Research Article

Exploring the Effects of GDPR on the User Experience

Fernando Almeida [1]*, José Augusto Monteiro [2]

[1] University of Porto, INESC TEC, PORTUGAL
[2] Polytechnic Institute of Gaya, ISPGAYA, PORTUGAL
*Corresponding Author: almd@fe.up.pt

ARTICLE INFO	ABSTRACT
	With the implementation of the General Data Protection Regulation (GDPR) in the European Union, companies must be able to ensure that applications requesting the user to record personal data inform the user of the purpose for which the data collected is being collected. Furthermore, it is also necessary to ensure the data owner has given his/her explicit consent to the collection of these data and that such consent is recorded. This imperative has required a reworking of the interfaces of the applications. In this sense, this study seeks to explore the policies and practices that are being followed by organizations in designing interfaces. Four case studies were considered in the development of this study to explore this phenomenon in the dimensions of pragmatic hedonic processes of interface design, approaches to collect consent, and how personal data is managed. **Keywords:** GDPR, user experience, interfaces, data privacy, data management

INTRODUCTION

The General Data Protection Regulation (GDPR) is a new European legal framework that entered into force on May 25, 2018, in the European Union (EU). This regulation arose to strengthen the protection of personal data and sought to harmonize existing legislation in the EU Member States, creating the basis for the digital single market. It focuses on the protection, collection, and management of personal data, and applies to all EU companies and organizations that hold or process personal data in the EU Member States and even to companies in third countries that provide goods or services to people in the EU or monitor their behavior there.

The legislation introduced by the GDPR is directly reflected in the way users' data are treated. In the form of a legal device, it translates the right to be informed, the right to access, and the right to be forgotten, in the context of electronic platforms operating within the EU. It has therefore conferred greater autonomy on users in making informed decisions and easier control over access to their data (Poritskiy et al., 2019; Van Ooijen and Vrabec, 2019). The relationship between this new legislation and interface design and the user experience lies in the need to convey information and greater control over the user's actions in an easy-to-use and pleasant manner.

The new legislation has made it imperative to rethink the interfaces to incorporate the elements intended to inform the user about the processing of his data. Furthermore, it is also necessary to collect their agreement and (or) their consent to

their use (Hallinan, 2020; Mulder and Tudorica, 2019). Another change with an impact on interfaces is to reduce the collection of information on the user to that strictly necessary for each purpose (Crutzen et al., 2019). These changes in interfaces have an impact on their design, namely how the graphical elements are used and (re)organized to maintain or enhance the quality of the user experience.

Keeping these transformations in mind, guidelines have emerged proposing practices to be adopted in the design of new interfaces to ensure high standards in the user experience. The "Privacy by Design" model proposes the following six principles to be adopted (Barrett, 2019; Rostama et al., 2017): (i) choosing to participate: the user should decide to activate the collection and use of his/her data. The actions resulting from the option to participate should be easy to use, clear, and easy to understand; (ii) granular: in the activities whose user data will be processed, there should be verification of the explicit consent of the user. To assist the user, in each case where data collection takes place, it is recommended that a consent form be displayed in the context in which such collection takes place; (iii) withdrawable: users should be able to easily withdraw their consent at any time. The interface should be designed to understand the user's right and facilitate access to the withdrawal of consent; (iv) transparent: the user should be informed of which areas or departments of the organization promoting the data collection will have access to and process their data. It is argued that if the organization cannot clearly explain why it is collecting the data and how it will process it, then it should not collect it; (v) separation: the

law considers consent separate from agreement to the terms and conditions. For this reason, the user's action on these should be separated and communicated in such a way that it is clear to the user what they are accepting; and (vi) beneficial: in addition to the need to obtain the user's consent to the collection and processing of their data, it is argued that it should be clearly explained to the user how their consent will benefit their experience.

