



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

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

Shreyash Warang, Rutik Rain, Vinayak Wake, Prof. Waman Parulekar

Department of MCA, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India

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. Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

KEYWORDS: GDPR Compliance, E-Learning platform.

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 data¹ 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.

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. LITERATURE REVIEW

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].

1. *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 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.

2. *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 the purpose of informing them about offers, then a relevant consent from them will be additionally required.

3. *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"*.

4. *Right of Access and Right to 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.

5. *Right to Rectification:*

The Right to Rectification is defined in the GDPR in Article 16 stating that a data subject² 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. Any changes done should be directly, or without undue delay, applied and presented.

6. *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.

III. PROBLEM DEFINITION

The General Data Protection Regulation (GDPR) is a comprehensive data protection law implemented by the European Union (EU) to safeguard individuals' personal data and privacy. Compliance with GDPR is crucial for any organization handling EU citizens' data, including e-learning platforms. The INFORM e-Learning Platform, designed to provide educational content and training, must adhere to GDPR requirements to ensure the protection of user data, avoid legal penalties, and build trust with its users.

The INFORM e-Learning Platform currently faces challenges in achieving full GDPR compliance. These challenges include ensuring transparent data collection processes, obtaining explicit user consent, implementing robust data security measures, and providing users with rights to access, rectify, and delete their data. Non-compliance not only risks substantial fines but also undermines user trust and the platform's reputation.

IV. OBJECTIVE & SCOPE

General Data Protection Regulation impacts all organizations that process the personal data of EU citizens, including every company that offers goods and services or employs people in the EU even if an entity is based outside the EU.

GDPR applies to companies, associations, organizations, authorities and in some cases private individuals.

GDPR covers the whole European Union, and it applies to all the member states and covers the European Economic Area countries, such as Iceland, Lichtenstein, Norway, and the United Kingdom.

V. RESEARCH METHODOLOGY

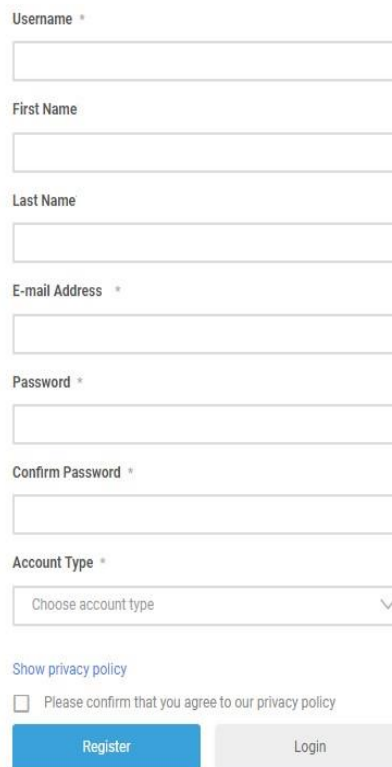
In this section we show the previously discussed GDPR articles in practice describing how they have been integrated into the e-Learning environment of the INFORM Platform. Please note that the Data Protection Privacy Policy of the INFORM platform is publicly available for any user to access through the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

1. *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.



The registration form contains the following fields and elements:

- Username ***: Text input field.
- First Name**: Text input field.
- Last Name**: Text input field.
- E-mail Address ***: Text input field.
- Password ***: Text input field.
- Confirm Password ***: Text input field.
- Account Type ***: Dropdown menu with the option "Choose account type".
- Show privacy policy**: A link.
- Please confirm that you agree to our privacy policy
- Register**: A blue button.
- Login**: A grey button.

2. Lawfulness of Processing

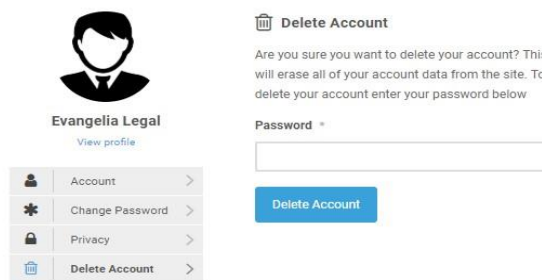
As explained in the Privacy Policy, during the registration procedure, a user is considered to be taking steps towards entering a contract in order to benefit from the free provided services. These services are accessed from the e-Learning platform with all of its content and features. The INFORM platform 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 above figure.

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.

3. *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 6. 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.



4. *Right to Access of Data and Right to 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.

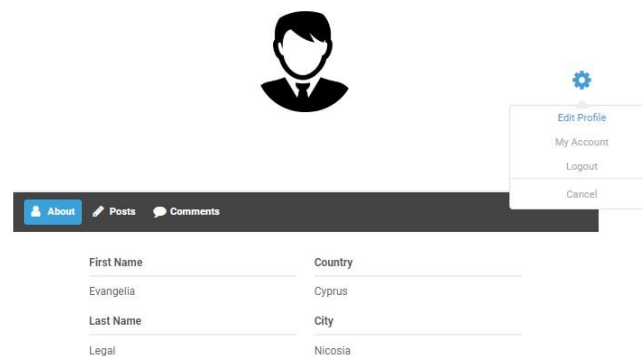
5. *Right to Rectification*

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.

6. 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.



VI. ANALYSIS AND FINDINGS Studies

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. Growing sophistication: Extortion tactics are becoming more targeted and personalized, increasing the pressure on victims to pay.

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.

VII. LIMITATIONS & FUTURE SCOPE

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.

VIII. CONCLUSION

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.

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. Garc'ia Penalvo, M. A. Conde Garc'ia, 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 sociotechnical 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 Metayer, "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. S. Ahmadian, S. Peldszus, Q. Ramadan, and J. Jurjens, "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. Struber, J. J" urjens, 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. Struber, M. Salnitri, V. Riediger, and J. J" urjens, "De-" tecting 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.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details