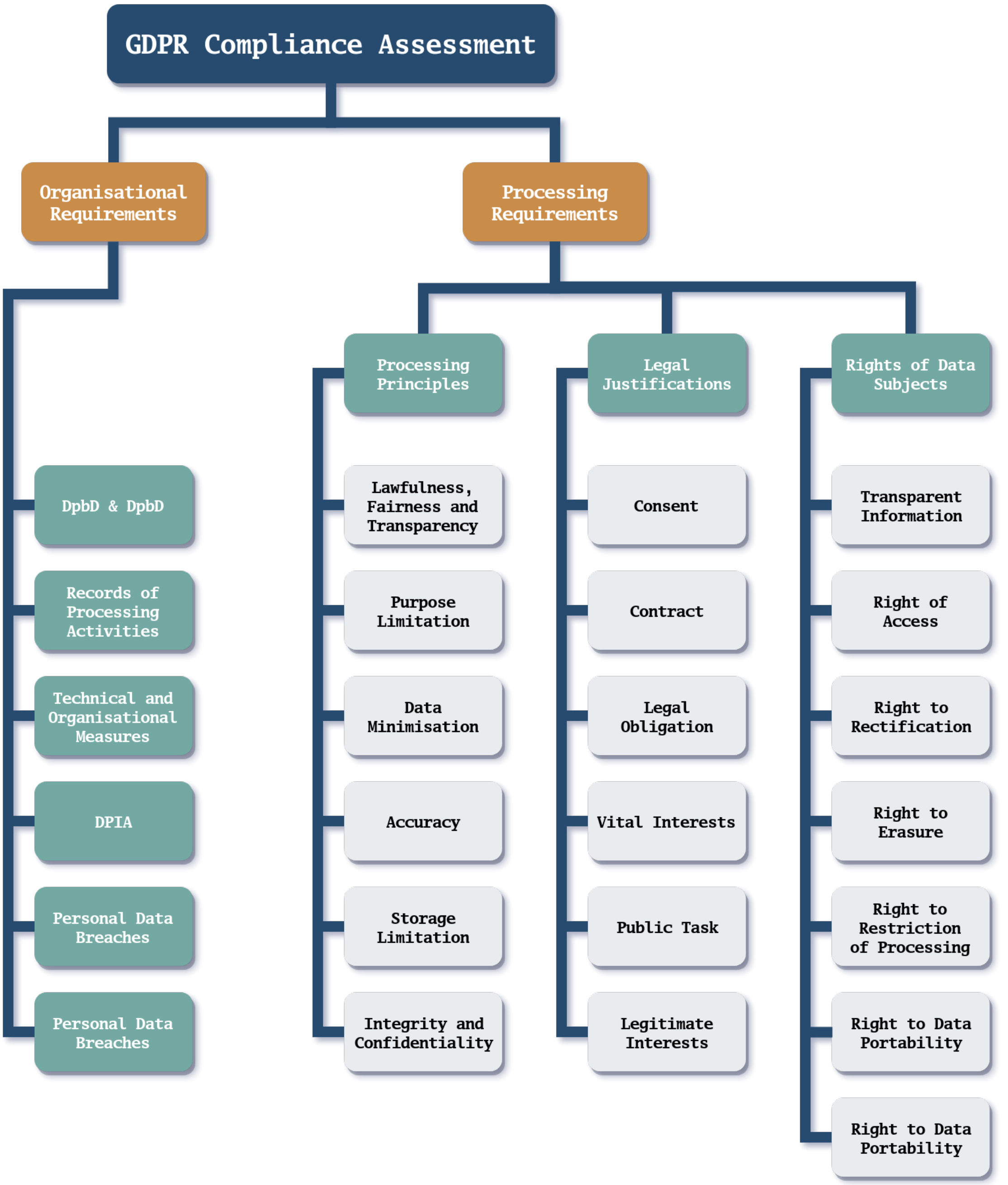


Figure 2.1.: Breakdown of the Examined Organisational and Processing Requirements

3. Compliance Assessment

3.1. Methodology

The conceptualisation of the evaluation model and the subsequent development of a system which assesses the compliance of an individual or SME with the complex requirements of the regulation is plausibly a challenging responsibility. Plus, several significant restrictions and limitations apply which the fourth section of the first chapter of this document describes in more detail.

It is reasonable that individuals and SMEs who process personal data can be affected by the articles and concepts of the regulation that the last section of the previous chapter summarises. For that purpose, the primary function of the system is to estimate the compliance with said articles and concepts.

This thesis splits the examined requirements of the regulation into organisational requirements and processing requirements. Thus, the system needs to determine the compliance of an organisation with both types of requirements. The organisational requirements merely apply to the organisation as a whole, while processing requirements are targeting each processing operation.

As a further matter, the GDPR often requires controllers to perform a DPIA. The conducting of such an assessment is mandatory when data processing operations may impose a high risk to the rights and freedoms of data subjects. Contrarily, individuals and SMEs may lack the expertise and resources to fulfil this obligation. Thus, the secondary function of the system is to support the conducting of DPIAs.

In order to evaluate the compliance of an organisation, the system needs to make decisions based on discrete circumstances. There are multiple paradigms to consider, such as sophisticated methods involving artificial intelligence and machine learning, although rules-based decision-making appears to be the simplest of all concerning the limitations and objectives of this diploma thesis. Implementations offering rule-based decision-making expect predictable arguments and depend on strictly predefined sets of rules to produce decisions. Mukundan, Ramani, Muthu Raman, Anjaneyulu, and Chandrasekar (2007) propose that, in rule-based systems, the knowledge about the domain under consideration should be made available in a machine-readable format, e.g. if-then rules. Therefore, the system is going to follow a comparable approach which seemingly bypasses the formulation of an intricate evaluation model.

This diploma thesis proposes an uncomplicated process for individuals and SMEs that need to assess and improve their compliance with the regulation. The intended user of the system initiates the process by submitting processing activities that reflect the processing operations performed by the entity they represent. As soon as the user finishes adding the processing activities, they can continue with the GDPR assessment which asks the user a few questions and meanwhile takes into account the previously submitted processing activities; the system checks the answers of the user and evaluates the compliance of the processing activities based on a predefined set of rules. If the conducting of a DPIA is deemed necessary, the user proceeds with such an assessment based on CNIL's PIA methodology. The flowchart in Figure 3.1 illustrates the proposed methodology described above.

The following two subsections focus on the analysis and design the system. The third subsection briefly describes the implementation of the system which takes place beyond this document. Finally, the fourth and final subsection outlines the evaluation of the system by a diverse set of experts and professionals.

3.2. Analysis

Kendall and Kendall (2013) suggest that analysts perform systems analysis and design to understand the requirements behind data input and flow, processing or transformation, and storage and the output of information in connection with a particular organisation or business. A thorough analysis is imperative as it encourages analysts to recognise and overcome obstacles and meanwhile perform improvements to support end-users.

The envisioned system is split into three central but separate subsystems. The first subsystem collects processing activities which count as records of processing activities under Art. 32 GDPR; different subsystems can also access previously-saved processing activities for carrying out assessments. The second subsystem is responsible for conducting GDPR Assessments, i.e., evaluating the alignment of an entity with the regulation. The third and last subsystem helps users perform DPIAs if deemed necessary by one or more of the three conditions set within Art. 35 Par. 3 GDPR.

3.2.1. Processing Activity

The Processing Activity subsystem, in essence, performs simplified data mappings tailored to the context of the GDPR. Organisations need to arrange and manage their processing activities before assessing their compliance with the regulation. This subsystem enables them to recognise what kind of data they collect, for which purposes they collect them, which entities have access to the corresponding data sets, and how

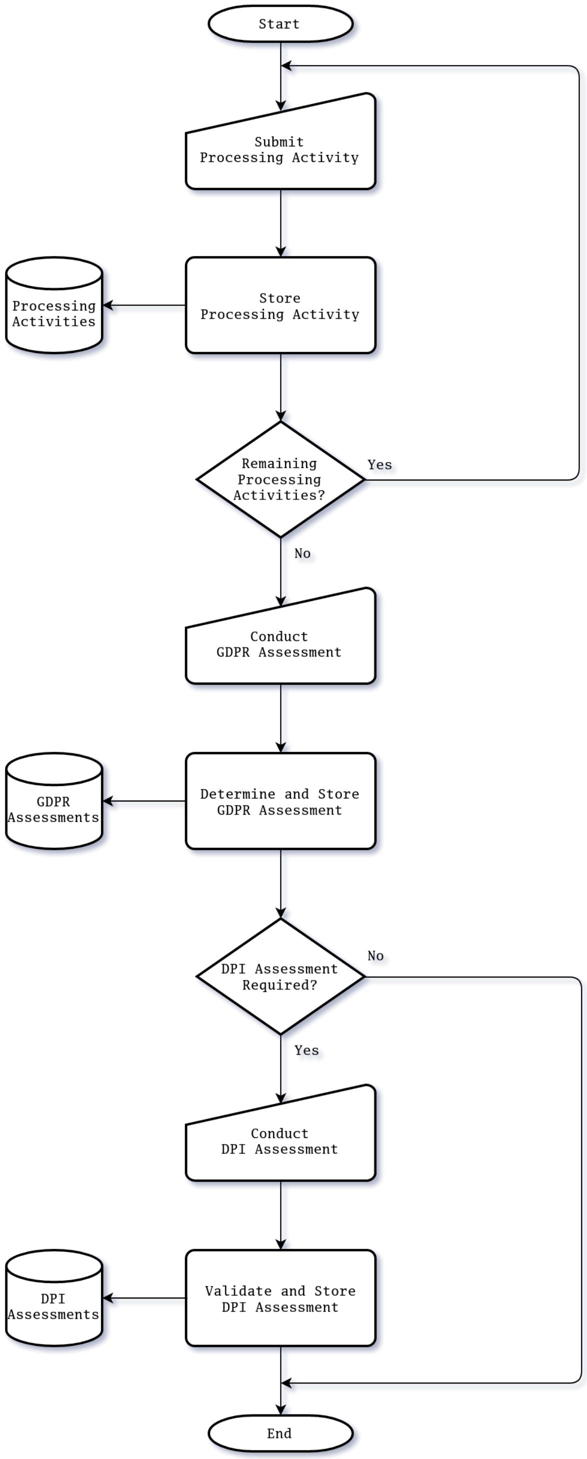

Start
Submit Processing Activity
Store Processing Activity
Processing Activities
Remaining Processing Activities?
Yes
No
Conduct GDPR Assessment
Determine and Store GDPR Assessment
GDPR Assessments
DPI Assessment Required?
No
Yes
Conduct DPI Assessment
Validate and Store DPI Assessment
DPI Assessments
End

Figure 3.1.: Flowchart Representing the Proposed Methodology

data flows through information systems. More importantly, it does so while keeping the regulation and its relevant articles in mind.

3.2.1.1. Essential Information

The subsystem begins with requesting the user to enter their full name and to designate their organisation name and job title. This information contributes towards providing a personalised user experience and is also useful for the future linking and categorisation of processing activities.

3.2.1.2. Summary

The subsystem continues with conceptualising the most mattering aspects of the examined processing activity. This knowledge helps the controller and the processor maintain up-to-date records of processing activities and can also serve as the basis for assessing the compliance of the organisation with the processing requirements of the regulation when conducting GDPR Assessments.

Processing Activity Name The subsystem asks the user to designate a friendly name for the engaged processing activity, i.e., a nickname used for identification and classification purposes.

Controller Name The subsystem asks the user to identify the corresponding controller or controllers. This information, among others, is required by Art. 30 Par. 1 GDPR.

Processor Name The subsystem asks the user to name the affiliated processor or processors. Likewise, this information is required by Art. 30 Par. 1 GDPR.

Processing Activity Description The subsystem asks the user to explain the purposes of the processing and provide a brief description of the implemented technical and organisational measures. If the user's organisation transfers personal data to recipients in third countries or international organisations, the subsystem requests the user to elaborate further. This information is also required by Art. 30 Par. 1 GDPR.

Storage Method The subsystem asks the user to specify the designated storage method for personal data. The user can choose among digital, physical, and the combination of both storage methods. The regulation does not strictly require this information.