These principles, as well as others that will be proposed, result in a transposition of the general data protection regulation into a language that can be understood by the main operators in the technological field. This approach intends to maintain the appeal and ease of use of the products and services offered by companies. The window of opportunity to relate the User Experience (UX) with the GDPR arises through the identification and proposal of guidelines that transpose the legislation to the technology. However, this has been slightly scientifically explored, despite its undeniable relevance, since UX is expected to be a key element for users to understand and use the GDPR in their interactions with companies. In this sense, this study seeks to understand the models and guidelines that should be followed in designing interfaces for the applicability of the GDPR. It also seeks to analyze through four case studies with UX designers and Chief Information Officers (CIOs) how the process of interface development was changed by the emergence of the GDPR, and intends to explore how users can manage their consents and personal data using these interfaces.

This study is organized as follows: Initially, a theoretical contextualization of UX and its relevance in GDPR implementation is performed. After that, the methodology of the study is presented. Next, the main results of this study are reported and discussed. Finally, the main conclusions are drawn. In this last section, the limitations of this study are also explored, and some future work topics are suggested.

LITERATURE REVIEW

The Concept and Relevance of UX

The human being has always sought different forms of study about the user to facilitate the use of objects that are created over time. The way a person interacts and feels about the use of a product, system or service results in user perceptions about practical aspects such as usefulness, ease of use, and system efficiency (Karray et al., 2008). However, these experiences are necessarily subjective. Each person has a different experience when using an application. According to Shneiderman et al. (2016), this experience is influenced by human factors (e.g., ability to use the application, technical knowledge, motor skills, ability to read and interpret, etc.) and also by external factors (e.g., the environment, the context in which it is used, the time of day, etc.). But, although subjective, these experiences are projected by someone who has designed and conceived these interfaces.

Interface designers take responsibility for influencing user behavior through what they can produce. Bakker and Niemantsverdriet (2016) advocate that in developing a new technological solution a user-centered design methodology should be followed. This methodology should be focused on its objectives and should pay special attention to the user and how he/she will interact with the system, to offer a positive experience with the product/service. Once these needs are identified, it is the designers' responsibility to explore the way the solution will accommodate and respond to user behaviors.

A key framework in this area was developed by Moville (2004): The User Experience Honeycomb (UEH). According to this model, information is consumed according to the content of the information, the user accessing the information, and the context in which it is consumed. The components of the UEH include the following elements (Moville, 2004): (i) useful: the usefulness of the system should be questioned and it should be ensured that the final product/service creates value for those who use it; (ii) usable: ease of use is vital for the adoption of a system; (iii) desirable: elements relating to emotional design should be considered; (iv) findable, the user must be able to easily find what they are looking for; (v) accessible: to people with special needs; (vi) credible: users must trust the resources they are accessing; and (vii) valuable: applications must deliver value to stakeholders and contribute to increasing user satisfaction. Although the UEH has been designed for web environments, it has high applicability in other areas, especially in the design of user-centric interface projects. Yu (2018) states that in this type of project the experience of using a system has a high emotional load that adds value to the product.

From the HEU concept, it is concluded that UX is holistic, as it is necessary to consider all the details about the interaction between users and the product (Lee et al., 2018). This includes the perception of how the product works and whether it meets its goals, needs, and expectations in any context. UX is focused on addressing human needs beyond the instrumental, in which the quality of the product is enriched, and a holistic interaction is created. Furthermore, Saariluoma and Jokinen (2014) state that UX should also look at emotions as fundamental elements for the use of the product and explain ways to emphasize the experience produced by interactive products. Regardless of whether it is a service, product, website, electronic device, or object of personal satisfaction, the importance of UX is to ensure that the user always feels good throughout the user experience.

A poorly designed and developed design can result in a disaster for the company. As Chiosa and Anastasiei (2017) pointed out, a negative message about a bad user experience causes it to be transmitted exponentially. Consequently, it will bring negative results for the company. Any extraordinary effort that has been made in the computational process component may not be properly recognized by the user or have a negative impact if the interface is not pleasantly usable.

One of the most common errors in interface design identified by Cooper et al. (2007) is the lack of user-focused product planning. Often the focus of the company is on meeting the functional requirements of projects. This approach may lead to overly technological solutions that may be difficult to use (Thew and Sutcliffe, 2018). In contrast, Cooper et al. (2007) consider that the product should be developed in a way that enables users to achieve their goals. This will lead to more satisfied users and a higher probability

of purchasing a product or using a service proposed by the company (Marsh, 2018).

