GDPR Compliance in the Design of the INFORM e-Learning Platform: a Case Study

Evangelia Vanezi, Dimitrios Kouzapas, Georgia M. Kapitsaki, Theodora Costi, Alexandros Yeratziotis, Christos Mettouris, Anna Philippou, and George A. Papadopoulos
Department of Computer Science
University of Cyprus
Nicosia, Cyprus
{evanez01,dimitrios.kouzapas,gkapi,tcosti02}@cs.ucy.ac.cy,alexis.yeratziotis@gmail.com
{mettour,annap,george}@cs.ucy.ac.cy

***Abstract*—The European Union General Data Protection Regulation (GDPR) governs personal data processing, aiming to ensure privacy in all systems handling such data. All systems that process personal data, including software systems are legally obliged to comply to all articles of the GDPR applicable to them. In this paper, the case study of an e-Learning software platform, namely the INFORM platform and its compliance to relevant articles of the GDPR is presented. The e-Learning platform was developed with the objective to host the educational material developed under the JUSTICE EU-funded project INFORM, targeting judiciary, court staff and legal practitioners, in order to provide free and open distance access to the content. In particular, the paper demonstrates the compliance of the platform with the articles and principles of: Data Minimisation, Lawfulness of Processing, Right to Erasure, Right of Access, Right to Data Portability, Right to Rectification and Security of Processing. By applying these articles, conformance to the provision for Data Protection by design is also achieved; the platform's software development process integrates the articles of the GDPR early in the development steps, from the specification and design phases. We show how the design process progressed and demonstrate the corresponding functionality within the e-Learning platform. The paper extracts a list of lessons learned and conclusions on software GDPR compliance.**

***Index Terms*—Privacy by Design, e-Learning, Case Study, GDPR**

I. Introduction

Personal data privacy protection in information systems is crucial in our era due to the widespread use of mobile, distributed and web applications that store and process personal data of an increasingly large number of users, in order to provide context-aware and personalized services. This need is reflected in the new EU regulation, the General Data Protection Regulation (GDPR) [1], applied since 25 May 2018 not only to organizations established in the EU but also to non-EU organizations that store and process personal data[1] of EU residents. GDPR defines several articles that can be mapped to software functionality and thus, from now on, all new systems need to incorporate such functionality. Furthermore, existing systems should be adapted in order to conform to these provisions.

e-Learning platforms store and process personal information of registered users and may also utilize this information to adapt to the needs of each user providing a personalized user experience [2], [3]. As all other systems incorporating user-management environments, such platforms need to be designed and developed in a way that will lead to their conformance to the data protection regulation and the emerging privacy needs.

However, it is still not clear how the GDPR articles can be precisely reflected in software systems and few works have addressed GDPR compliance. In this paper, we discuss certain GDPR provisions in regards to software and specifically in web environments in an attempt to draft guidelines towards GDPR compliance and personal data privacy protection. We examine the application of our analysis for the design and the development of an actual e-Learning platform, the INFORM Platform, a platform aimed to host and provide access to the content elaborated under the JUSTICE EU-funded project INFORM: *"INtroduction of the data protection reFORM to the judicial system"*. Similar mechanisms can be integrated in any system that includes a user-management module.

This is a first step towards integrating GDPR principles in the system design of some common software features. For many designers and developers these guidelines may be evident, as they may be already applying privacy requirements without being aware that they are essentially applying GDPR provisions. Hence, the objective of this paper is to demonstrate to designers and developers how we embedded some of the GDPR articles into the design of an e-Learning platform in an attempt towards compliance. In the case of experienced developers who have already been designing and integrating such features, our aim is to enable them to understand which of these features should be integrated in order to achieve compliance to GDPR provisions. For those who have no prior experience, our aim is to make them aware of GDPR provisions and their possible application. To the best of our knowledge, this is the first attempt towards mapping GDPR provisions to functionality related to user management in a software system presented from a more practical perspective.

[1]Personal Data is any information relating to an identified or identifiable natural person ('data subject')

978-1-7281-4844-1/19/18/$31.00

The rest of the paper is structured as follows. Section II presents previous works in the area whereas Section III introduces the GDPR articles we are focusing on. The objectives, the specifications, the design and some details about the implementation of the INFORM platform are presented in Section IV. Section V maps the GDPR articles under consideration to the way they were handled in the INFORM platform giving a view into implementation. Lessons learnt are summarized in Section VI, and, finally, Section VII concludes the paper. An appendix to the paper presents all GDPR articles.

II. Related Work

Information Privacy has been an issue of consideration and discussion for many years. The most widely used taxonomy for privacy based on potential privacy violations has been provided by Solove [4]. The link between the taxonomy of Solove and technology has been performed in [5], where the authors try to relate it with technology and refer to the terms of *data holder* and *data subject*. Privacy in the Internet Age in a more social context is discussed in [6] focusing on philosophical, political, and economic aspects of privacy.

Users' concerns about the privacy of their personal data while using context aware mobile applications are discussed in [7]. Such concerns have been addressed in various previous works that introduce specific mechanisms for protecting user privacy in different domains, e.g., in web applications, so that users define their privacy preferences for HTML5 applications that are adapted accordingly [8], or for reconciling developers' revenue and user privacy, e.g., in mobile applications in the form of a feedback control loop that adjusts the level of privacy protection on mobile phones [9].

A pattern catalog in order to help privacy regulation integration in organizations for systems comprised of business methods, human interaction and software is discussed in [10]. Another work discusses GDPR in the framework of socio-technical systems [11]. The authors also define a goal-based modeling language that can be used to model social aspects of the GDPR, including the relationship between data subjects, employer and employees.

GDPR's provisions for consent withdrawal and the right to forget are discussed in [12]. Privacy by design towards Data Minimisation is discussed in [13]. Privacy Design Strategies towards Privacy by Design are discussed in [14]. In [15], the use of static analysis to assist GDPR compliance of software systems is presented, whereas ENISA[2] has introduced a tool to assess Privacy Enhancing Technologies [16]. A more technical approach can be found in CARiSMA that focuses on model-based security analysis of IT systems [17]. This work has been motivated by the Article 25 of Regulation (EU) 2016/679 that concerns the protection of natural persons with regard to the processing of personal data. A use case on birth certificate registration in Municipality of Athens using the tool is presented. A model-based security engineering framework for supporting the system design based on BPMN (Business Process Model and Notation) and UML (Unified Modeling Language) is introduced in [18]. A case study of an Air Traffic Management system was used. An extension to BPMN 2.0 business process modeling language is also proposed in [19] with the aim of detecting conflicts between security and data-minimization requirements [19].