However, it serves towards formulating the comprehensive overview of the involved processing activity.

- Digital
- Physical
- Digital and Physical

Data Type Likewise, the user needs to specify the type of data; they can either be personal data or special categories of personal data. Art. 4 Par. 1 GDPR and Art. 9 Par. 1 GDPR define personal data and the special categories of personal data respectively.

- Personal Data
- Special Categories of Personal Data

Legal Justification Art. 6 Par. 1 GDPR confirms six distinct legal justifications, under which processors are permitted to perform the processing. The subsystem asks the user to select one of the possible justifications. The user has the additional option to refrain from selecting the legal basis, by setting their response to 'None'.

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests
- None

Security Measures The subsystem asks the user to declare whether their organisation has implemented any technical and organisational measures which the regulation, under Art. 32 Par. 1 GDPR, considers to be necessary.

- The organisation has implemented all appropriate technical and organisational measures.
- The organisation has implemented some appropriate technical and organisational measures.
- The organisation has not implemented any technical and organisational measures.
- It is unknown whether the organisation has implemented any appropriate technical and organisational measures.

Processing Principles The subsystem asks the user to mention whether the existent processing activity complies with the six fundamental processing principles set in Art. 5 Par. 1 GDPR. As usual, the user may provide a negative or neutral response.

- The organisation upholds all six processing principles.
- The organisation upholds some processing principles.
- The organisation does not uphold any processing principle.
- It is unknown whether the organisation upholds any processing principle.

Data Subject Rights The regulation empowers data subjects with six fundamental rights, set in Art. 15 GDPR, Art. 16 GDPR, Art. 17 GDPR, Art. 18 GDPR, Art. 20 GDPR and Art. 21 GDPR. The previous chapter of this document discusses these rights of data subjects. Besides, there are Art. 8 GDPR and Art. 22 GDPR for the protection of minors and the protection of data subjects against automated decision-making respectively which this thesis does not address.

Deliberately, during this question, the system does not identify which articles of the regulation apply. Generally, organisations must comply with all perspectives of the regulation wherever applicable.

- The organisation helps data subjects exercise all of their rights wherever applicable.
- The organisation helps data subjects exercise some of their rights.
- The organisation does not help data subjects exercise their rights.
- It is unknown wherever the organisation helps data subjects exercise their rights.

3.2.2. GDPR Assessment

The GDPR Assessment subsystem is perhaps the most valuable and relevant subsystem because it identifies the compliance of an entity with the regulation and, if applicable, indicates the wrongdoings and suggests improvements. Specifically, this subsystem examines whether an entity meets the organisational requirements of the regulation based on predefined rules and also examines the previously submitted processing activities to determine compliance with the processing requirements. It does acknowledge every essential requirement appearing in Figure 2.1 of the previous chapter.

3.2.2.1. Essential Information

Similarly to the equivalent section of the previous subsystem, this subsystem starts by asking the user to enter their full name, and indicate their organisation and job title. This information purposes to ease the further categorisation and identification of the assessments.

Which of the following best describes the role of the organisation? This question means to determine the role of the organisation under assessment. An organisation can assume the role of the controller, the processor or the joint controller. Also, an organisation may assume the roles of the controller and the processor at the same time. Art. 4 GDPR provides these definitions.

- The organisation determines the purposes and means of data processing.
- The organisation processes data on behalf of another organisation.
- The organisation jointly determines the purposes and means of data processing with another organisation.
- The organisation both determines the purposes and means of data processing and processes data.

Does the organisation involve data subjects in the EU? The subsystem asks whether the organisation involves data subjects in the EU and therefore seeks to discover whether the territorial scope under Art. 3 GDPR applies. Note that the subsystem does not address the material scope which Art. 2 GDPR defines.

- The organisation processes personal data relating to data subjects in the EU.
- The organisation does not process personal data of EU residents.
- It is unknown whether the organisation processes personal data relating to data subjects in the EU.

3.2.2.2. Organisational Requirements

The organisational requirements are obligations that data controllers and, wherever applicable, processors must carefully consider throughout the planning of their entire operations. During this step, the subsystem asks the user six discrete questions and, based on the answers of the user, checks compliance with Art. 13 GDPR, Art. 14 GDPR, Art. 25 GDPR, Art. 30 GDPR, Art. 32 GDPR, Art. 33 GDPR, Art. 34 GDPR, and Art. 37 GDPR.

Has the organisation implemented appropriate technical and organisational measures? As aforementioned, Art. 32 GDPR expects controllers and processors to implement appropriate technical and organisational activities. Therefore, the user should report on the status of the organisation regarding this matter.

- The organisation has implemented appropriate technical and organisational measures for the safeguarding of personal data.

- The organisation has not implemented appropriate technical and organisational measures for the safeguarding of personal data.
- The unknown whether the organisation has implemented appropriate technical and organisational measures for the safeguarding of personal data.

Does the organisation maintain records of processing activities? Likewise, both controllers and processors should maintain records of processing activities. Art. 30 GDPR sets the maintenance of records of processing activities to be mandatory for both controllers and processors. The subsystem asks the user to verify whether these records exist.

- The organisation maintains records of processing activities.
- The organisation does not maintain records of processing activities.
- The unknown whether the organisation maintains records of processing activities.

Has the organisation published an easy-to-understand privacy policy? Art. 13 GDPR and Art. 14 GDPR require the controller to provide particular information to the data subject wherever the former obtains personal data from the data subject or another source. The privacy policy is an essential practice that explains how data controllers and processors handle personal data. They also inform data subjects about their rights and provide contact information.

- There is a publicly available privacy policy that explains data processing activities and guides data subjects through exercising their rights.
- There isn't such a document published anywhere.
- It is unknown whether the organisation has published an easy-to-understand privacy policy.

Does the organisation embrace data protection by design and by default? Art. 25 GDPR requires the controller to implement appropriate measures to protect personal data right from the start and to process personal data while offering the highest privacy protection. The user needs to specify if the organisation embraces these two principles.

- The organisation embraces data protection by design and by default in accordance with Art. 25 GDPR.
- The organisation does not embrace data protection by design and by default.
- It is unknown whether the organisation embraces data protection by design and by default.

Has the organisation established a procedure in the event of a data breach? If a personal data breach occurs, controllers should usually inform the responsible supervisory authority within 72 hours from the moment they have acknowledged the breach. Art. 33 GDPR focuses and elaborates on this requirement. According to Art. 34 GDPR, controllers may also need to notify the data subjects affected by the breach if there is a high risk involving their rights and freedoms. Therefore, it is crucial that organisations are well-prepared for such occasions. This question expects to estimate the readiness of the organisation concerning personal data breaches.

- The organisation has established a procedure in the event of a data breach.
- The organisation has not established a procedure in the event of a data breach.
- It is unknown whether the organisation has established a procedure in the event of a data breach.

Has the organisation appointed a data protection officer? Under particular circumstances, controllers and processors must appoint a data protection officer who is responsible for ensuring the compliance of the organisation and its processing duties with the regulation. Art. 37 GDPR illustrates these circumstances, while Art. 38 GDPR and Art. 39 GDPR analyse the position and the tasks of the DPO respectively.

- The organisation has appointed a data protection officer.
- The organisation does not need to appoint a data protection officer.
- The organisation has not appointed a data protection officer.
- It is unknown whether the organisation needs to appoint a data protection officer.
- It is unknown whether the organisation has appointed a data protection officer.

3.2.2.3. Processing Requirements

The previous chapter addresses the processing requirements of the regulation alongside the organisational requirements. Substantially, the processing requirements affect the specific processing activities of an organisation, whereas the organisational requirements concentrate on the generic business processes of an organisation. The subsystem is, therefore, going to investigate the processing activities in order to determine the organisation's overall compliance with the GDPR's processing requirements.

During this step, the user may choose as many processing activities as they have submitted earlier in the previous subsystem. If the user does not select any processing activity, the subsystem is still able to conduct the assessment; however, in this instance, the subsystem only considers the organisational requirements and does not produce a comprehensive assessment. Furthermore, if the user has not submitted any processing activities before running the assessment, the subsystem suggests them to do so yet is still able to carry an inadequate assessment as explained right above. It is up to the user to determine whether to include the processing activities and hence consider the processing requirements.

3.2.2.4. Validation

As soon as the user submits the assessment, the subsystem performs every necessary validation against an extensive set of predefined rules. Then, the subsystem stores the assessment under the user's userspace and displays informational messages for the answers the user provides to each of the previous questions. If the user includes processing activities in the assessment, the subsystem checks every processing activity against another set of pre-established rules.

The subsystem assesses with strict criteria. An assessment is labelled Compliant provided the organisation is fully complying with the regulation. If there are up to four (4) conflicts with the requirements of the regulation, the organisation is considered Semi-Compliant. If there are five (5) conflicts or more, the organisation is considered Non-Compliant. The subsystem always provides the user with clear indications and highlights the elements of the assessment which pass and the ones which fail. It also presents informational messages which connect to the corresponding articles of the regulation.

Has your organisation implemented appropriate technical and organisational measures? The first message the subsystem displays refers to the implementation of appropriate technical and organisational measures. The box containing the informational message is coloured green if the user's answer is correct. If the answer is wrong, the box is coloured red.

> *Art. 32 Par. 1 GDPR expects controllers and processors to implement appropriate technical and organisational measures to ensure the continuous protection of personal data.*

Does your organisation maintain records of processing activities? The second informational message concerns the maintenance of records of processing activities. It is apparent that every message connects with the specific articles of the regulation. The user can consult the original legal text for further knowledge.

> *Art. 30 Par. 1 GDPR stresses the necessity of maintaining records of processing activities which burdens both controllers and processors.*

Has your organisation published an easy-to-understand privacy policy? The subsystem continues with displaying another box, this time for the obligation to provide information to the data subject under Art. 13 GDPR and Art. 14 GDPR. As stated before, the subsystem correlates these requirements with the presence of an easy-to-understand privacy policy.

> *Art. 13 and 14 GDPR require controllers to provide data subjects with particular information wherever they obtain personal data from the data subject or from another source.*

Does your organisation embrace data protection by design and by default? Data protection by design and by default is reasonably one of the most wide-spread commitments under the GDPR. Likewise, the subsystem displays another informational message about this segment.

> *Art. 25 GDPR expects controllers to safeguard personal data right from the start and to process personal data with the highest privacy protection.*

Has your organisation established a procedure in the event of a data breach? While the regulation, strictly speaking, does not command controllers to establish procedures for personal data breaches, organisations still have clear responsibilities under Art. 33 GDPR and Art. 34 GDPR. Consequently, procedures are indeed meant to help organisations overcome unforeseen consequences.

> *In the case of a personal data breach, Art. 33 GDPR and Art. 34 GDPR expect controllers to notify the respective supervisory authority and, in certain circumstances, the data subjects.*

Has your organisation appointed a data protection officer (DPO)? It is noteworthy that the subsystem does not investigate whether the organisation must designate a DPO but relies entirely on the user's answer. If, for example, the user claims their organisation does not need to appoint a DPO, the subsystem will regard the user's answer as valid without conducting further analyses. The subsystem's set of predefined rules may be refreshed in the future to accommodate this sort of investigations.

> *Art. 37 Par. 1 GDPR requires the controller and the processor to designate a data protection officer, in certain circumstances.*

Legal Justification The subsystem then iterates through all the processing activities selected previously by the user. The organisation must specify an actual legal justification, implement adequate technical and organisational measures, honour every processing principle and every right of data subjects wherever applicable. If the subsystem determines that one or more factors are ineffectual, it displays informational messages similarly with the organisational requirements.

The first requirement is the legal justification. The regulation specifies six distinct legal bases, under Art. 6 Par. 1, for rendering the processing lawful.

> *Art. 6 Par. 1 GDPR establishes six legal bases for rendering the processing lawful.*

Security Measures Technical and organisational measures fall under both organisational and processing requirements. The subsystem takes their occurrence into account for every separate processing activity. In reality, organisations may choose to utilise security mechanisms only for certain processing activities while other processing activities may be left unprotected. Therefore, it is substantial to evaluate every processing activity.