Finally, it becomes relevant to look at UX assessment approaches. The model proposed by Hassenzahl et al. (2010) is one of the most widely used and proposes an approach involving pragmatic aspects, which are related to the performance of tasks, and hedonic elements, which stand out for being related to emotions. This model considers UX as a broader concept than usability, which focuses only on pragmatic aspects. This view also confirms the initial approach of Thüring and Mahlke (2007), in which usability is one of the components of UX.

In this sense, this study assumes that hedonic aspects contribute directly to positive user experience, while pragmatic aspects make users feel competent when achieving their objectives. In line with this premise, the following research question was defined:

RQ1: What are the pragmatic and hedonic aspects that should be considered when designing an interface to meet the objectives established in the GDPR?

The Changes Imposed by GDPR on the UX

The GDPR affects how data is maintained and processed by organizations, but also how interfaces are designed. The solutions built by organizations need to help users make informed decisions about their privacy. Equally important is that users can intuitively consult their personal data and have control over it (Van Ooijen and Vrabec, 2019).

The individual rights are guaranteed in the GDPR in Chapter 3 (Art. 12-23). Eight principles can be identified: (i) right to be informed: provide transparency over how personal data is collected, stored, managed, protected, and processed; (ii) right to access: provide individual's access to their data and explain how supplemental data are used; (iii) reject automated decisions: comply with requests not to automate decision making using personal data; (iv) right to correction: correct any personal data if incomplete or inaccurate; (v) right to be deleted: remove personal data on request when there is no compelling reason to keep it; (vi) right to restrict processing: honor requested not to process an individual's data for specific purposes; (vii) right to data portability: provide copies of all stored data in a portable format; and (viii) right to stop processing: allow individual's data to be stored but not processed.

It is necessary to collect the consent of individuals to ensure compliance with these individual rights. The GDPR (Art. 7) explicitly indicates the conditions applicable to consent. The organization needs to obtain consent from the user, to receive any kind of communication or for the processing of personal data by the company. Therefore, all personal data processing activities including collection, storage, and sharing need to be based on explicit and active consent from an individual (Hoofnagle et al., 2019). A consequence of this process is that organizations must support complete content lifecycle management to ensure that individuals can review and revoke the consent given at any point.

The way this consent can be given is not unique. There are many approaches like collecting written statements from users, adopting checkboxes, collecting signatures, etc. However, for consent to be valid it has to comply with the following six rules (ICO, 2017: (i) it must be freely given; (ii) it must indicate the purposes of the processing, the type of activity, and the name of the controller; (iii) the conditions must be explicit and concise, and disconnected from other terms; (iv) it must be obvious and imply positive action by the user; (v) it must be confirmed in words; and (vi) its duration will depend on the context. Consistent with the last item, it is the responsibility of organizations to review and update consent when appropriate or its purpose is changed.

Several authors have proposed best practices to be followed by organizations to obtain explicit consent from users. Barrett (2019) states that the time of collection of personal data must be accompanied by a form for collecting the user's consent. This consent must be explicit and no pre-verified consent boxes or other default means of consent must be used (Van Ooijen and Vrabec, 2019). Hallinan (2020) stresses that the collection of consent must be granular. In this sense, rather than using a generalist option, the terms of consent should be clearly stated. Consent to Terms and Services agreements cannot be used as evidence for consent to the data collection. Similarly, opt-out consent is not valid since they are identical to the pre-ticked boxed model (Irwin, 2017). Users should also have the possibility to withdraw their consent at any time (Politou et al., 2018). The process of withdrawing consent should be as easy as giving consent. Finally, it is also essential that the consent given by the user is accompanied by expected benefits. For this reason, Barrett (2019) advocates that it should be explicit how the consent given by the user will benefit his experience in contacting the organization.

The collection and management of consent processes emerge as one of the most visible aspects and changes the way application interfaces must be designed. In this sense, this study established the following research questions:

RQ2: What approaches UX designers adopt to obtain consent from users?

RQ3: How can users manage their personal data?