In relevance to related work, we do not offer a new management approach, but present our insight from the design of the INFORM platform considering GDPR compliance from the initial development stages. Listing and explaining how GDPR aspects are handled in a specific system design is an aspect that is missing from previous works.

III. GDPR Analysis Towards Software Compliance

Since GDPR was published in the Official Journal of the EU in May 2016, it became a subject of consideration and analysis for many disciplines. Many existing studies analyse GDPR, e.g., the work in [20] discusses the regulation principles and compares them to the principles of the previous directive. In [21], a complete analysis of all the provisions of the GDPR is presented, comparing them with previous legislation and providing notes and explanation on the new provisions impact. The Isle of Man Information Commissioner provided a series of guides about the GDPR, such as [22], explaining the Principle of Transparency and the [23] that explains the whole set of principles.

Only a number of GDPR Articles are applicable to Software Systems, and thus in this section we are displaying the analysis we conducted on them, in order to extract conclusion for the needed corresponding functionality in software systems and specifically in the context of an e-Learning platform. We will focus on analyzing this set of provisions specifically in relation to designing and implementing the software system. All other Articles are described in the Appendix in order to document our choice, by explaining what are the rest of the Articles about. Additionally, Article 32 *"Security of processing"*, defining that *"appropriate technical and organisational measures to ensure a level of security appropriate to the risk"* should be taken, will be explained in the context of the platform's design and implementation phases.

A. Data Minimisation

Data Minimisation is one of the principles related to the processing of personal data defined in Article 5 of the GDPR, stating that only personal data relevant and necessary for the processing purposes of each specific system should be asked, collected or in any way processed, except if the user *chooses* to provide more personal data.

This can be reflected in the framework of a web platform handling user data by separating the user profile fields in two subsets: mandatory fields and optional fields. For registering a user and for any subsequent actions, only fields declared as absolutely necessary for the processing purposes of the specific platform should be asked and stored in the system. Additional personal data (e.g., data that might be considered useful for providing a better user experience) should not be requested or

[2]https://www.enisa.europa.eu/

obtained from the user as obligatory. Instead, a user's profile may contain many more fields to be completed as optional ones and their completion will depend upon the user's own will to share the associated data. If the user decides to leave the optional fields empty, this will not block him from using the platform's functionality.

B. Lawfulness of Processing

Lawfulness of Processing is defined in Article 6, providing six potential lawful bases for processing. All systems should declare one of them to be their basis, in order to be able to proceed with storing or processing any personal data. We will be examining the cases of (i) **providing consent** defined in Article 6(1a) as *"the data subject has given consent to the processing of his or her personal data for one or more specific purposes"* and in Article 7, and of (ii) **performance of a contract** defined in Article 6(1b) as *"processing is 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"*. The above lawful bases implies that before any storing or processing of personal data occurs, the associated user should provide her consent freely and clearly, or confirm her intention to enter in a contract with the system, i.e., accept to provide the necessary data in order to receive specific services. Both should be evidently provided by their own will, not being at any way deceived e.g. by an already filled-in consent form or confirmation check box. Additionally, both should be provided based on the processing purposes of the platform described in the privacy policy and the terms of use. The notion of *purpose* constitutes a central notion of the GDPR, describing which personal data will be used for which purposes by which entities. This policy should be consisting of a precise and easy to understand, human-readable text, in order for the users to be able to fully comprehend its content before accepting it.

Most web platforms interacting with users should apply, depending on their functionality, either consent or performance of a contract, or both. For example, an e-store providing services and goods to a customer will be functioning on the lawful basis of performance on a contract and it can reflect this provision by not accepting or proceeding with any user's order unless confirmation was provided by the user for her acceptance of providing personal data in order to fulfill the requested services purpose, i.e., in this case, deliver the order. In contrast, if the e-store needs to ask users if they accept to keep their data stored for example for the purpose of informing them about offers, then a relevant consent from them will be additionally required.

C. Right to Erasure

Right to Erasure is defined in Article 17, as *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data"*. This right can be applied under different grounds.

A software system interacting with users should be able to provide each user with the option to be able at any given time to stop existing as a user of the platform, and to be able to withdraw his or her consent along with all of the personal data that by that time were stored and processed. Furthermore, after instructing a delete action no more personal data of the specific user should be able to be received or in any way processed, unless the user re-provides her consent or confirmation following the Lawfulness of Processing principle as explained in 3.B.

The Right to Erasure requires that all personal data will be removed from the system's database, unless some data is properly anonymised, thus no longer relating to an individual or being able to identify the previously associated person from that data, setting the storage and processing on those data outside the scope of the GDPR as explained in Recital 26 *"Not applicable to anonymous data"*.

D. Right of Access and Right to Data Portability

The Right of Access by the data subject is defined in Article 15 of the GDPR declaring that an individual should be able to obtain a confirmation from a system as to whether or not personal data concerning this person are being processed and, if they are, then the user should be able to obtain access to that data and to the additional information described in 15(a)-15(h). The Right to Data Portability is defined in Article 20 stating that a data subject should be able to obtain all of her own personal data processed in the system *"in a structured, commonly used and machine-readable format"* and that she have *"the right to transmit those data to another controller"*. Concerning a software system, a user that has her personal data stored and processed by that system should be able to easily ask for access to all of these data and with no undue delay the user should receive a packet, e.g., a compressed folder or a document, containing all the information related to her. It is important, that the user gets authenticated before receiving the information. The additional information defined in the Right of Access is considered static, or a mixture of static and dynamic information already known before the subject requests access and can be included in the same packet, or be published in a part of the system, where all users can read it e.g. in the Privacy Policy.

E. Right to Rectification

The Right to Rectification is defined in the GDPR in Article 16 stating that a data subject[3] should be able to require and obtain the rectification of inaccurate personal data or the completion of incomplete personal data. A software system handling user profiles and storing their personal data should provide users with the option to edit all of their personal data, either by providing new values to replace the previous ones, by adding values where no data was previously given e.g. in an optional field, or by removing values out of such fields.

[3]Data subject is any person whose personal data is being collected, held or processed by an organization.

Any changes done should be directly, or without undue delay, applied and presented.