> *Art. 32 Par. 1 GDPR expects controllers and processors to implement appropriate technical and organisatinal measures to ensure the confidentiality, integrity, and availability of processing systems.*

Processing Principles Every processing activity must conform to the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. Art. 5 GDPR describes those requirements with expanded detail.

> *Art. 5 Par. 1 GDPR highlights six principles relating to the processing of personal data. Art. 5 Par. 2 GDPR holds controllers accountable for compliance with these principles.*

Data Subject Rights Art. 15 GDPR, Art. 16 GDPR, Art. 17 GDPR, Art. 18 GDPR, Art. 20 GDPR and Art. 21 GDPR introduce the right of access, the right to rectification, the right to erasure, the right to the restriction of processing, the right to data portability, and the right to object sequentially.

> *Art. 15 GDPR, Art. 16 GDPR, Art. 17 GDPR, Art. 18 GDPR, Art. 20 GDPR and Art. 21 GDPR introduce six fundamental rights of data subjects. Controllers must honour these rights, where applicable.*

3.2.3. DPI Assessment

The third and final subsystem supports users to perform DPIAs wherever required by the regulation. It relies profoundly upon the CNIL's PIA methodology which spans across four main stages. CNIL also provides an open-source PIA tool which complements their methodology; the subsystem draws some inspiration from the CNIL's implementation but strives to make the process easier and more straightforward.

3.2.3.1. Context

The study of the context is the first step when performing the PIA. According to CNIL's official guide, this measure aims to provide an overview of the engaged personal data processing operations. Besides, the study of the context helps with the preparation and classification of the process.

Data Processing The user starts with naming the engaged data processing activity, then includes a short description, and explains its essential processing purposes.

Responsibilities Then, the user continues with specifying any associated data controllers and data processors, as well as with listing their respective responsibilities.

Relevant Standards The organisation may possess codes of conduct and certifications which are relevant to the engaged processing activity. The user may designate these standards.

Data Involved The user proceeds with describing what kind of data is collected and processed, then defines the respective storage periods, and specifies which persons hold access.

Data Life Cycle Then, the user explains the fundamental aspects of the process and describes how data flows through information systems.

Data Supporting Assets Last but not least, the user may include any relevant, to the engaged processing activity, data supporting assets, e.g., operating systems, applications and configurations.

3.2.3.2. Fundamental Principles

The study of the fundamental principles behind the processing frames the second step of the methodology. Users should elaborate on the choices their organisation has made to comply with the particular requirements of the regulation. Meanwhile, the PIA seeks to evaluate the actions the organisation has performed for honouring the rights of the data subjects.

Explicitness and Legitimacy The user starts by justifying why the processing purposes are specified, explicit and legitimate.

Lawfulness Afterwards, the user provides the legal basis for the lawful processing of personal data.

Data Minimisation The user continues by describing how data are adequate, relevant and limited to what is necessary for the purposes for which they are processed.

Data Accuracy The user then explains how data remain accurate and up-to-date.

Storage Duration The user also needs to determine the estimated storage duration(s) of the data involved.

Communication Controllers are expected to communicate with the data subjects. The user needs to specify what kind of information the data subjects receive and via which means of communication.

Access and Portability The regulation establishes the rights of data subjects. The user mentions whether and how data subjects can exercise their right of access and their right to portability.

Rectification and Erasure Then, the user explains whether and how data subjects can exercise their right to rectification and their right to erasure.

Restriction and Object Moreover, the user describes whether and how data subjects can exercise their right to restriction and their right to object.

Contract Governance The user further elaborates on the responsibilities of the processor or processors and the existence of relevant standards.

International Data Transfer If the organisation performs international data transfers, the user needs to name the recipient countries and to describe the corresponding data protection levels and provisions.

Additional Information Finally, the user can provide any additional information they deem important.

3.2.3.3. Risks

Wright and Hert (2012) suggest that any PIA methodology should depend on a risk assessment and management process. They also acknowledge that such methodology can fit into the organisation's overall risk management strategy.

An organisation that processes personal data encompasses various risks and directing a PIA can ease the identification, avoidance or mitigation of those risks. The third step of the CNIL's PIA methodology expectedly examines the risks related to the security of personal data, and this section of the subsystem allows users to recognise and analyse those risks.

Security Measures The user mentions which security measures, also known as security controls, the organisation has already implemented. Admittedly, the current version of the subsystem does not make the most optimal use of this knowledge. Future versions may offer automated suggestions of security controls and also render this information helpful through the validation step.

Illegitimate Access to Data, Unwanted Modification of Data and Data Disappearance The assessment considers three separate scenarios, particularly the illegitimate access to data, the unwanted modification of data and data disappearance. The user first describes the potential impact this scenario can impose upon data subjects, then designates the main threats associated with these scenarios and defines the connected risk sources.

Additionally, the user determines the potential severity and likelihood for every scenario. In other words, each scenario's anticipated impact and probability of occurrence. The subsystem uses this information to produce and present the risk matrix during the validation step. Every severity and likelihood applies one of the following attributes:

- Undefined
- Negligible
- Limited
- Important
- Maximum

3.2.3.4. Validation

The execution of the methodology completes with the validation of the assessment. Unlike the GDPR Assessment subsystem, the DPI Assessment subsystem cannot determine whether the investigated data processing operations comply with the requirements of the regulation. This particular subsystem merely assists the user with assessing DPI Assessments on their own.

During the validation step, the subsystem displays a risk matrix which determines the level of risk concerning the illegitimate access to data, the unwanted modification of data and data disappearance scenarios. The risk matrix renders a visual representation of the associated risks and can subsequently assist the user with making appropriate decisions. Based on the aforementioned visual representation, the user recommends additional measures to minimise the risks and also includes the opinion of the organisation's designated DPO to be taken into account. The validation concludes with the user either approving the assessment or rejecting it.

Additional Measures The user suggests additional technical and organisational measures for future implementation.

DPO's Opinion The user also includes the opinion of the organisation's designated Data Protection Officer.

3.3. Design

3.3.1. Use-Case Specifications

Rumbaugh, Jacobson, and Booch (1999) communicate that use-cases describe a set of sequences where elements outside the system, which are called actors, interact with the system itself. Analysts outline use-cases to visualise, define, assemble and document the intended behaviour of the system undergoing requirements analysis. Large and more complicated systems regularly incorporate use-cases that are contained within other use-cases and also use-cases that extend the operation of other central use-cases.

This subsection illustrates the primary use-cases which correspond to the system. Figure 3.2 concentrates and emphasises the critical use-cases. Aside from the three subsystems mentioned beforehand, the system includes an e-mail based authentication mechanism which in turn involves several operations including user registration, user login, and user logout. The system itself must also be compliant with the regulation, and therefore it is necessary to acknowledge additional use-cases that satisfy such requirements. Use-case specifications are illustrated using the basic use-case template of Cockburn (1998).

Non-functional requirements supplement each use-case specification. While functional requirements define, as their name suggests, the functions of the system, non-functional requirements tend to describe the technical constraints and attributes that belong to the system. Leffingwell and Widrig (2003) split non-functional requirements into four discrete categories and associate them with the usability, reliability, performance and supportability of the system. The resulting non-functional requirements of the system embrace the same pattern and classification paradigm, with an extension of non-functional requirements covering security.

3.3.1.1. User Registration

Registration is compulsory for everyone before they can practice the system to its full potential. The registration process is designed to be straightforward and to require minimum user interaction. The prospective user starts by completing the registration form within the signup page, and then the system validates the form's contents before proceeding with the actual user registration. Every user account entry in the database contains the full name of the user in order to sign the processing activities and assessments, the e-mail address to ensure that legitimate users sign-up for the system and also to support password resets, the username to associate the user with processing activities and assessments, and the password to authenticate the user.

Table 3.1.: Use Case #1: User Registration

Use Case #1	User Registration	
Goal in Context	Enable the prospective user to register their user account.	
Scope & Level	Authentication Subsystem, Primary Task	
Preconditions	The prospective user accesses the system via the web.	
Success End Condition	The prospective user registers their user account.	
Failed End Condition	The prospective user does not register their user account.	
Primary Actor	Prospective User	
Description	**Step**	**Action**
	1	The prospective user requests the 'signup' page.
	2	The system presents the 'signup' page to the prospective user.
	3	The prospective user fills the form contained within the 'signup' page.
	4	The system validates the contents of the form.

	5	The system creates the user account, redirects the user to the 'signin' page and displays a success message.
Extensions	**Step**	**Branching Action**
	4a	The validation of the contents of the form is unsuccessful.
		4a1. The system redirects the prospective user back to the 'signup' page and notifies the prospective user of the unsuccessful validation.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.2.: Use Case #1: Non-Functional Requirements

ID	**Category**	**Description**
NF1.1	Usability	The system should provide practical and unambiguous information to the user wherever registration is unsuccessful.
NF1.2	Usability	The system should preserve the previous contents of the registration form, except for user passwords, if the registration form does not pass the required validation checks.
NF1.3	Performance	Upon successful validation of the registration form, the system should perform every subsequent transaction promptly.
NF1.4	Security	The system should protect requests against CSRF exploits and related attacks.
NF1.5	Security	The system should implement sufficient mechanisms to encrypt the registration data submitted over the network.
NF1.6	Security	The system should hash and salt the user password before storing it to the database.
NF1.7	Supportability	The registration form should support the future implementation of CAPTCHA challenges.

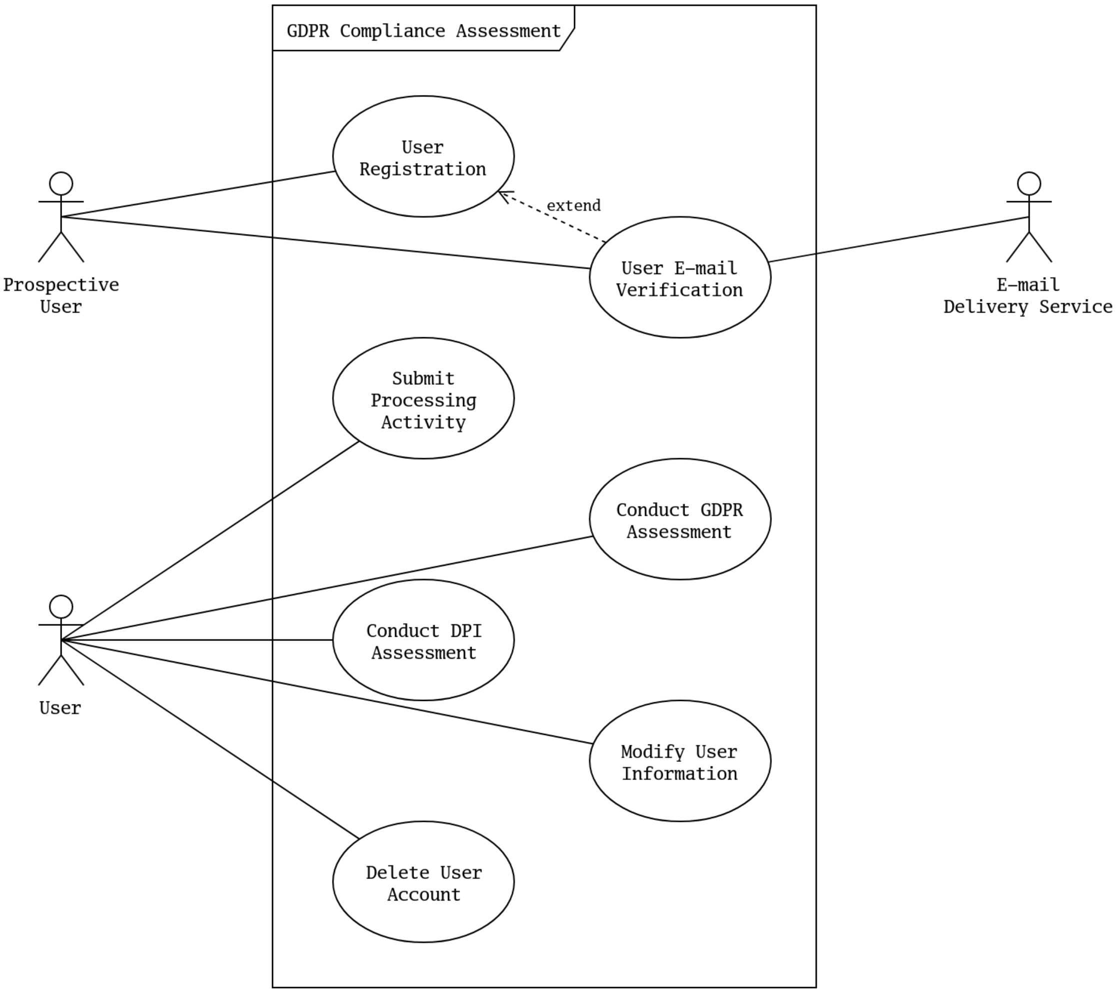


Figure 3.2.: Use-Case Diagram Emphasising the Critical Use-Cases

3.3.1.2. User E-mail Verification

E-mail address verification is mandatory before users can successfully log into the system with their user account. This requirement helps prevent the enrollment of spam accounts and also enables legitimate users to perform password resets if needed. Upon successful registration, the system sends an e-mail to the e-mail address the user designates during the sign-up process. The verification e-mail message includes a pseudorandomly-generated verification token. The user accesses their mailbox, opens the e-mail message and selects the verification URL that has the verification token embedded within. The browser redirects the user back to the system where the system validates the verification token and verifies the user account.