METHODOLOGY

This study employs a qualitative methodology through four case studies. Two case studies are conducted with UX designers and intend to address the first two research questions, while to answer the third research question two case studies are conducted with CIOs. **Table 1** performs a mapping between the target audience, the lines of research, and the posed questions. In total 11 questions were prepared, the first 7 are for UX designers and the last 4 for CIOs. This approach ensures that the questions are relevant to the professional functions performed by each person within the organization. Four semi-structured interviews were conducted. According to Jamshed (2014), the semi-structured interview offers a compromise between the script of questions previously established and defined in **Table 1** with some level of autonomy and spontaneity on the part of the interviewer. In this sense, the interviewer takes the previously established guideline as the starting point but has some degree of flexibility to change their order or modify the way they are

Table 1. Mapping research questions

Target	Research questions	Questions
UX designers	RQ1: What are the pragmatic and hedonic aspects that should be considered when designing an interface to meet the objectives established in the GDPR?	Q1. What are the pragmatic aspects considered in designing an interface to meet the objectives of GDPR? Q2. What are the hedonic aspects considered in designing an interface to meet the objectives of GDPR? Q3. What is the relative importance of each?
UX designers	RQ2: What approaches UX designers adopt to obtain consent from users?	Q4. How are agreement and consent separated? Q5. What means are used to obtain consent? Q6. Who contributes to the definition of these means? Q7. Are any best practice manuals being followed?
CIOs	RQ3: How can users manage their personal data?	Q8. What is the personal information maintained by the applications (i.e., web and mobile)? Q9. Who defines the relevance of this information? Q10. How is this information accessed? Q11. How are historical data recorded and maintained?

Table 2. Profile of respondents

Case study	Description
CS1	He has over 5 years of experience as UX designer for web and mobile applications. He has worked as a freelancer and integrated teams specialized in software industry. He is currently a UX designer in a software company that develops collaborative solutions for the enterprise market.
CS2	He has more than 5 years of professional experience in web development and design. He occupies professional functions as a UX designer and web developer in a company responsible for the digital transformation of the sports industry.
CS3	He has more than 20 years of professional experience as a teacher in higher education and project manager. He is currently the CIO of a micro company providing services in the area of installation and maintenance of computer equipment.
CS4	He has over 10 years of professional experience as a software developer, project manager, and international business management. He is currently the CIO of a company that operates in the gamification market of business processes.

constructed. This is a fundamental element in this study because the effects of GDPR on the user experience is necessarily interdisciplinary and requires custom depth levels according to the background of the interviewee. Moreover, the interviews were conducted employing visual elements (e.g., examples of interfaces) that allow exploring elements of the interface and understanding the decisions made by the interviewees.

The use of case studies allows us to rely on theoretical propositions previously defined in the literature review, which also supports the data collection and analysis processes. Furthermore, Queirós et al. (2017) argue this approach is adequate in situations where the phenomenon and context are not clear. An important point was the choice of multiple and not unique case studies in this investigation. Precisely because we are not facing a classic context, in which the conditions of the business environment are previously known or established, the adoption of multiple study cases as indicated by Yin (2017) allows us to offer more comparative situations of analysis, thus contributing to increase the reliability in the triangulation of the material produced. The recommendations of Yin (2017) regarding the reliability and robustness aspects of the analysis through multiple study cases were also followed: (i) the validity of the construct through the definition of a protocol for the conduct of the study cases and semi-structured interviews; (ii) the internal validity through the understanding of the interdependence between the emergence of the GDPR and the need to adapt the interfaces to comply with the rules imposed by the GDPR; (iii) the external validity through the replication of the study in four companies; and (iv) the reliability through the collection of information from each company and discussion of the adopted practices.

The interviews were conducted following a dual interaction model. In the first phase, the interviews were distributed by email to the interviewees and were answered in writing. After that, an interview was conducted by Skype and Zoom to confirm and clarify the answers given, and to complement the analysis of the information with material provided by each company. **Table 2** provides an overview of each interviewee's profile.

The interviews were conducted between 12th May 2020 and 8th June 2020. After that, a thematic analysis was carried out to identify the themes found in each interview. After that, the themes were catalogued in two groups: convergent themes, and divergent themes. In the convergent themes, the themes that deserved consensus in both interviews appeared, while in the divergent themes, the answers that did not deserve consensus were mapped. In the case of the themes that did not deserve consensus, the contextual reasons that allow exploring this phenomenon were explored.