F. Data Protection by Design

The Principle of Data Protection by Design and by Default defined in Article 25 of the GDPR, determines that *"the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures...in order to meet the requirements of this Regulation and protect the rights of data subjects"*. Privacy by Design was referred in [24] suggesting that *"Privacy by design is characterized by proactive rather than reactive measures"*, demonstrating a need for embedding compliance from the first steps of a software development, i.e., from the requirements phase, and a continuation of the efforts throughout the whole software engineering procedure. Following a traditional software engineering development methodology, during the requirements analysis phase, specially elaborated specifications should be drafted in order to describe GDPR necessary functions additionally to the actual software's requirements. Specifications should be reflected in the model created at the design phase, and implemented as functionality in the implementation step, whereas all GDPR-relevant aspects need to be verified and validated.

IV. The INFORM Platform

The INFORM Platform is a web platform for open and distance e-Learning, aimed to host and provide access to the content elaborated under the JUSTICE EU funded project INFORM[4]: *"INtroduction of the data protection reFORM to the judicial system"*. The platform includes functionality open to all users, namely a news blog, as well as additional functionality requiring users to be registered and logged in, in order to have access to it.

By incorporating user registration, it is also required to have a user management mechanism in order to create user accounts and profiles, store and process their personal information, authenticate them, and allow them to use the respective functionality. Functionality that is available only to registered users includes mechanisms for viewing a directory and the profiles of all platform users, as well as having access to all e-Learning material available on the platform including reading tutorials and interactive self assessments.

The material included in the specific platform is comprised of legal e-manuals and content related to the new data protection regulation, regarding the judicial system aimed towards three main target groups: Legal Practitioners, Judiciary and Court Staff. We do not provide more detail on the types of material available via the platform, as it does not affect the functionality we are focusing on in the context of this work. In the rest of the section we discuss the Specifications, Design and Implementation Phases of the platform.

[4]http://informproject.eu

TABLE I
INFORM Platform Specifications

	Specification	Type
(1)	User Registration	Project Requirement
(2)	User Login	Project Requirement
(3)	Password Reset	Project Requirement
(4)	Self-assessment	Project Requirement
(5)	Users' Directory	Project Requirement
(6)	Search for Users	Project Requirement
(7)	View User Profile	Project Requirement
(8)	Blog	Project Requirement
(9)	Access / Download Material	Project Requirement
(10)	Display Privacy Policy	Lawfulness of Processing
(11)	Edit User Profile	Right to Rectification
(12)	Edit User Account Information	Right to Rectification
(13)	Delete User Account	Right to Erasure
(14)	Access own personal data	Right to Access
(15)	Move own personal data	Right to Portability
(16)	Cookies Acceptance/Rejection	Data Min. / Consent

A. Platform Specifications

A basic definition of the required functionality of the platform was described during the proposal stage of the project in the respective document. Thus, during the specifications step, requirements were extracted from the document at first. Additionally, a specially elaborated questionnaire was prepared and distributed to the project's consortium members in order to precisely define a complete set of **project-based requirements**. The responses were gathered and analyzed in order to prepare the System Requirements Specification Document (SRS). The SRS was then enhanced with **GDPR-based required functionality**, extracted from our previous analysis on the GDPR articles and from the Privacy Policy of the platform.

The Privacy Policy[5] was custom drafted by the Law and Internet Foundation legal team, in Sofia, Bulgaria [25]. The policy defines the purposes and the processing of personal data by the e-Learning platform in compliance to the GDPR. It specifically states the Privacy by Design principle. The conformance to the Data Minimisation Article also defines and justifies the minimal data required for the platform to provide a user with a complete functional user experience. The policy explicitly states the purposes of processing and storing personal data in the platform in order for processing to be considered lawful. The erasure strategy and the anonymization strategy of certain data are also defined in the Privacy Policy. Finally, the Privacy Policy lists the Rights of the User in full compliance with the GDPR. These rights include the Right of Access, the Right of Rectification, the Right to Erasure, the Right to Withdraw Consent, etc.

In Table I, we list the software requirements based on: (1) the project specifications as determined by the application document and by the responses gathered from the questionnaires (rows 1-9), and (2), the additional requirements added because of the need for compliance to the articles of GDPR and the Privacy Policy (rows 10-16). Additionally, the principle of

[5]https://www.elearning-informproject.eu/data-processing/

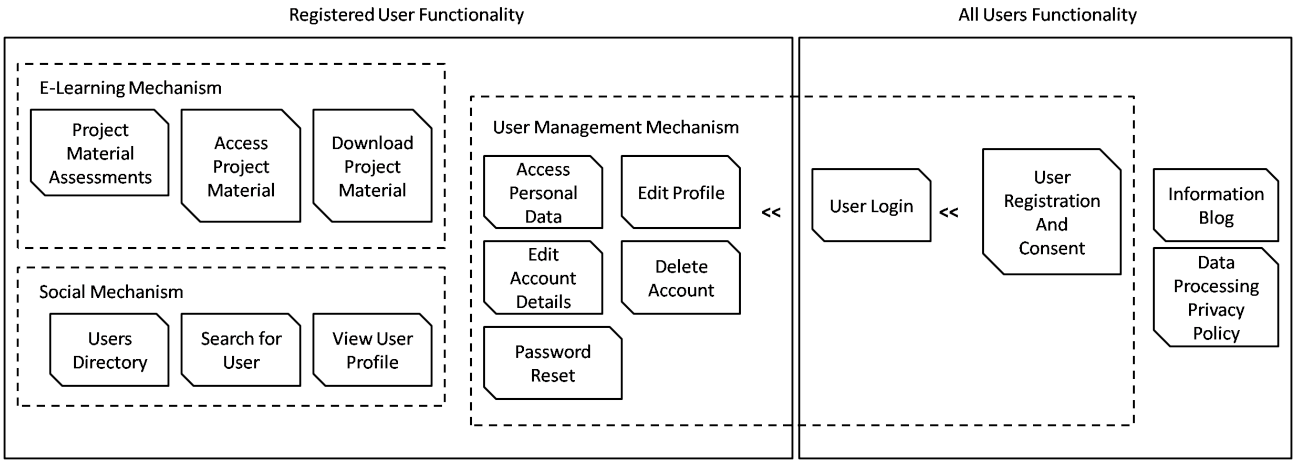


Fig. 1. INFORM Platform Architecture

"Data Minimisation" should be incorporated in all platform's functionality.