Table 3.3.: Use Case #2: User E-mail Verification

Use Case #2	User E-mail Verification	
Goal in Context	Verify the e-mail address that belongs to the user.	
Scope & Level	Authentication Subsystem, Subfunction	
Preconditions	The user registers their user account.	
Success End Condition	The user verifies their e-mail address.	
Failed End Condition	The user does not verify their e-mail address.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The system sends a verification e-mail message to the e-mail address the user designates during registration.
	2	The user opens the e-mail message and selects the verification URL that has the verification token embedded within.
	3	The browser redirects the user back to the system.
	4	The system validates the verification URL.
	5	The system verifies the user account, redirects the user to the 'signin' page and displays a success message.
Extensions	**Step**	**Branching Action**
	4a	The validation of the verification token is unsuccessful.
		4a1. The system redirects the user back to the 'signin' page and notifies the user of the unsuccessful validation.
Sub-Variations	**Step**	**Branching Action**

	N/A	N/A

Table 3.4.: Use Case #2: Non-Functional Requirements

ID	Category	Description
NF2.1	Usability	The system should provide practical and unambiguous information to the user wherever e-mail verification is unsuccessful.
NF2.2	Usability	The verification e-mail should contain minimum information besides the verification URL.
NF2.3	Usability	The verification e-mail should also contain an alternative version of the same verification URL in plain text, in case the user's e-mail client does not render HTML.
NF2.4	Performance	Upon successful validation of the verification token, the system should perform every subsequent transaction promptly.
NF5.5	Security	The system should ensure that verification e-mails follow enforced SPF, DKIM and DMARC policies and are therefore not mistakenly classified as phishing e-mails.

3.3.1.3. User Login

The system supports e-mail based user authentication. Users should be able to log into the system using their credentials and authentication should be uncomplicated and based on the something-you-know factor. Therefore, the combination of the username or user e-mail address and password should be sufficient for this kind of purpose. In the future, users may also be able to use their usernames, instead of their e-mail addresses, to log-in. Integration with existing authentication systems can also be examined and considered.

Table 3.5.: Use Case #3: User Login

Use Case #3	User Login
Goal in Context	Enable the user to log into the system.
Scope & Level	Authentication Subsystem, Primary Task
Preconditions	The user validates their e-mail address.
Success End Condition	The user logs into the system.

Failed End Condition	The user does not log into the system.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the ‘signin’ page.
	2	The system presents the ‘signin’ page to the user.
	3	The user fills the form contained within the ‘signin’ page.
	4	The system validates the contents of the form.
	5	The system additionally checks whether the user has verified their account.
	6	The system proceeds with the login, and redirects the user to the ‘dashboard’ page.
Extensions	**Step**	**Branching Action**
	4a	The validation of the contents of the form is unsuccessful.
		4a1. The system redirects the user back to the ‘signin’ page and notifies the user of the unsuccessful validation.
	5a	The user has not verified the account.
		5a1. The system redirects the user back to the ‘signin’ page and notifies the user of the unsuccessful verification.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.6.: Use Case #3: Non-Functional Requirements

ID	Category	Description
NF3.1	Usability	The system should provide practical and unambiguous information to the user wherever login is unsuccessful.
NF3.2	Usability	The system should preserve the previous contents of the login form, except for the user password, if the login form does not pass the required validation checks.
NF3.3	Performance	Upon successful validation of the login form, the system should perform every subsequent transaction promptly.

NF3.4	Security	The system should protect requests against CSRF exploits and related attacks.
NF3.5	Security	The system should implement sufficient mechanisms to encrypt the login data submitted over the network.
NF3.6	Security	The system should log every successful and unsuccessful login attempt.
NF3.7	Supportability	The login form should support the future implementation of CAPTCHA challenges.

3.3.1.4. User Log Out

The system supports manual user logout. Users should be able to log out whenever they wish. Manual user logout is highly important for privacy reasons and also lets users sign into the system with another user account while on the same web browser. The user first requests the log-out; then the system de-authenticates the user and redirects them to the index page.

Table 3.7.: Use Case #4: User Account Log Out

Use Case #4	User Log Out	
Goal in Context	Enable the user to log out of the system.	
Scope & Level	Authentication Subsystem, Subfunction	
Preconditions	The user logs into the system.	
Success End Condition	The user logs out of the system.	
Failed End Condition	The user does not log out of the system.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the ‘signout’ page.
	2	The system proceeds with the logout, and redirects the user to the ‘home’ page.
Extensions	**Step**	**Branching Action**
	1a	The user is not logged into the system when requesting the ‘signout’ page.
		1a1. The system does not consider the request.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.8.: Use Case #4: Non-Functional Requirements

ID	Category	Description
NF4.1	Usability	The system should provide the user with easy and visible access to logout functionality.
NF4.2	Performance	Upon successful request of the logout page, the system should perform every subsequent transaction promptly.
NF4.3	Security	The system should automatically perform the logout after an administratively-configurable maximum period regardless of user activity.
NF4.4	Security	The system should guarantee that the particular session of the user is invalidated when the user logs out.

3.3.1.5. Reset User Password

The system supports password resets. If users forget their passwords, they should be able to reset them. The password recovery process helps prevent users from being permanently locked out of their userspace, and subsequently the system. The user visits the, designed explicitly for that purpose, recovery page and designates their e-mail address. Then, the system sends an e-mail message, which includes one pseudo-randomly generated password reset token, to the verified e-mail address of the user who requests the password reset. The user selects the reset URL, and the browser redirects them to back the system where the latter validates the password reset token and presents a password reset form to the user. The user enters their new desired password, submits the form and the system implements the change.

Table 3.9.: Use Case #5: Reset User Password

Use Case #5	Reset User Password	
Goal in Context	Enable the user to reset their password.	
Scope & Level	Authentication Subsystem, Subfunction	
Preconditions	The user registers their user account.	
Success End Condition	The user resets their password.	
Failed End Condition	The user does not reset their password.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the ‘forgotpassword’ page.
	2	The system presents the ‘forgotpassword’ page to the user.

	3	The user fills the form contained within the ‘forgotpassword’ page.
	4	The system validates the contents of the form.
	5	The system sends a password reset e-mail message to the e-mail address the user designates during step #3.
	6	The user opens the e-mail message and selects the password reset URL that has the password reset token embedded within.
	7	The browser redirects the user back to the system.
	8	The system validates the password reset URL.
	9	The system presents the ‘resetpassword’ page to the user.
	10	The user fills the form contained within the ‘resetpassword’ page.
	11	The system validates the contents of the form.
	12	The system changes the user’s password, redirects the user to the ‘signin’ page and displays a success message.
Extensions	**Step**	**Branching Action**
	8a	The validation of the password reset token is unsuccessful.
		8a1. The system redirects the user back to the ‘forgotpassword’ page and notifies the user of the unsuccessful validation.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.10.: Use Case #5: Non-Functional Requirements

ID	Category	Description
NF5.1	Usability	The password reset e-mail should contain minimum information besides the password reset URL.
NF5.2	Usability	The password reset e-mail should also contain an alternative version of the same password reset URL in plain text, in case the user’s e-mail client does not render HTML.

NF5.3	Usability	The system should provide practical and unambiguous information to the user wherever password reset is unsuccessful.
NF5.4	Performance	Upon successful validation of the password reset token, the system should perform every subsequent transaction promptly.
NF5.5	Security	The system should use a well-implemented password recovery mechanism that utilises pseudorandomly generated tokens.
NF5.6	Security	The system should prevent malicious attackers from abusing the password reset mechanism to lock out legitimate users.
NF5.7	Security	The system should ensure that password reset e-mails follow enforced SPF, DKIM and DMARC policies and are therefore not mistakenly classified as phishing e-mails.

3.3.1.6. Modify User Information

The system enables users to change their personal information. This process embraces the right to rectification under Art. 16 GDPR. The user visits the account settings page which includes a prefilled form with their existing information. Next, the user can change any pieces of information and submit the form. Eventually, the system validates the new contents of the form and updates the database entries accordingly.

Table 3.11.: Use Case #6: Modify User Information

Use Case #6	Modify User Information	
Goal in Context	Enable the user to modify their personal information.	
Scope & Level	Account Settings Subsystem, Primary Task	
Preconditions	The user registers their user account.	
Success End Condition	The user modifies their personal information.	
Failed End Condition	The user does not modify their personal information.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the ‘accountsettings’ page.
	2	The system presents the ‘accountsettings’ page to the user.

	3	The user fills the form contained within the 'accountsettings' page.
	4	The system validates the contents of the form.
	5	The system proceeds with modifying the user's information, and redirects the user to the 'accountsettings' page.
Extensions	**Step**	**Branching Action**
	4a	The validation of the contents of the form is unsuccessful.
		4a1. The system redirects the user back to the 'accountsettings' page and notifies the user of the unsuccessful validation.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.12.: Use Case #6: Non-Functional Requirements

ID	Category	Description
NF1.1	Usability	The system should provide practical and unambiguous information to the user wherever the modification of user information is unsuccessful.
NF1.2	Usability	The system should preserve the previous contents of the user information form, except for user passwords, if the user information form does not pass the required validation checks.
NF1.3	Usability	If the user changes their password, the system should require the confirmation of the new password.
NF1.4	Performance	Upon successful validation of the user information form, the system should perform every subsequent transaction promptly.
NF1.5	Security	The system should prevent the user from changing their username which remains permanently associated with their particular UUID.
NF1.6	Security	The system should protect requests against CSRF exploits and related attacks.
NF1.7	Security	The system should implement sufficient mechanisms to encrypt passwords submitted over the network.

NF1.8	Security	If the user changes their password, the system should hash and salt the new password before storing it to the database.

3.3.1.7. Delete User Account

The system supports the permanent deletion of user accounts and therefore honours the right to erasure as outlined in Art. 17 GDPR. The user visits the account settings page and selects the option to delete their user account. Then, the system presents another subpage to confirm the account deletion. As soon as the user reaffirms their choice, the system logs the user out and proceeds with the removing the corresponding entries from the database.

Table 3.13.: Use Case #7: Delete User Account

Use Case #7	Delete User Account	
Goal in Context	Enable the user to delete their account.	
Scope & Level	Authentication Subsystem, Subfunction	
Preconditions	The user registers their user account.	
Success End Condition	The user deletes their account.	
Failed End Condition	The user does not delete their account.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the ‘accountsettings’ page.
	2	The system presents the ‘accountsettings’ page to the user.
	3	The user requests the ‘deleteaccount’ subpage contained within the ‘accountsettings’ page.
	4	The system presents the ‘deleteaccount’ subpage to the user.
	5	The user selects the ‘deleteaccount’ button contained within the ‘delete accounts’ subpage.
	6	The system logs the user out, then proceeds with deleting the user account and redirects the now-former user to the ‘home’ page.
Extensions	**Step**	**Branching Action**
	1a	The user is not logged into the system when requesting the ‘accountsettings’ page.
		1a1. The system does not consider the request.