RESULTS AND DISCUSSION

Table 3 summarizes the findings of the thematic analysis. The data were grouped according to the 11 formulated questions. In total, 31 themes were identified, most of which result in convergent themes among the case studies.

RQ1: What are the Pragmatic and Hedonic Aspects that should be Considered when Designing an Interface to Meet the Objectives Established in the GDPR?

The clarity of the interface is fundamental for the user to interact with the technological solutions developed by companies. It must be clear to the user how he or she can

Table 3. Thematic analysis process

Question	Convergent theme	Divergent theme
Q1	Clarity of the interface Consequences of the actions Explanation of benefits	CS1: Required and optional data CS2: Speed CS2: Efficiency
Q2	Control over data User confidence	
Q3	Importance of both High interconnection and dependence	
Q4	Unbundled	
Q5	Checkboxes	CS2: Cookies and subscription forms
Q6	UI and UX designers	CS2: Project manager CS2: Legal office
Q7	Absence of a good practice manual Adoption of most used standards	
Q8	Minimization of information Accountability Independence of access type	CS4: 3rd party processing
Q9	Project manager Interdisciplinary teams	CS3: Multiple roles
Q10	Personal area Revoke consent	
Q11	Proportionality to objectives For legal purposes Definition of granularity	CS4: Data reminders

interact with the application and it must be explained the consequences that a certain action may have on the user's data. Furthermore, it is also important to show the benefits of the consents given by the users. Barrett (2019) emphasizes that showing the value of each user action will encourage users to give their consent. By doing so, the company can help each user to maximize his/her experience. The key question that emerges is how to balance the benefits for users by using their data to create a positive experience for them while maintaining credibility and trust in their data.

CS1 gives some examples of how to have a clear and simple interface. For example, it should be clear where and how a user can delete their account. Emails should also have the option of easy opt-in/opt-out access. Even in the case of cookies, it should be clearly stated which cookies are used and for what purpose. It is relevant to note that it is necessary to obtain the user's consent before storing cookies on the device or tracking them. A link to the page detailing the cookies used on the website should also be included. Recently Europe's top court made it clear that consent must be obtained before non-essential cookies, like tracking cookies for advertising purposes (Lomas, 2019). In the case of third-party cookies, the website is not responsible for managing them but must include a link to their privacy policy (Hu and Sastry, 2019).

CS2 highlights the role of speed and efficiency. As these are two generic terms, it is important to look at how they are applied in the context of GDPR. Speed can be seen as the time needed for the user to agree to the privacy policy and give consent to access and processing of their personal data. This is a factor that has an impact on the usability of the website and, consequently, on its acceptance rate. The study by Utz et al. (2019) tested different cookie consent notices with different choice mechanisms (e.g., binary, confirmation, categories, vendors) and found that the layout and interaction model had a significant impact on their acceptance. Finally, efficiency is a result of the way users achieve complete tasks. Therefore, at the same time as speed, a pleasant user experience should be offered.

This last point highlighted in CS2 launches the challenge of looking at the hedonic aspects of the interface. Control over data emerges as a key point and is highlighted in GDPR, since one of the major objectives of EU data protection rules is to give users greater control over their personal data, enabling them to surf the Internet with confidence. After the consent given by users, it should be possible to have full control over their data. This includes searching, changing, and removing personal data. Navigation panels should be clear and unambiguous to allow access to these features. User confidence should be progressively gained through clarity and ease of access to their personal data. According to Denning (2018), the hedonic aspects related to trust and credibility are achieved through the transparent use of user data.

In both cases, the importance of both the pragmatic and hedonic components was stressed. There are a high interconnection and dependence between the two components. Indeed, the perception of user confidence is strongly affected by the perception of the importance and value of their personal data. The study conducted by Kujala et al. (2011) demonstrates the relevance of these two factors but highlights that the hedonic component tends to gain more relevance than the pragmatic aspects as the user-product relationship evolves. Users need to feel how their data improve their user experience (Newman, 2017). Furthermore, Distler et al. (2020) refer to the importance of free consent as a key element for the user to trust the application. In this sense, browsing a website or app should consider that user consent is not always possible and therefore it is necessary to offer a minimalist interaction that allows the use of services in private mode. When this does not become possible, then it must be fully explicit how the personal data of users will be used by the company.