B. Platform Design

Architecture. In Figure 1, the architecture of the INFORM platform system is demonstrated. The diagram presents all the functionality of the platform including functionality available to all users, either *visitors* (users that are not logged in) or *registered users* (logged in), and functionality available *only to registered users*. In both sets, common web platform features are incorporated, such as the Information Blog. Further to that, a User Management System is embedded in the architecture in order to hold and manage the accounts of the registered users. In that part of the system, the following GDPR-related modules were added: *Access of Personal Data* (also representing Portability), *Editing of Account Details*, *Editing of Profile*, *Deletion of Account*, and *Consent* (or Confirmation) along with the *User Registration form*. Additionally, the *Data Processing Privacy Policy* is presented as a separate module, easily accessed by any user. In Figures 2 and 3 we use sequence diagrams to present the desired personal data flow from the user towards the platform data management functionality and the database, concerning the GDPR related provisions already discussed. The figures demonstrate the data flow concerning Data Minimisation, Lawfulness of Processing, Right to Rectification, Right to Erasure, Right to Access (and thus Right to Data Portability). Let us note that the User Profile User Interface (UI) entity represents the set of pages related to user information input, update or access.

In Figure 2, the flow is initiated by the User sending a set of data or a request towards the system. We first observe the data flow related to the registration of a new user: the user entity sends the minimal personal data set required along with his/her confirmation for acceptance of the processing towards the registration functionality. The data flow then proceeds towards the User Profile UI, and the Database, which in turn sends the set of profile data back to the User Profile UI. Subsequently, we observe the data flow related to editing the user profile. The user is sending new personal data directly to the User Profile UI, which then forwards them to the Database. A flow from the Database to the User Profile UI and from the User Profile UI to the User acknowledges the rectification. The third data flow sequence in Figure 2 presents the case where the user sends a delete request to the User Profile UI, which forwards it to the Database. The Database continues to send an Acknowledgment directly to the User. In Figure 3, the data flow related to accessing personal data of a user is displayed. The same flow represents both the cases of accessing or moving personal data. The user sends his/her request via email towards the platform admin, who then sends a request to the Personal Data Reporting functionality. The functionality then forwards the request to the Database and receives the data. It then forwards the report created with the data to the admin of the platform, who must then find a way to communicate them to the user, in a non automatic way.

Selected Tools. The Wordpress Content Management System (CMS) was selected to function as the basic core in the development of the INFORM e-Learning platform. The specific CMS was selected because of its user-friendly interface, the multiple responsive themes offered, the numerous available plugins and, most importantly, the possibilities provided by the fact that the CMS is open source: to add functionality on top of it with own coded plugins, or by customising its own code. Additionally, Wordpress sets the foundations necessary for security measures in a web platform. Lately, Wordpress has taken some measures towards GDPR compliance[6]. Nevertheless, the underlying Wordpress CMS implementation and the available plugins are not guaranteed to be GDPR compliant. A form of GDPR compliance for the INFORM platform is based on the assumption of trusting that the plugins of a popular and well maintained CMS, such as Wordpress, do not do anything more than their advertised specification. According to W3Techs[7], Wordpress is used by 33.1% of all websites,

[6]www.wordpress.org/news/2018/05/wordpress-4-9-6-privacy-and-maintenance-release/
[7]https://w3techs.com/technologies/details/cm-wordpress/all/all

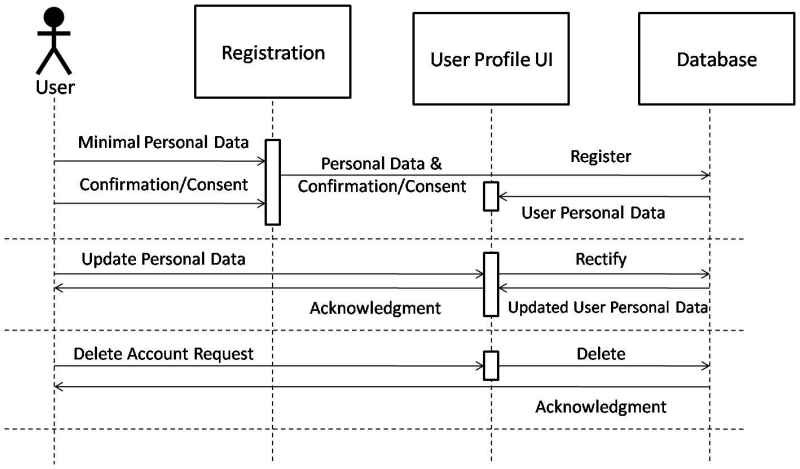


Fig. 2. INFORM Platform Sequence Diagram: GDPR-compliant Register, Rectify, and Delete

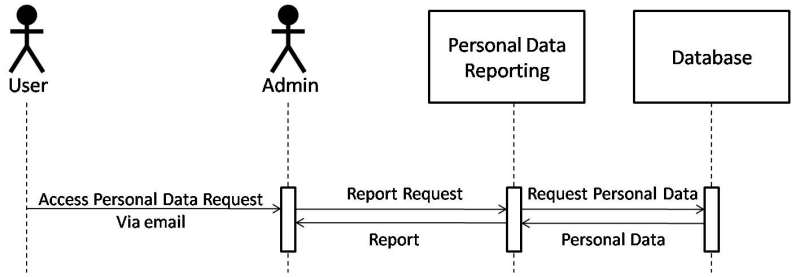


Fig. 3. INFORM Platform Sequence Diagram: GDPR-compliant Access and Portability

nowadays. Wordpress has been also studied a lot in scientific research, e.g., [26].

At this point, a study of the existing state of the art was conducted in order to identify available plugins implementing the required specifications drafted in the previous phase, namely project requirements and GDPR provisions, into Wordpress based platforms. Table II shows the above mentioned research results: in the first column the associated project requirement or GDPR associated functionality is noted and in the second column plugins identified as able and appropriate to cover that requirement are listed. Furthermore, in the second column we demonstrate additionally which functionality is covered by Wordpress itself, as from version 4.9.6. For demonstration purposes, some specifications were grouped, e.g., User Login, User Registration, and Password Reset are named as User Management Specifications. Similarly, User Directory, Search for Users, and View User Profile are named as Users Directory Specifications. Additionally, during the research, the plugins' code were examined to locate the points where the execution of the promised functionality is implemented, along with data offered from the Wordpress Plugins Directory, such as the number of active installations, the last update date, the compatible Wordpress version and the reviews. All above parameters were taken into account when deciding on the plugins to be used.