	3a	The user is not logged into the system when requesting the ‘deleteaccount’ subpage.
		3a1. The system does not consider the request.
	3b	The user is not present in the ‘accountsettings’ page when requesting the ‘deleteaccount’ subpage.
		3b1. The system does not consider the request.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.14.: Use Case #7: Non-Functional Requirements

ID	Category	Description
NF7.1	Usability	The system should provide practical and unambiguous information to the user wherever the account deletion is unsuccessful.
NF7.2	Performance	Upon successful selection of the ‘deleteaccount’ button, the system should perform every subsequent transaction promptly.
NF7.3	Security	The system should protect requests against CSRF exploits and related attacks.

3.3.1.8. Submit Processing Activity

The system supports the declaration, categorisation and integration of processing activities. Users are strongly recommended to submit involved processing activities before conducting an extensive GDPR assessment. Besides considering the organisational requirements, the GDPR assessment subsystem additionally evaluates the compliance with the processing requirements of the regulation which the processing activities indicate. The user submits the processing activity to the system by filling a form whose elements the previous section of this chapter analyses. Last but not least, the collection and maintenance of records of processing activities are in accordance with the requirements and obligations set in Art. 30 GDPR.

Table 3.15.: Use Case #8: Submit Processing Activity

Use Case #8	Submit Processing Activity
Goal in Context	Enable the user to submit a Processing Activity.
Scope & Level	Processing Activity Subsystem, Primary Task

Preconditions	The user logs into the system.	
Success End Condition	The user submits a Processing Activity.	
Failed End Condition	The user does not submit a Processing Activity.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the 'processingactivity' page.
	2	The system presents the 'processingactivity' page to the user.
	3	The user fills the form contained within the 'processingactivity' page.
	4	The system validates the contents of the form.
	5	The system proceeds with creating the processing activity and redirects the user to the 'view.processingactivity' page which displays the contents of the particular Processing Activity.
Extensions	**Step**	**Branching Action**
	1a	The user is not logged into the system when requesting the 'processingactivity' page.
		1a1. The system does not consider the request.
	4a	The validation of the contents of the form is unsuccessful.
		4a1. The system redirects the user back to the 'processingactivity' page and notifies the user of the unsuccessful validation.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.16.: Use Case #8: Non-Functional Requirements

ID	Category	Description
NF8.1	Usability	The system should provide practical and unambiguous information to the user wherever the submission of the processing activity is unsuccessful.
NF8.2	Usability	The system should preserve the previous contents of the processing activity form, if the processing activity form does not pass the required validation checks.

NF8.3	Performance	Upon successful validation of the processing activity form, the system should perform every subsequent transaction promptly.
NF8.4	Security	The system should protect requests against CSRF exploits and related attacks.

3.3.1.9. Conduct GDPR Assessment

The system reasonably emerges around the GDPR assessment subsystem which constitutes its focus segment. Users seek to evaluate their compliance with the regulation, after all. Firstly, the user answers short questions regarding the status of the organisation under assessment. Then, they are able to select and import previously-submitted processing activities to be examined during the assessment. As soon as the user submits the assessment, the system compares the answers of the user against a strictly predefined collection of rules. Next, the system investigates the imported processing activities similarly. The system terminates the assessment with labelling the organisation as Compliant, Semi-Compliant or Non-Compliant. Likewise, the previous section of this chapter consolidates additional details on the methodology behind the GDPR assessment.

Table 3.17.: Use Case #9: Conduct GDPR Assessment

Use Case #9	Conduct GDPR Assessment	
Goal in Context	Enable the user to conduct a GDPR Assessment.	
Scope & Level	GDPR Assessment Subsystem, Primary Task	
Preconditions	The user logs into the system.	
Success End Condition	The user conducts a GDPR Assessment.	
Failed End Condition	The user does not conduct a GDPR Assessment.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the ‘gdprassessment’ page.
	2	The system presents the ‘gdprassessment’ page to the user.
	3	The user fills the form contained within the ‘gdprassessment’ page.
	4	The system validates the contents of the form.

	5	The system proceeds with creating the GDPR Assessment and redirects the user to the 'view.gdprassessment' page which displays the contents of the particular GDPR Assessment.
Extensions	**Step**	**Branching Action**
	1a	The user is not logged into the system when requesting the 'processingactivity' page.
		1a1. The system does not consider the request.
	4a	The validation of the contents of the form is unsuccessful.
		4a1. The system redirects the user back to the 'gdprassessment' page and notifies the user of the unsuccessful validation.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.18.: Use Case #9: Non-Functional Requirements

ID	Category	Description
NF9.1	Usability	The system should provide practical and unambiguous information to the user wherever the submission of the GDPR assessment is unsuccessful.
NF9.2	Usability	The system should preserve the previous contents of the GDPR assessment form, if the GDPR assessment form does not pass the required validation checks.
NF9.3	Performance	Upon successful validation of the GDPR assessment form, the system should perform every subsequent transaction promptly.
NF9.4	Security	The system should protect requests against CSRF exploits and related attacks.

3.3.1.10. Conduct DPI Assessment

As suggested earlier, the secondary objective of the system is to support users with conducting DPIAs. The DPI assessment subsystem implements and adjusts the CNIL's well-established PIA methodology. The user begins by providing detailed information regarding the processing activity under impact assessment. The system continues with determining and mapping the risks associated with three scenarios, and the user concludes the DPIA with providing further recommendations, the opinion of the designated DPO and the final approval or rejection.

Table 3.19.: Use Case #10: Conduct DPI Assessment

Use Case #10	Conduct DPI Assessment	
Goal in Context	Enable the user to conduct a DPI Assessment.	
Scope & Level	DPI Assessment Subsystem, Primary Task	
Preconditions	The user logs into the system.	
Success End Condition	The user conducts a DPI Assessment.	
Failed End Condition	The user does not conduct a DPI Assessment.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the 'dpiassessment' page.
	2	The system presents the 'dpiassessment' page to the user.
	3	The user fills the form contained within the 'dpiassessment' page.
	4	The system validates the contents of the form.
	5	The system proceeds with creating the DPI Assessment and redirects the user to the 'view.dpiassessment' page which displays the contents of the particular DPI Assessment.
	6	The user fills the supplementary form fields contained within the 'view.dpiassessment' page and then validates the DPI Assessment by selecting either the 'Reject Assessment' or 'Approve Assessment' button.
	7	The system validates the contents of the supplementary form fields.
	8	The system proceeds with updating the DPI Assessment accordingly and redirects the user to the 'view.dpiassessment' page which displays the updated contents of the particular DPI Assessment.
Extensions	**Step**	**Branching Action**
	1a	The user is not logged into the system when requesting the 'processingactivity' page.
		1a1. The system does not consider the request.

	4a	The validation of the contents of the form is unsuccessful.
		4a1. The system redirects the user back to the ‘dpiassessment’ page and notifies the user of the unsuccessful validation.
	7a	The validation of the contents of the supplementary form fields is unsuccessful.
		7a1. The system redirects the user back to the ‘view.dpiassessment’ page and notifies the user of the unsuccessful validation.
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.20.: Use Case #10: Non-Functional Requirements

ID	Category	Description
NF10.1	Usability	The system should provide practical and unambiguous information to the user wherever the submission of the DPI assessment is unsuccessful.
NF10.2	Usability	The system should preserve the previous contents of the DPI assessment form, if the DPI assessment form does not pass the required validation checks.
NF10.3	Performance	Upon successful validation of the DPI assessment form, the system should perform every subsequent transaction promptly.
NF10.4	Security	The system should protect requests against CSRF exploits and related attacks.

3.3.1.11. View Completed Assessments

The system supports the aggregation and display of every processing activity and assessment connected with each user. The user can access the respective, for this purpose, page which includes three separate tables. The first table incorporates the processing activities; the second table lists every GDPR assessment, and the third one lists every DPI assessment. Every table entry specifies the associated organisation, the date and time of submission and, if applicable, the current status of the assessment.

Table 3.21.: Use Case #11: View Completed Assessments

Use Case #11	View Completed Assessments	
Goal in Context	Enable the user to view completed assessments.	
Scope & Level	Completed Assessments Subsystem, Primary Task	
Preconditions	The user logs into the system.	
Success End Condition	The user views completed assessments.	
Failed End Condition	The user does not view completed assessments.	
Primary Actor	User	
Description	**Step**	**Action**
	1	The user requests the 'completedassessments' page.
	2	The system retrieves every Processing Activity, GDPR Assessment and DPI Assessment associated with the user.
	3	The system presents the 'completedassessments' page to the user which includes every Processing Activity, GDPR Assessment and DPI Assessment which the system previously retrieved.
Extensions	**Step**	**Branching Action**
	2a	
Sub-Variations	**Step**	**Branching Action**
	N/A	N/A

Table 3.22.: Use Case #11: Non-Functional Requirements

ID	Category	Description
NF11.1	Usability	The system should inform the user if there are no processing activities or assessments present within their userspace.

3.3.2. Entity-Relationship Model

Analysts use entity-relationship diagrams to model database systems and figure out the data that an information system accommodates. The diagram acts as the blueprint which specifies the actual data to store (Bagui & Earp, 2003). Thalheim (2000) further adds that database design is a unique knowledge representation process which should contain all the information required by the users for the efficient behaviour of the entire information system.

The user can submit many processing activities, and each processing activity belongs to a single user. Hence, this description indicates a one-to-many relationship.GDPR assessments feature two separate dependencies. The user can submit many GDPR assessments, and each GDPR assessment belongs to a single user; this shows a one-to-many relationship as previously. Meanwhile, each GDPR assessment can include many processing activities, and each processing activity can be included in many GDPR assessments; this is instead a many-to-many relationship. Lastly, DPI assessments do not depend on GDPR assessments. Each user can submit many DPI assessments, but each DPI assessment belongs to a single user; this implies a one-to-many relationship again. The resulting logical Entity-Relationship Diagram (ERD) in Figure 3.3 reflects the above entity-relationship descriptions and indicates the system's most common data requirements.

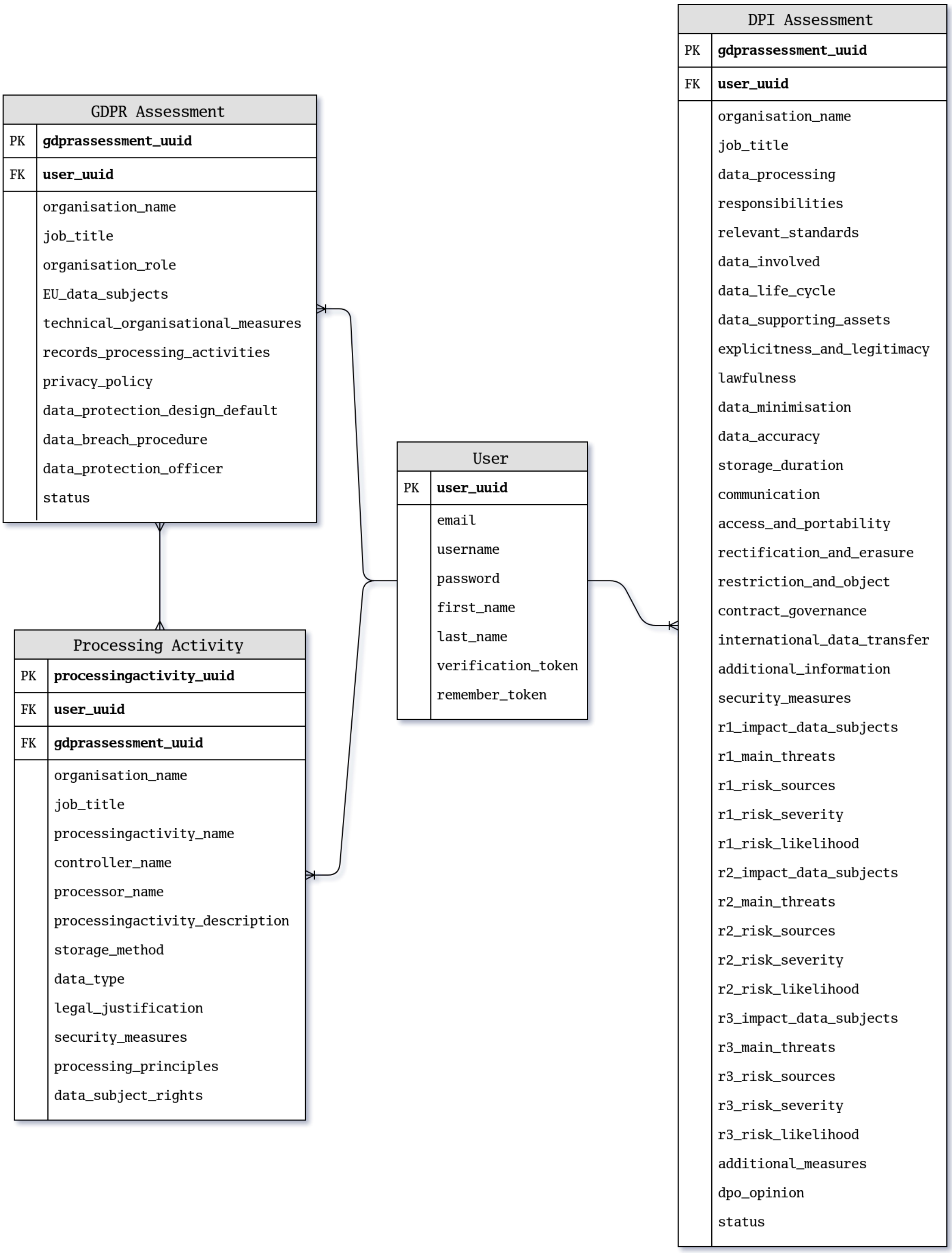
3.4. Implementation

Kroll and Kruchten (2003) claim that the construction phase is typically the most time-consuming and involves the vast majority of the work. The subsystems and the most critical use-cases are already defined, but the system does not exist yet. They also suggest that during the implementation, the focus is to develop high-quality code cost-effectively while benefiting from existing architectural mechanisms to accelerate the production of code.

3.4.1. Software Development

The system's use-cases and requirements are defined and the author proceds with the development of the system. As far as the selection of the development strategy is concerned, an elegant web application that emphasises minimalistic and responsive web design emerges as a good candidate. Native desktop or mobile applications usually perform remarkably faster compared to their web-based counterparts. However, they require extra time and resources for their development, and each native implementation typically targets specific platforms. Plus, the envisioned system does not require access to any device hardware with which native applications integrate well. So, the possibility of developing the system as native applications does not seem reasonable.

There exist many exceptional programming languages in web development. The author chooses PHP and the Laravel framework since he feels more familiar with the language and the particular workflow; this preference is mostly subjective though. The utilisation of any framework is a determining factor for the successful implementation of this system as it minimises and expedites the foundational work required and furthermore helps ensure that the application follows responsible practices in terms of performance and security.



GDPR Assessment	
PK	**gdprassessment_uuid**
FK	**user_uuid**
	organisation_name
	job_title
	organisation_role
	EU_data_subjects
	technical_organisational_measures
	records_processing_activities
	privacy_policy
	data_protection_design_default
	data_breach_procedure
	data_protection_officer
	status

Processing Activity	
PK	**processingactivity_uuid**
FK	**user_uuid**
FK	**gdprassessment_uuid**
	organisation_name
	job_title
	processingactivity_name
	controller_name
	processor_name
	processingactivity_description
	storage_method
	data_type
	legal_justification
	security_measures
	processing_principles
	data_subject_rights

User	
PK	**user_uuid**
	email
	username
	password
	first_name
	last_name
	verification_token
	remember_token

DPI Assessment	
PK	**gdprassessment_uuid**
FK	**user_uuid**
	organisation_name
	job_title
	data_processing
	responsibilities
	relevant_standards
	data_involved
	data_life_cycle
	data_supporting_assets
	explicitness_and_legitimacy
	lawfulness
	data_minimisation
	data_accuracy
	storage_duration
	communication
	access_and_portability
	rectification_and_erasure
	restriction_and_object
	contract_governance
	international_data_transfer
	additional_information
	security_measures
	r1_impact_data_subjects
	r1_main_threats
	r1_risk_sources
	r1_risk_severity
	r1_risk_likelihood
	r2_impact_data_subjects
	r2_main_threats
	r2_risk_sources
	r2_risk_severity
	r2_risk_likelihood
	r3_impact_data_subjects
	r3_main_threats
	r3_risk_sources
	r3_risk_severity
	r3_risk_likelihood
	additional_measures
	dpo_opinion
	status

Figure 3.3.: Logical Entity-Relationship Diagram Indicating the System's Data Requirements

3.4.1.1. Back-End Web Development

Back-end frameworks provide useful conventions that encourage developers to focus on the actual development of the intended software than spending their efforts on understanding the underlying technologies.

The system's back-end is based on Laravel. Laravel is a rapid application development framework which minimises the steps needed for publishing the software (Stauffer, 2016). The framework focuses on simplicity and is bundled with tools and components for enhancing the development experience. Laravel, for example, features Eloquent Object-Relational Mapping (ORM) that simplifies the process of working with databases.

The architecture of the system matches the Model-View-Controller (MVC) software design pattern which divides an application into three main logical and interconnected component types: the models, the views and the controllers. Pitt (2012) explains that models keep the logic of the application and specify the information that the application accesses in a database. He adds that views contain the user interface elements of the application that the user sees and interacts with; these include HTML, CSS and JavaScript files. Finally, he informs that controllers connect models with views and handle how the application responds to user interactions within the views. The developed system

Models The system's back-end depends on four models which the logical ERD in Figure 3.3 similarly suggests. For each model, there exists an analogous table in a MySQL relational database management system that the system operates.

- User.php
- ProcessingActivity.php
- GDPRAssessment.php
- DPIAssessment.php

Views Laravel uses the Blade templating engine towards the design of layouts. Views feature a combination of typical HTML markup and PHP code for performing actions. The system can present a total of fifteen views to the user. There are also two custom views for 403 and 404 HTTP status codes.

- forgotpassword.blade.php
- resetpassword.blade.php
- signin.blade.php
- signup.blade.php
- accountsettings.blade.php

- completedassessments.blade.php
- dpiassessment.blade.php
- gdprassessment.blade.php
- processingactivity.blade.php
- 403.blade.php
- 404.blade.php
- privacypolicy.blade.php
- termsofuse.blade.php
- dashboard.blade.php
- documentation.blade.php
- home.blade.php
- knowledgebase.blade.php

Controllers The system uses twelve controllers to facilitate the interactions of the users. These controllers process requests, manipulate data according to the models and interact with the views to display the system's output.

- AuthController.php
- ForgotPasswordController.php
- ResetPasswordController.php
- AccountSettingsController.php
- CompletedAssessmentsController.php
- DashboardController.php
- DPIAssessmentController.php
- GDPRAssessmentController.php
- ProcessingActivityController.php
- DocumentationController.php
- HomeController.php
- KnowledgeBaseController.php

3.4.1.2. Front-End Web Development

The system uses Bootstrap, the most popular front-end framework on the planet. Bootstrap is a powerful prototyping tool, as most of the configuration is prearranged and allows developers to build a prototype without making substantial time commitments (M. Lambert, 2016). Its famous grid system facilitates the design of web pages which support different screen dimensions and resolutions without hassle.

The previous sub-subsection displays a list including the seventeen views developed for the system's front-end which are primarily based on Bootstrap and can connect with

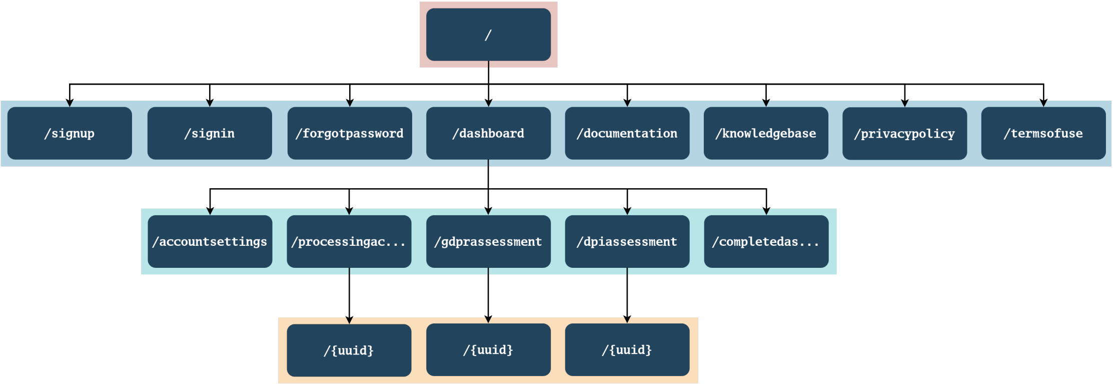


Figure 3.4.: Sitemap Listing the System's Key Routes

the back-end using Laravel's Blade templating engine. Figure Figure 3.4 meanwhile shows the system's most prominent routes which connect the user to the views of the front-end.

3.4.1.3. Version Control

Nowadays, version control systems are the foundation of software development. They are capable of recording the changes made to a set of files over a timeline and allow developers to recall particular versions of those files (Somasundaram, 2012). The software development process of the system utilises Git, an open-source version control system used by millions of developers worldwide.

3.4.1.4. Licensing

Laurent (2004) points out that open-source licensing restricts anybody from particularly abusing the work of others. At the same time, free and open-source software provides users with an extended set of rights. They can run the software for personal and commercial reasons, study the source code of the software, modify the software and redistribute their modified versions to everyone.

The system applies the GNU Affero General Public License v3. The GNU AGPL v3 focuses on software transmitted through networks and has one added requirement compared to the well-known GNU GPL v3. It requires users running modified versions of the software on servers to provide the source code corresponding to those modified versions, thus preventing the loophole which exists with the GNU GPL v3.

3.4.2. Brand Identity

Wheeler (2009) comments that strong brands can stand out in densely crowded marketplaces. The success of any brand depends on its perception by people, regardless of whether it is a start-up, a non-profit, or a product. She also mentions that brand identity uses different components and connects them into entire systems with the aim of inspiring recognition, amplifying differentiation, and making big ideas accessible.

The implemented front-end of the system follows a minimalistic responsive web design approach, features selective typography rules and appropriates a discrete multi-colour palette. The aim is to maintain design consistency across screens and present an appealing and stylish user interface while avoiding clutter.

3.4.2.1. Typography

The system's front-end makes complete use of Lato, which is a humanist sans-serif typeface freely available under the SIL Open Font License. It includes extended Latin, Cyrillic, and Greek characters and therefore supports many languages. Lato features nine diverse weights and their corresponding italics.

3.4.2.2. Color Palette

The primary colour is matte blue (HEX #284B6E) and generally covers the navigation bar, the sidebar, all hyperlinks and primary buttons of the system. The system also uses matte gray (HEX #E9ECEF) to colour miscellaneous Bootstrap components such as breadcrumbs, jumbotrons and the footer. There also exist supporting matte red (HEX #BD584F), matte yellow (HEX #CA8D49), matte cyan (HEX #73A9A2) and matte green (HEX #719768) colours to symbolise errors, warnings, information and success messages and indications of the system. Figure 3.5 illustrates the color palette of the system's front-end.

3.4.3. Documentation

Kukulska-Hulme (1999) compares documentation to the instruction manuals that people always obtain, but very few are going to read. She implies that documentation is regularly full of instructions that do not work, do not make sense, or are just plain wrong. She appends that we cannot assure effective communication every time we speak or write and therefore users cannot always depend on computer application displays or handbooks to thoroughly understand the message. Furthermore, she points out that user manuals and guides which adopt an overtly friendly style of writing sometimes fail to assist users meaningfully.