The Ultimate Member plugin was then selected to be used as the main plugin of the platform, due to the user management functionality it offers covering the main specifications, but also covering some of the GDPR requirements, namely "Edit User Profile", "Edit User Account Information" and "Delete User Account". The latter requirement is also covered by Wordpress in its latest updated version, with the difference that the plain Wordpress procedure is semi-automated: an admin has to manually request the deletion of a user by referring to his/her email address. Ultimate member plugin covers this requirement automatically, by allowing the user to select the "Delete" button in his/her account options. All specifications covered sufficiently by Wordpress and Ultimate Member plugin was decided to be exploited that way. Access to own Personal Data and Data Portability are included in the Wordpress new updated version. Providing and Withdrawing consent is implied by filling-in or emptying the optional fields, respectively. An independent plugin is needed in order to control cookies preferences, as Wordpress stores cookies for logged-in users[8].

C. Platform Implementation

As already described, the Wordpress CMS was used for the basis of our implementation, on which we have built by the addition of existing plugins and the creation of our own coded plugins for implementing all desirable functionality. Using

[8]https://codex.wordpress.org/WordPress_Cookies

TABLE II
STATE OF THE ART

Specification	Wordpress Plugin Name	Resource
User Management Specifications	(1) Ultimate Member Plugin by Ultimate Member Ltd et al.	https://ultimatemember.com/
Edit User Profile/Account	(1) GDPR by Trew Knowledge[1], (2) Ultimate Member Plugin	https://trewknowledge.com/[1]
User Directory Specifications	(1) Ultimate Member Plugin	
Self-assessment	* No suitable plugin	
Access / Download Material	* Wordpress Basic Core by Wordpress	https://wordpress.org/
Blog	* Wordpress Basic Core	
Privacy Policy	(1) Wordpress Updated Version, (2) GDPR	
Anonymize User Posts Information	* Wordpress Basic Core	
Delete User Account	(1) WP GDPR Compliance by Vans Ons[2], (2) GDPR (3) Wordpress updated version, (4) Ultimate Member Plugin	https://www.van-ons.nl/[2]
Access / Move own personal data	(1) GDPR, (2) Wordpress Updated Version	
Cookies Preferences	(1) GDPR, (2) WP GDPR Compliance	
Track Data Flow	(1) GDPR	

the basic Wordpress services we implemented the "Access and Download Material" functionality, the "Privacy Policy" page, the "Information Blog", as well as the "Export Data" functionality.

Furthermore, as decided during the design phase, the Ultimate Member plugin was embedded. All the User Management functionality, the Edit of User Profile and Account Information, the User Directory functionality, and the Delete User Account functionality were enabled and structured through the plugin. Our own coded plugins for the Self-assessments were developed using web technologies, i.e., HTML, PHP and JavaScript. At this point, where most of the desired functionality was already covered we identified a gap: The "Cookies Preferences" functionality. The GDPR plugin by Trew Knowledge[9], was selected for this feature. Using this plugin users can opt in or out of cookies that are being used on the site including Cookies that will be always active or required for the site to function and Cookies that can be activated or blocked based on the user preferences.

The same plugin provides the Telemetry Tracker functionality. This feature displays all data that is being sent outside of the platform's server to any other destination, indicating additionally the plugin or theme responsible, the file and line where the data is being sent, as some plugins can gather data and send them to outside servers. At this point, this is not needed in our platform, having installed only basic versions of plugins, as WordPress Plugin Repository does not allow plugins to do that, as long as they are not in a premium version. According to the Wordpress Plugins Directory guidelines[10] *"A stable version of a plugin must be available from its WordPress Plugin Directory page"*, meaning the basic free and open versions.

Regarding security, some measures additional to those implemented by Wordpress were taken, e.g., an SSL Certificate was purchased and added on the platform's domain for employing HTTPS instead of HTTP, i.e., the secure version of HTTP.

[9]https://wordpress.org/plugins/gdpr/

[10]https://developer.wordpress.org/plugins/wordpress-org/detailed-plugin-guidelines/

V. GDPR PROVISIONS IN THE IMPLEMENTATION OF THE INFORM PLATFORM

In this section we show the previously discussed GDPR articles in practice describing how they have been integrated into the e-Learning environment of the INFORM Platform. Please note that the Data Protection Privacy Policy of the INFORM platform is publicly available for any user to access through the interface of the platform.

A. Data Minimisation

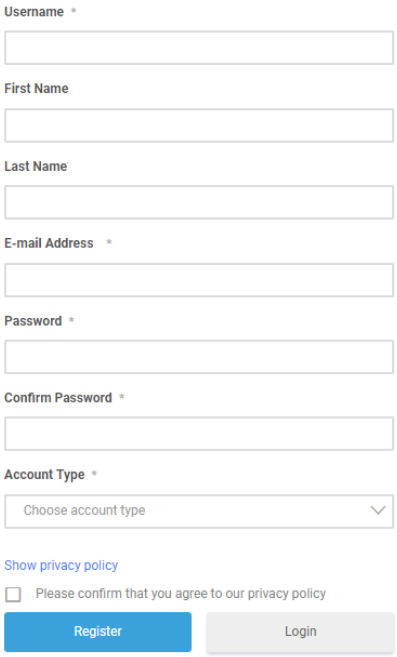
The INFORM platform complies to the Data Minimisation Article, which is applied by asking a user to willingly provide only the necessary personal data required for the purposes and the functionality of the e-Learning platform. These personal data are provided during user registration and are the following: i) username; ii) e-mail address; iii) password; and iv) account type. Username and password are absolutely necessary to enable the log in function of a user into the member's area of the platform. E-mail address is used to confirm the user's identity, necessary to complete registration. Account type, which is considered part of personal data because it declares a property of the user, is also necessary since it enables specific functions based on the user profile. Finally, first and last name can be given as optional information in order to offer better user experience, but not being obligatory thus conforming to Data Minimisation. Figure 4 shows the mandatory fields that request minimal data and are required to be filled for the purpose of registration along with the optional registration fields.

Beyond data minimisation, a user may optionally and willingly provide additional personal information for the purpose of a complete e-Learning profile. This information contains data, such as spoken languages, current organisation, education, biography, etc. There is no mechanism to store additional data (e.g. concerning the user session). Every user can also utilize the functionality available for visitors without providing any personal data. The purpose of storing and processing any of the aforementioned user data is described in the Privacy Policy of the INFORM platform.