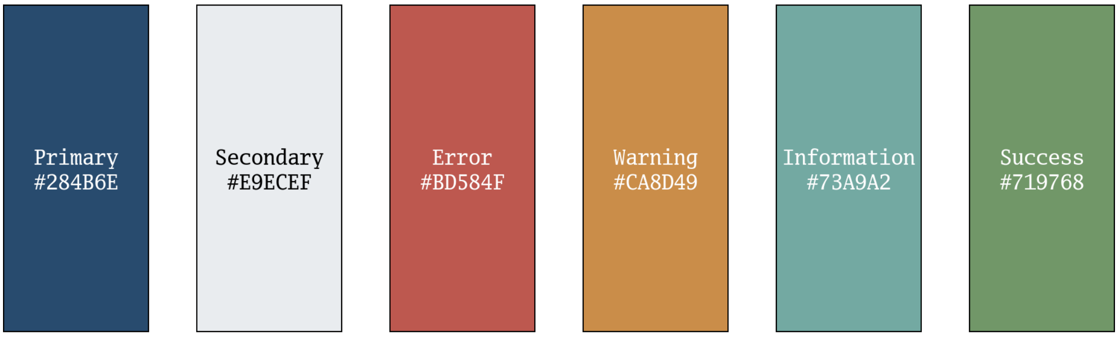


Figure 3.5.: The Color Palette of the System's Front-End

The system should take the above considerations into account for the entirety of its documentation which breaks down into three separate parts: the end-user documentation, the knowledge base and the technical documentation. The end-user documentation complements the minimalistic and user-friendly design concepts present within the system's front-end, the knowledge base helps users become acquainted with the regulation, and, finally, the technical documentation supports developers and technologists.

3.4.3.1. End-User Documentation

The end-user documentation provides brief information on how the system functions and meanwhile leads users through using the system. All three subsystems, i.e., the Processing Activity, GDPR Assessment and DPI Assessment subsystems, include information icons which connect the user with the corresponding sections of the end-user documentation.

3.4.3.2. Knowledge Base

The knowledge base is part of the broader documentation and intends to aid users with the interpretation and conceptualisation of the most critical aspects of the regulation. It describes the essential terminology and presents the organisational and processing requirements of the GDPR.

3.4.3.3. Technical Documentation

The technical documentation refers to software developers and technologists who wish to adopt, manage or further develop the system using their own technological means and infrastructure. It highlights the software and hardware requirements, includes a short installation guide and assists with troubleshooting.

3.5. Evaluation

Merriam and Tisdell (2015) consider that evaluation research constitutes one form of applied research that involves the collection of data or evidence on the worth or value of a program, process, or technique. The primary purpose of evaluation research is to assess the effectiveness of the program and arrange for improvements and to inform decisions about future programming (Patton, 2014).

Following the analysis, design and implementation of the system, this segment seeks to ascertain if the developed system meets specific criteria. It is essential to discover whether the system fulfils the initial scope of this diploma thesis, to assess its usability and performance and to subsequently determine whether it can be beneficial to its intended target users. Furthermore, it is desirable to receive advice on how to improve the system and its integrated features.

The author of this thesis and sole developer of the system refers to a diverse set of experts to study and evaluate the system. Experts frequently experience time constraints; therefore the evaluation process is minimal and does not assume an extensive review of the system, nor does it expect prolonged feedback from the experts. The following subsection provides more information regarding the said process.

3.5.1. Process

The author of this diploma thesis first deploys the experimental version of the system on the Internet. For this specific purpose, he chooses a well-established cloud service provider to accommodate the experimental system and also integrates the experimental system with a cloud-based e-mail delivery service. Next, the author creates temporary and anonymised user accounts to provide to the experts. The author then reaches out to the experts and provides them with detailed information about the evaluation process. Apart from specifying the steps needed to evaluate the system, the author provides the experts with a two-minute introductory video that briefly explains the primary functions of the system and their workflow.

In the beginning, the expert logs into the test system with their credentials and browses through the pages while examining the core functions and attempting to perform some designated activities. Preferably, the expert experiments at least with the three core subsystems, i.e. the Processing Activity, the GDPR Assessment and the DPI Assessment. The expert later previews the processing activities and assessments that their userspace contains. As soon as they finish experimenting with the system, they refer to the evaluation questionnaire which contains the following three questions:

What is your background? The expert describes their background using as few details as possible.

Which elements did you find most interesting? The expert designates the features of the system they find to be engaging and helpful for the person conducting the assessment.

Did you see any issues? What do you think can be further improved? The expert points out any potential issues or features that are missing. Plus, they provide recommendations to improve the effectiveness and overall user experience of the system.

Is there anything else you would like to add? The expert is free to supplement any additional information they consider to be important.

This evaluation process makes considerable effort to respect the privacy of the experts and does not publish their names and affiliated organisations in this document. Instead, the following snippets, that include the feedback of the experts, merely provide some generic and non-identifiable background information about the experts.

Upon the submission of the evaluation questionnaires, the author of this thesis thanks the experts for their participation and significant contribution, disables the respective test user accounts and terminates this process.

3.5.2. Execution

This subsection encompasses five unique expert opinions on the functionality and usefulness of the developed system. Each opinion indicates the features that are practical for the intended users. In the meantime, the experts point to the elements and the functions that are either missing or can be refined and provide recommendations for future versions.

3.5.2.1. Expert Opinion #1

The first expert is an academic who focuses and performs research on privacy engineering. He has authored several research papers in international scientific journals and conferences and has also been involved with the public sector as an advisor.

This expert mentions that all elements, which the system includes, are beneficial for the privacy analyst or security officer who wishes to assess the alignment of an organisation with the GDPR. Concerning usability, he suggests splitting the process behind the conducting of the assessments into separate screens since every screen includes too much information currently. Last but not least, he recommends adding some helpful information above every group of fields whenever applicable.

3.5.2.2. Expert Opinion #2

The second expert is the data protection officer at a public European university which consists of more than ten thousand students. He possesses technical expertise in the domain of ICT.

This expert highlights the fact that the system includes a process for creating records of processing activities and suggests that this is an essential requirement which should be carried out carefully in order ensure that nothing is missing when mapping the data that an organisation processes. He considers that the GDPR Assessment lacks comprehensiveness and suggests that the process should be further analysed and expanded while considering more options. Finally, he recommends that the DPI Assessment should include metrics in order to measure and quantify the impact of each potential incident.

3.5.2.3. Expert Opinion #3

The author of this thesis contacted an open-source design agency and asked for their help to assess the overall design and usability of the developed system. One open-source designer, one usability researcher and one tester participated in this evaluation and jointly provided their feedback.

Their usability test presents overall positive results but highlights some small improvements. To begin with, the system's user interface is proved to be responsive across different screens and resolutions. The experts recommend providing additional information on the home page about the GDPR assessment, for new users who are not very familiar. Moreover, they suggest choosing more relevant photos for the home page and also changing its title font or font size for readability purposes as it currently appears that the title and subtitle are together. Regarding the end-user documentation, they propose adopting a more user-friendly approach that avoids writing in the third-person but instead addresses the users directly. Furthermore, they mention that the dashboard should first connect users with the processing activity subsystem rather than the GDPR assessment; the current association can confuse users if they are unaware of the process.

The experts continue by suggesting that the text should be fully compliant with the Web Content Accessibility Guidelines (WCAG) 2.0; the hero section within the home page barely passes AA, whereas it should have a more significant contrast ratio with the background to be AAA compliant. Further, they advise that the dashboard card icons might benefit from being coloured black (with 25% opacity or similar) instead of pure white as on some resolutions the text may override the icon. Finally, they encourage expanding the margins between the sidebar and the content of every page.

3.5.2.4. Expert Opinion #4

The fourth expert maintains a background in law and data science and is part of an EU-based organisation that promotes digital rights.

This expert overall believes that the system has a well-designed interface that is easy-to-use by the end-user. He adds that this is particularly important; had the system been complex, it would have created unnecessary confusion. He also mentions that the dashboard provides easy access to the different functions of the system. This expert finds the approach of recording the processing activities to be smart and also explains that the questions within the GDPR assessment are clear and to the point. Concerning the DPI assessment, this expert believes the system allows for detailed input as supposed and provides basic guidance towards the end-users to help them understand how to keep their description short and to the point.

He reaffirms that the developed system is a student project, and for such a project the quality is great; the time and effort that the student has put into it have resulted in an easy-to-use tool, he appends. This expert seems concerned about the authentication process and suggests that a two-step authentication can probably help users keep their accounts secure if for any reason their e-mail account is compromised. Moreover, he advises adding a visualisation tool for the data mapping which can appeal to people attending meetings and performing evaluations. Finally, he recommends making mandatory the filling of some depending on the previous selections that the user has made during the assessment.

Last but not least, this expert says the brief introductory video accompanying the test instance of the system was very enjoyable. He believes it would perhaps be helpful if the video were a bit longer and more detailed so that prospective users can see additional functionality and therefore gain some initial understanding.

3.5.2.5. Expert Opinion #5

The fifth expert is an entrepreneur and business consultant offering free and open-source software services. He has worked with multiple communities to deliver projects to the public sector.

This expert begins with commending the idea behind the developed system and comments that very few similar implementations exist. He considers the user experience to be satisfactory but believes it can nonetheless be further improved to create an enhanced workflow. He advises creating an automated process for users to request their account data, although he acknowledges the additional amount of work needed. Furthermore, he recommends using an open-source platform for hosting and managing the content of both the system's documentation and the knowledge base more efficiently. Last but not least, he suggests creating a community around the project and inviting contributors to translate the system's interface into different languages.

3.5.3. Summary

All experts agree that the developed system serves its intended purposes and produces an overall pleasant user experience. The core subsystems of the platform are relevant and helpful for the person who wishes to assess their organisation's compliance with the regulation.

The experts suggested that the user experience can be further improved by modifying existing elements and adding new characteristics. Likewise, some of them proposed minor tweaks and additions to the workflow of the processing activities and the GDPR and DPI assessments. They also raised some concerns regarding the security of the system, which is adequate but needs to be further enhanced to minimise the risk of unlawful incidents. The second subsection of the fourth and last chapter reflects the suggestions and feedback of the experts and expands upon them.

4. Conclusion

4.1. Summary

This diploma thesis concludes with the delivery and validation of the envisioned open-source web-based system that assists individuals and organisations to adapt to the regulation. The study of the GDPR's final legal text and recently-published academic work eased the design of an elementary assessment model which applies to many everyday business processes of SMEs.

The proposed system does not directly oppose advanced business solutions that are prepared and offered by professional software companies and consulting firms. Nevertheless, it does exhibit satisfactory evaluations directed toward the majority of individuals and SMEs that are coping with compliance. Experts have recommended improvements for the system to increase its effectiveness, efficiency, and scope. The next and final section reflects those suggestions and provides future recommendations.

The regulation, at the time of writing, has been into effect for approximately eight months. Many organisations face harsh regulatory responses, no matter their size. CNIL (2019), for example, recently imposed a financial penalty of 50 million Euros against Google for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization. Therefore, it seems that even predominant companies are not fully complying with the regulation which in turn indicates severe gaps in the global privacy and data protection field.

Technology evolves rapidly. So does the spread and exchange of massive amounts of personal data from one side of the planet to another. It is vital for technologists and ICT professionals to highlight the importance of privacy and increase awareness around data protection matters. Citizens should be made aware of the risks related to the treatment of their personal data as well as of the available controls they possess. Conclusively, organisations, and pretty much everyone who processes personal data, should consider investing in cybersecurity and information security management to ensure the adequate protection of their digital and physical infrastructure.

4.2. Recommendations

Although the system appears to be practical and relevant to the purposes of this diploma thesis, it does require adjustments to maximise its efficiency and improve its usability. Experts have recommended dividing the steps of the processing activity and assessment subsystems into separate screens and rearranging the content to avoid confusion and to present elegant user interfaces. The assessment model can be expanded further to include additional chapters and articles of the regulation even beyond the discrete requirements currently examined by this thesis. Consequently, the set of rules and algorithms behind the subsystems as well as their corresponding interfaces can be updated and extended.

Furthermore, the system can append additional features to the existing subsystems. Users, for example, can benefit from the ability to download or print records of processing activities and assessments and to transfer or forward such content to different user accounts. The authentication subsystem can support logging-in with the combination of the username and password as an alternative to the e-mail address and password combination used currently. Third-party authentication support, such as the integration of popular Single Sign-On (SSO) implementations, can also be regarded as a very advantageous characteristic for the potential adoption of the system by organisations with such infrastructure.

The proposed system incorporates appropriate security and validation mechanisms to prevent malicious attackers from performing unauthorised and unlawful activities and strives to improve its production-ready status. However, the system requires more thorough testing and security assessments to guarantee and strengthen the ongoing confidentiality, integrity and availability of the information it stores and processes. The system can also employ CAPTCHA challenges or refer to infrastructure-based controls to show resistance to illegitimate user registration attempts and brute force attacks.

The source code behind the system features established coding standards on both the front-end and the back-end section. There are source code components, however, which can be updated or slightly reworked using more elegant and streamlined coding approaches. The current implementation should support hundreds or even a few thousands of submitted processing activities and stored assessments, but there are currently strict limitations which may prevent the system from scaling-up as they would cause delayed response times. The database storage mechanisms would, as a result, need adjustment on that occasion.

Appendices

A. Existing Implementations

A.1. Introduction

The IAPP (2018) notices that the privacy technology market has grown remarkably during the last year; more than one hundred new and pre-established companies are now part of its expanding privacy tech vendor list. Furthermore, existing vendors offer additional privacy technology services and thus jointly create a vibrant marketplace.

While the thorough analysis and evaluation of existing implementations lie beyond the scope of this diploma thesis, this appendix examines and discusses some of the existing solutions that are available on the market. This limited and restrained study aims to indicate that the privacy and data protection domain can benefit from an open-source tool that can perform comprehensive assessments.

A.2. Comparison

This study divides examined implementations into three main categories mostly depending on their distribution and licensing model:

- Paid Software, whose licensing models involve payments and are usually intended for organisations rather than individual users;
- Freeware, which is available free-of-charge but may impose restrictions to users while its source code remains proprietary; and
- Free and Open-Source Software, which permits users to run the software without restrictions, to view the source code and make any modifications, and to distribute copies of the original or the modified software to others.

A.2.1. Paid Software

This subsection explores OneTrust's GDPR Validation and BigID's GDPR Compliance solutions which are specialised services mostly targeting businesses.

A.2.1.1. OneTrust's GDPR Validation

OneTrust seemingly centres its business model around privacy management and consulting and offers sophisticated and comprehensive solutions to its clients.

OneTrust's GDPR Validation appears to examine the readiness of an organisation including the conducting of DPIAs, the procedures for the handling of personal data breaches, and the function of the DPO. The GDPR Validation is said to integrate with OneTrust's Assessment Automation tool and help streamline the validation process of the customer. OneTrust privacy professionals can also analyse the output of the assessment and provide consulting with customised recommendations.

The above description is however according to the official marketing material since OneTrust offers premium services. OneTrust does seem to provide demonstrations of their products and services which unfortunately are not easily obtainable.

A.2.1.2. BigID's GDPR Compliance

BigID likewise offers advanced services in the domain of privacy and data protection. They provide software solutions for compliance with the GDPR, too.

The company mentions its platform helps with achieving data minimisation, the handling of the requests of data subjects, consent management, data residency and compliance with breach notification windows. BigID offers additional solutions for miscellaneous necessities, such as the maintenance of records of processing activities and the conducting of DPIAs.

Similarly to OneTrust, BigID does not appear to provide an easily accessible demonstration of its platform as it requires an appointment in advance.

A.2.2. Freeware

This subsection examines Microsoft's GDPR Detailed Assessment and Kaspersky's Online Assessment Tool which are both available at no cost.

A.2.2.1. Microsoft's GDPR Detailed Assessment

Microsoft seems to have put significant effort to help prepare its customers and partners with the obligations of the regulation and offers various tools and informational material related to the GDPR. The GDPR Detailed Assessment is Microsoft's tool that its partners can use to help their customers evaluate the readiness of their employees, processes, and technology to the requirements GDPR.

The GDPR Detailed Assessment is not a software solution but merely a spreadsheet, prepared for the Microsoft Office suite, which covers a wide range of organisational and processing requirements, presents visuals and provides recommendations to organisations that wish to improve their compliance levels. The spreadsheet is available in multiple foreign languages.

A.2.2.2. Kaspersky's Online Assessment Tool

Kaspersky Lab has created a section on its website and offers practical information about the GDPR to its customers. They created an animated video for providing an introduction to the expectations of the regulation and meanwhile offer a whitepaper and diagram describing the alignment of businesses with the requirements of the GDPR. More importantly, they used to offer an online assessment tool that asked users about the readiness of their organisation with the GDPR, offered advice and guidance regarding GDPR compliance and provided users with their customised evaluation.

While the aforementioned online assessment tool must have helped towards increasing awareness around the regulation, it did not let users perform comprehensive assessments, record and analyse their processing activities nor conduct DPIAs.

A.2.3. Open-Source Software

This subsection considers CNIL's PIA Software and Privacy Radius' GDPR Checklist which are free and open-source software offering unrestricted usage and customisation options.

A.2.3.1. CNIL's PIA Software

The CNIL's open-source PIA tool primarily targets data controllers who are already somewhat familiar with the PIA methodology. The software is cross-platform and is available in its portable version, which supports Microsoft Windows, macOS and GNU/Linux, and in its web version which anyone can deploy on their own infrastructure.

The software practices the CNIL's well-established PIA methodology and assists controllers with performing DPIAs. However, it does not offer any means of assessing the compliance of an organisation with the regulation. Furthermore, the CNIL does not appear to be offering any software-specific documentation besides the official PIA guides.

A.2.3.2. Privacy Radius' GDPR Checklist

Privacy Radius currently maintains three separate privacy and data protection-related projects, two of which are available as open-source software.

The GDPR Compliance Checklist is an online checklist, as its name suggests. Data controllers and data processors can interact with the checklist and manually determine how they are performing compared to the obligations set by the regulation. The checklist appears to be considering most requirements, although it does not enable users to perform an actual evaluation. Furthermore, it does not provide any support for handling records of processing activities or conducting DPIAs.

A.3. Conclusion

The global marketplace currently offers multiple privacy management and GDPR compliance services that can satisfy different kinds of needs and expectations. Solutions that are accessible free-of-charge or are licensed as open-source software tend to lack fundamental characteristics that can support organisations with their necessary compliance efforts. On the contrary, there are solutions which aim at helping organisations fulfil the majority of the GDPR's obligations. However, they are premium and not easily accessible by those who cannot afford their acquirement and preservation.

Consequently, individuals and SMEs interested in increasing their privacy and data protection efforts, and meanwhile meeting every applicable requirement of the GDPR, can presumably benefit from the open-source web-based system that this diploma thesis produces. This system has the following strengths:

- Available free-of-charge, meaning its intended users do not need to pay for its obtainment;
- Released as open-source software, allowing everyone with the necessary knowledge to view the source code and perform any modifications;
- Performs comprehensive assessments, beginning with the collection of processing activities, then continuing with organisation-wide GDPR assessments and finally concluding with DPI assessments; and
- Showcases a modern and responsive user interface, plus supports multiple device types, operating systems and screen resolutions.

Bibliography

Bagui, S., & Earp, R. (2003). *Database Design Using Entity-Relationship Diagrams* (1st ed.). Foundations of database design series. Auerbach.

CNIL. (2019). The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. Retrieved February 15, 2019, from https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Cockburn, A. (1998). Basic Use Case Template.

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). *OJ*, *L 281*.

Folsom, R. H., Lake, R. B., & Nanda, V. P. (1996). *European Union Law After Maastricht: Practical Guide for Lawyers Outside the Common Market* (1st ed.). Kluwer Law International.

Garber, J. (2018). GDPR - compliance nightmare or business opportunity? *Computer Fraud & Security*.

Gkoulalas-Divanis, A., & Bettini, C. (2018). *Handbook of Mobile Data Privacy*. Springer.

Gregg Latchams Solicitors. (2017). A practical guide to the General Data Protection Regulation. Retrieved February 15, 2019, from https://www.gregglatchams.com/news-and-events/news/gregg-latchams-launches-guide-gdpr/

Hansen, M., Kosta, E., Nai-Fovino, I., & Fischer-Hübner, S. (2018). Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool.

Hert, P. D., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2017). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*.

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (1st ed.). Law, Governance and Technology Series 31. Springer International Publishing.

Houser, W. G., Kimberly; Voss. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *SSRN Electronic Journal*.

IAPP. (2018). 2018 Privacy Tech Vendor Report. Retrieved February 15, 2019, from https://iapp.org/resources/article/2018-privacy-tech-vendor-report/

Information Commissioner's Office. (2018a). Guide to the General Data Protection Regulation (GDPR). Retrieved February 15, 2019, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Information Commissioner's Office. (2018b). When can we rely on legitimate interests? Retrieved February 15, 2019, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/

Kendall, K. E., & Kendall, J. E. (2013). *Systems Analysis and Design* (9th ed.). Pearson.

Kroll, P., & Kruchten, P. (2003). *The Rational Unified Process Made Easy : A Practitioner's Guide to the RUP*. Addison-Wesley Object Technology Series. Addison-Wesley.

Kukulska-Hulme, A. (1999). *Language and Communication: Essential Concepts for User Interface and Documentation Design*. Oxford University Press.

Lambert, M. (2016). *Learning Bootstrap 4* (2nd ed.). Packt Publishing.

Lambert, P. (2016). *Data Protection Officer: Profession, Rules, and Role*. Auerbach Publications.

Laurent, A. M. S. (2004). *Understanding Open Source and Free Software Licensing* (1st ed.). O'Reilly Media.

Leenes, R., van Brakel, R., Gutwirth, S., & Hert, P. D. (2017). *Data Protection and Privacy: The Age of Intelligent Machines*. Hart Publishing.

Leffingwell, D., & Widrig, D. (2003). *Managing Software Requirements: A Use Case Approach* (2nd ed.). Addison-Wesley.

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative Research: A Guide to Design and Implementation* (4th ed.). Jossey-Bass.

Miglicco, G. (2018). GDPR is here and it is time to get serious. *Computer Fraud & Security*.

Mittal, S. (2017). Old Wine with a New Label: Rights of Data Subjects Under GDPR. *SSRN Electronic Journal*.

Moore, A. (2018). *The GDPR & Managing Data Risk For Dummies, Symantec Special Edition*. For Dummies. Wiley.

Mukundan, S., Ramani, S., Muthu Raman, S., Anjaneyulu, K., & Chandrasekar, R. (2007). A Practical Introduction to Rule Based Expert Systems.

Patton, M. Q. (2014). *Qualitative Research & Evaluation Methods* (4th ed.). Sage Publications, Inc.

Pitt, C. (2012). *Pro PHP MVC*. Expert's Voice in Open Source. Apress.

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*.

Quelle, C. (2015). The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing. *SSRN Electronic Journal*.

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). (2016). *OJ*, *L 119*.

Rumbaugh, J., Jacobson, I., & Booch, G. (1999). *The Unified Modeling Language Reference Manual*. Addison-Wesley Object Technology Series. Addison-Wesley.

Somasundaram, R. (2012). *Git: Version Control for Everyone*. Packt Publishing.

Stauffer, M. (2016). *Laravel: Up and Running: A Framework for Building Modern PHP Apps*. O'Reilly.

Steiner, J., Woods, L., & Twigg-Flesner, C. (2006). *EU Law* (9th ed.). Oxford University Press.

Synodinou, T.-E., Jougleux, P., Markou, C., & Prastitou, T. (2017). *EU Internet Law: Regulation and Enforcement* (1st ed.). Springer International Publishing.

Tamò-Larrieux, A. (2018). *Designing for Privacy and its Legal Framework* (1st ed.). Law, Governance and Technology Series 40. Springer International Publishing.

Thalheim, B. (2000). *Entity-Relationship Modeling: Foundations of Database Technology* (1st ed.). Springer-Verlag Berlin Heidelberg.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st ed.). Springer International Publishing.

Wachter, S. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *SSRN Electronic Journal*.

Wachter, S. (2018). The GDPR and the Internet of Things: a three-step transparency model. *Law Innovation and Technology*.

Wheeler, A. (2009). *Designing Brand Identity: An Essential Guide for the Whole Branding Team* (3rd ed.). John Wiley & Sons.

Wright, D., & Hert, P. D. (2012). *Privacy Impact Assessment* (1st ed.). Law, Governance and Technology Series 6. Springer Netherlands.