TABLE III
MAPPING OF GDPR ARTICLES TO E-LEARNING PLATFORM FEATURES

GDPR Article	INFORM Platform Feature
Data Protection by Design - Article 25(1)	Privacy requirements detailed in system specification
Data Minimisation - Article 5	Minimal required fields for user input and data (e.g. user registration)
Lawfulness of Processing - Article 6	Asking and receiving user consent
Right to Erasure - Article 17	Delete user profile in database and relevant logs
Right to Access of Data - Article 15	Data retrieval and report creation upon user demand
Right to Rectification - Article 16	Profile updated by the user

Fig. 4. Minimum Required Fields in Registration



B. Lawfulness of Processing

As explained in the Privacy Policy, during the registration procedure, a user is considered to be taking steps towards entering a contract in order to benefit from the free provided services. These services are accessed from the e-Learning platform with all of its content and features. The INFORM platform complies to the Article of Lawfulness of Processing by requesting from the user to confirm her acceptance of storing and processing her personal data, in order to be able to use the platform's provided services, thus complying to the lawful basis of performance of a contract. The lawful basis establishment is deployed during the registration of a user to the INFORM platform; a user willingly fills the registration form with the personal data and moreover, the user is obliged to tick a check box declaring the user's acceptance for these data to be stored by the platform and processed as described in the Data Processing Privacy Policy of the INFORM platform. The Data Processing Privacy Policy is enunciated in clear, detailed, and precise human-readable text, and it describes all purposes and corresponding processing the personal data might undergo. If all personal data fields are filled properly and a confirmation is provided by the user by checking the relevant check-box, then by clicking on the registration button the data are stored. The specifications of the INFORM platform ensure that these data will by all means be processed following the Data Protection Privacy Policy. If the user never clicks on the registration button, then the personal data are discarded and they are never stored or processed. The registration form is depicted in Figure 4.

Additionally, when a user fills in the optional information of the registration form of the user profile, then it is considered that she is concurrently giving consent for their storage and processing as defined in the Privacy Policy. Let us note that consent is supported by providing users with the option to delete the optional data at any time. Furthermore, users are aware that their profiles, including the optional information, will be visible to other users, as this is clearly stated in the privacy policy.

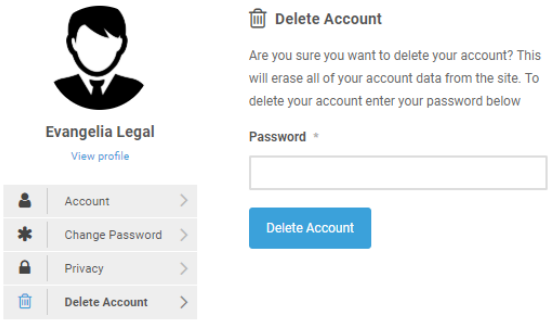
C. Right to Erasure

The Right to Erasure was integrated into the platform by providing the user with an option to delete her account at any given time, as explained in the Privacy Policy. When the Delete Account option is selected, the users are informed that their data will be deleted, and are called to confirm their identity by re-entering their password, as displayed in Figure 5. In order for the "Delete Account" functionality to be offered to the users, the Delete Tab should be enabled by the admin through the Ultimate Member plugin settings, and set to appear in users' account page. After a successful authorisation, the system proceeds with executing a set of database queries on all the relevant database tables, finding and deleting all the stored personal data associated with the specific user. No personal data should be kept after this procedure, unless their processing is for any reason subject to an exception rule, e.g., they are used for the public interest. The process for the erasure of data is described in detail in the data processing privacy policy.

Additionally, our own coded plugins are storing a set of Personal Data for each user, i.e. the text responses given to certain questions in the assessments, in one common database table for all three plugins. Thus, the "Delete Profile" functionality needs to be propagated to our own coded functionality triggering the deletion of any such set of data related to the specific user to be erased. To achieve this, the actual addition of code was done inside the Ultimate Member plugin functionality, where a delete query for the assessments responses

database table was written, in continuation to all other delete queries existing.

Fig. 5. Delete User Account option



D. Right to Access of Data and Right to Data Portability

Access to data provided by Wordpress allows users to export ZIP files containing their personal data, using data gathered by Wordpress and participating plugins. This is included by default in the "Tools" Side Menu, under the "Export Personal Data" option. A Double opt-in confirmation email system is added in this functionality for ensuring privacy protection. In the INFORM platform, a user may directly access a subset of her personal data, namely her profile personal data, stored in the system through the user profile page. However, other personal data are only accessible after a corresponding demand has been performed by the user. The INFORM platform is enabling the semi-automatic process offered by Wordpress for the user to access her personal data. As described in the Data Processing Privacy Policy, a user is required to contact the platform administration team via a specific e-mail format provided by the platform. In the email, the user must clearly state her demand for access, receive a confirmation for her personal data stored in the system, and, furthermore, receive the actual personal data. The administrators are then required to verify the user's identity, through the user's email, and use an automated administrator functionality to extract all the user personal data stored in the platform's database. The personal data are then compiled to a natural language report and are sent to the user. The automated procedure executes a set of database queries, based on the user identity to create the user personal data report.

Software systems with a larger user base are expected to have a complete automatic process, where upon request the process will verify the user, compile a report containing all the necessary personal user data and other information subject to the Right to Access of Data, and inform the user.

E. Right to Rectification

Right to Rectification is ensured by giving to all users the option to be able, at any given time, to edit their profile information as displayed in Figure 6, or to modify their account details as in Figure 7. This Right provides the user with the option to correct and update any information.

A user is able to edit all her personal data stored or asked except from the unique identifier credential, namely the user name. Specifically a user is able to give new values for her personal data information either the mandatory or the optional fields, to delete any previous given values leaving the field empty, for optional data, or complete data left in-completed by that time. Old information will be deleted, and the database tables will be updated with the new data through a set of database queries. All changes will be stored and presented to the user immediately. Similarly to the "Delete Account" functionality, for the "Edit Profile" functionality to be offered the Edit tab should be enabled by the admin on the Ultimate Member plugin settings.

F. Data Protection by Design

By integrating all above mentioned articles as explained, throughout the platform's software development process, from the specifications and design phases towards implementation of the system, conformance to the provision for Data Protection by design is also achieved.

Fig. 6. Edit User Profile Data

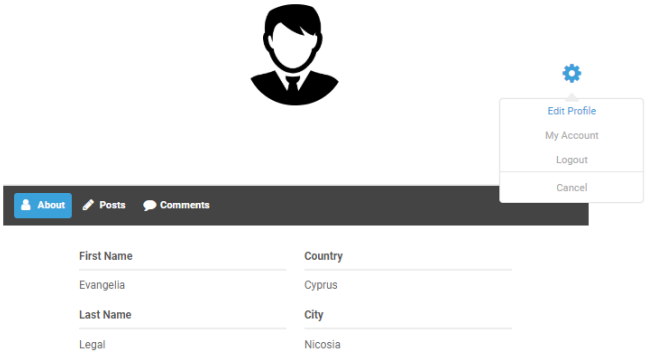
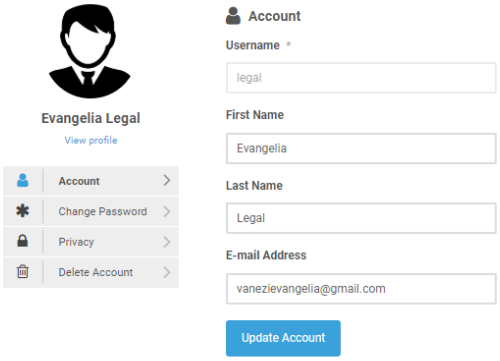


Fig. 7. Edit User Account Information



VI. Lessons Learned

The initial evaluation of the INFORM platform in terms of privacy protection and GDPR compliance has been performed with users in the University of Cyprus, in the Republic of Cyprus, in the framework of undergraduate and postgraduate courses, whereas exposure to the framework was provided to users during dedicated INFORM workshops. Future work will present evaluation results based on the exposure of the platform to a wider audience and external users. Based on the experience obtained via the implementation of the GDPR provisions for the INFORM platform, we summarize the main lessons learned that can be applied in the development of similar software systems:

1) Privacy and GDPR compliance should be considered throughout the whole software engineering process. It is not part of a single component but a required aspect of the system as a whole, serving also as an important quality attribute. In that respect, GDPR compliance planning should be initiated from the beginning of the system development and become part of relevant system functions. This is in essence captured in the Privacy by Design principle.
2) Receiving, storing and processing of any personal data of any user should only occur in the case the associated user willingly enters a contract or consents for the above mentioned, after being clearly informed about the respected processing purposes regarding her data. User consent is a requirement of GDPR, and for this reason it is important for provider to state their privacy policies clearly and in a user friendly manner.
3) Personal data required by the user as mandatory fields in order to use some of the platform's operations should be limited to minimum for fulfilling the described purposes, to which the user has consented or the services that the user entered into a contract in order to access them. Additional fields that may be useful but not essential, may be asked as optional fields. Communicating to the users that they will not be asked for more information than necessary is also important in that respect.
4) When a user needs to withdraw her consent or erase her account, this action should be easily initiated by the user and all data should be either deleted from the database and any other data stores or they should get anonymized, without any undue delay. It is important to provide to the user a way to perform this action via the system.
5) A user should be able, at any given time, to request to view the full set of personal data of her own that the software system is storing and in any way processing, and she should receive those data in a reasonable amount of time. A process needs to exist to support the above in all systems.
6) A user should be able to edit, change, fill or delete any information of those appearing in the user profile. For the mandatory information, the delete action should not apply. Changes should be immediately stored and presented.

Software GDPR compliance is eventually ensured when the code and the runtime environment that handles personal data is tested, verified/validated and eventually audited against the privacy policy requirements of the software. Implementations of platforms that are based on external modules need to provide guaranties of the GDPR compliance of these external modules. The GDPR compliance of the INFORM platform is based on a notion of trust that the plugins of a well-maintain and popular CMS, such as Wordpress, does exactly what their specification is describing.

VII. Conclusions

In this paper, we have presented a discussion and analysis of compliance with certain GDPR provisions towards the design and development of software systems. The under-study provisions have been applied in the framework of an e-Learning platform, namely the INFORM platform, that incorporates a user management mechanism and stores and processes personal data. We have presented the architectural diagram of the system showing the modules affected by privacy issues and GDPR. As an overall conclusion, we have introduced and presented a list of best practices deriving from our experience with the development of the GDPR compliance mechanisms. Let us note that, for more complex design decisions further investigation is required in order to examine and properly apply GDPR guidelines throughout the system architecture at both technical and design levels. Additionally, when a system is more complicated due to applying GDPR exceptions to the processing of data, such as collecting information for research purposes, then additional investigation should be done focused on the legal issues arising from this fact. As future work, we intend to expand on the compliance with more GDPR provisions, including regulation exceptions that complicate the functionality, introducing more elaborated mechanisms, whereas we intend to work on mechanisms that give users more freedom in the specification of their privacy policies, in relevance to service provider privacy policies.

Acknowledgment

The current publication is created within the project INtroduction of the data protection reFORM to the judicial system (INFORM). The project is funded by the European Unions Justice Programme (2014-2020) under Grant Agreement 763866. The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

References

[1] E. Parliament and C. of the European Union, "General data protection regulation," 2015, official Journal of the European Union.
[2] M. J. Rosenberg and R. Foshay, "E-learning: Strategies for delivering knowledge in the digital age," *Performance Improvement*, vol. 41, no. 5, pp. 50–51, 2002.
[3] F. J. García Peñalvo, M. Á. Conde García, M. Alier Forment, and M. J. Casany Guerrero, "Opening learning management systems to personal learning environments," *Journal of universal computer science: J. UCS*, vol. 17, no. 9, pp. 1222–1240, 2011.

[4] D. J. Solove, "A taxonomy of privacy," *U. Pa. L. Rev.*, vol. 154, p. 477, 2005.
[5] M. C. Tschantz and J. M. Wing, "Formal methods for privacy," in *International Symposium on Formal Methods*. Springer, 2009, pp. 1–15.
[6] S. Confer and K. Heuple, "A socialist theory of privacy in the internet age: An interdisciplinary analysis," *Philologia*, vol. 9, 2017.
[7] Z. Liu, J. Shan, R. Bonazzi, and Y. Pigneur, "Privacy as a tradeoff: Introducing the notion of privacy calculus for context-aware mobile applications," in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*. IEEE, 2014, pp. 1063–1072.
[8] G. M. Kapitsaki and T. Charalambous, "Privacysafer: Privacy adaptation for html5 web applications," in *International Conference on Web Information Systems Engineering*. Springer, 2017, pp. 247–262.
[9] I. Leontiadis, C. Efstratiou, M. Picone, and C. Mascolo, "Don't kill my ads!: balancing privacy in an ad-supported mobile application market," in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*. ACM, 2012, p. 2.
[10] D. Huth, "A pattern catalog for gdpr compliant data protection," 2017.
[11] M. Robol, M. Salnitri, and P. Giorgini, "Toward gdpr-compliant socio-technical systems: modeling language and reasoning framework," in *IFIP Working Conference on The Practice of Enterprise Modeling*. Springer, 2017, pp. 236–250.
[12] E. Politou, E. Alepis, and C. Patsakis, "Forgetting personal data and revoking consent under the gdpr: Challenges and proposed solutions," *Journal of Cybersecurity*, 2018.
[13] T. Antignac and D. Le Métayer, "Privacy architectures: Reasoning about data minimisation and integrity," in *International Workshop on Security and Trust Management*. Springer, 2014, pp. 17–32.
[14] J.-H. Hoepman, "Privacy design strategies," in *IFIP International Information Security Conference*. Springer, 2014, pp. 446–459.
[15] P. Ferrara and F. Spoto, "Static analysis for gdpr compliance." in *ITASEC*, 2018.
[16] E. U. A. for Network and I. Security, "A tool on privacy enhancing technologies (pets) knowledge management and maturity assessment," 2017.
[17] A. S. Ahmadian, S. Peldszus, Q. Ramadan, and J. Jürjens, "Model-based privacy and security analysis with carisma," in *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering*. ACM, 2017, pp. 989–993.
[18] Q. Ramadan, M. Salnitriy, D. Strüber, J. Jürjens, and P. Giorgini, "From secure business process modeling to design-level security verification," in *Model Driven Engineering Languages and Systems (MODELS), 2017 ACM/IEEE 20th International Conference on*. IEEE, 2017, pp. 123–133.
[19] Q. Ramadan, D. Strüber, M. Salnitri, V. Riediger, and J. Jürjens, "Detecting conflicts between data-minimization and security requirements in business process models," in *European Conference on Modelling Foundations and Applications*. Springer, 2018, pp. 179–198.
[20] T. H. D. Gabel, "Chapter 6: Data protection principles unlocking the eu general data protection regulation," 2016.
[21] U. I. C. Office, "Guide to the general data protection regulation (gdpr)," 2018.
[22] B. Fysseree, "A closer look at transparency," 2017, isle of Man Information Commissioner.
[23] B.Fysseree, "A closer look at principles," 2017, isle of Man Information Commissioner.
[24] A. Cavoukian, "Privacy by design," 2008, information Commissioner's Office.
[25] Law and I. Foundation. [Online]. Available: http://www.netlaw.bg/en
[26] S. K. Patel, V. Rathod, and J. B. Prajapati, "Performance analysis of content management systems-joomla, drupal and wordpress," *International Journal of Computer Applications*, vol. 21, no. 4, pp. 39–43, 2011.
[27] I. Consulting. [Online]. Available: https://gdpr-info.eu

APPENDIX

A. The GDPR Articles.

GDPR [1] is comprised out of 99 articles. The articles omitted in the analysis of section III are presented in this appendix. An existing online analysis by Intersoft Consulting [27] was used as the basis for the following.

- Articles 1-4 describe the regulation itself and provide definitions of terms referred to in the rest of the regulation, such as *'personal data'*.
- Article 8 refers to offering services directly to a child, and is not applicable for the specific platform target groups. Furthermore, Articles 9-11 refer to processing of special categories of personal data, which are also not applicable in our case.
- Beyond "Data Minimisation", Article 5 defines many other Principles such as lawfulness, fairness and transparency, and purpose limitation all of which are applicable to Software Systems, though not through the implementation, but rather if the system indeed keeps the promises given in the Privacy Policy, e.g. not using the data of the user in any other hidden purpose out of the scopes of the actual functionality.
- Articles 12-14 define the information that should be provided to the data subject. We conform to these Articles by providing this information in the Privacy Policy text.
- Article 19 is out of the scope of our platform, as it discusses details about the case of having third party recipients of the personal data handled by the system.
- Article 21, defining the *"Right to object"*, is applicable only when the lawful basis for processing is based on the public interest, or in the legitimate interests of the controller, none of which is the case in our e-Learning platform.
- Article 22 discuss *"Automated individual decision-making, including profiling"* which is also not applicable in our case.
- Article 23 states that each Member State *"may restrict by way of a legislative measure the scope of the obligations and rights"*. We are also not considering this article and abide to the GDPR text.
- Article 24 and articles 26-31 describe the role and obligations of the Data Controller(s) and Data Processor(s) of a system, in a rather general context, such as their cooperation with the supervisory authority when needed. Data Controller and Processor in our system along with the needed information about them are defined in the Privacy Policy of the platform, in a textual form.
- Articles 33 and 34 state that in the case of a Data Breach, the Supervisory Authority and the data subjects affected should be notified without any undue delay. This provision cannot be taken care of while implementing a system but its only applicable in the case of an actual data breach.
- Article 35, titled *"Data protection impact assessment"*, states that *"the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data"*, if *taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*. According to paragraph 3 of the Article, and to the UK In-

formation Commissioner's Office Guide[11] the INFORM platform does not fall into the cases likely to result in high risk, and is thus not required to carry out the assessment.
- Article 36 discusses further about the above mentioned assessment.
- Articles 37- 39 discuss the appointment and role of an individual as the Data Protection Officer in an organization. Articles 40-43 define the potential of drawing up Codes of Conduct and Certifications as means *"to contribute to the proper application of this Regulation"* by organizations.
- Articles 44-50 define how the transfer of personal data to third parties should be regulated. In our case, there is no transfer of personal data at all, as all data are handled by the platform.
- Articles 51-76 defines the conditions for the creation of Independent Supervisory Authorities in each Member State, responsible for monitoring the application of the regulation and their responsibilities.
- Articles 77-84 state the conditions, under which remedies and complaints can occur, and defines liability and penalties.
- Articles 85-91 discuss about how the regulation should be applied in specific processing situations. For instance, Article 88 refers to *"Processing in the context of employment"*.
- Article 92 discuss about adopting delegation acts in the regulation, and Article 93 states that *"The Commission shall be assisted by a committee."*
- The final provisions, Articles 94-99 discuss the relation of the regulation with the previous directive and other legal acts, and define the entry into force and application date of the GDPR.

From the above analysis, it is demonstrated how we ended up with the set of selected provisions to discuss in this paper, as applicable in the context of the INFORM e-Learning platform relating to design and implementation of the software.

[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/