RQ2: What Approaches UX Designers Adopt to Obtain Consent from Users?

In both case studies, the distinction between agreement and consent is unambiguous. It is important to assure that both processes are unbundled. Accordingly, requests for consent are separated from the other terms and conditions. An essential factor is that consent must give people real choice and control over how their data is used. Consent is therefore only valid if it is freely expressed. However, as Machuletz and Böhme (2020) state, companies are tempted to maximize the number of consents to maximize the value of personal data and their potential use for secondary uses. However, this practice is uneven according to the principles of minimization and the objectives of collecting personal data for specific purposes.

The choice of how consent is collected can take several approaches. The GDPR does not define the form or format in which the information should be provided. Accordingly, each company implements different approaches depending on the benchmark practices followed by other companies and the originality of the web designer. For example, CS1 states that it favors the adoption of pop-up windows for the collection of consent, while in CS2 a specific area is maintained in the main window using checkboxes. Cookies and subscription forms are also procedures for collecting consent adopted in CS2. Regardless of the models adopted, users must actively opt for the collection, storage, and use of their data. However, checkboxes cannot be pre-checked, to assure that the user's choice is balanced (Utz et al., 2019). Additionally, good practices emerge in the design of these interfaces. Auka (2018) states it is essential that the user makes a well-informed decision as he/she progresses in the use of the system. Consequently, the user's decision should not be biased, and to this end, all options should have the same visual prominence.

UI and UX designers are pointed out as the determining roles for defining the means of collecting consent. This reveals a great concern for the hedonic aspects of interface construction. In CS2 other roles emerge such as the project manager and the legal office. This emerges due to the company's concern to assume GDPR as a strategic element in the early stages of project design. Therefore, in the collection of requirements with the client, the mechanisms for the collection of personal data are already explicitly defined. Besides the project manager, the legal office has a decisive role in defining and verifying the necessary information to be collected.

In both cases of study, it is not adopted a good practice manual. However, from the interviews carried out, it was evident that both considered the relevance of their existence to reduce the time and risks associated with this process in the future. Both companies adopt the standards most used in the area, although there is no systematic process for identifying and collecting these good practices. There is an informal process of collecting these good practices from the competition analysis, but it is not properly sustained in the medium and long term.

RQ3: How can Users Manage their Personal Data?

The personal information that becomes necessary to maintain depends on the context of the application and its objectives. The type of access should not be a determining factor in defining or restricting the type of personal data that will be shared. Regardless of the type of access, the personal data of users will be unchanged. The principles of minimization and proportionality are fundamental to ensuring that the data are only used for the purposes for which they will be processed. The aim is to decrease the amount of data by collecting only those data that are essential for the application. Hoofnagle et al. (2019) maintain this principle should be applied to customers and employees. In CS4 the relevance of informing the user of the entities or companies with which the personal data will be shared is highlighted. However, the privacy challenge does not stop at this dimension alone and is also increased by the growth of the Internet of Things (IoT). The combination of information and access recorded on smart devices poses challenges to privacy as it generates a set of behaviors that can be used by cybercriminals (Almeida and Lourenço, 2020).

The relevance of the data to be collected is a strategic issue and should be defined in the early stages of project development. The project manager is a central player in this process and takes on the challenge of bringing together an interdisciplinary team capable of conceptually understanding the legal norms, but also of being able to assess their applicability to the organization in which the project is developed. At this level, Todorovic et al. (2018) suggest the creation of interdisciplinary teams consisting of three key roles: (i) expert for legal issues; (ii) expert for organizational issues; and (iii) expert for technical issues and information security. However, in CS3 it was highlighted that the available resources do not always allow for the construction of teams with this degree of comprehensiveness, and often the role of expert for legal issues and information security specialist is performed simultaneously by the same person.

The user's personal data information is accessed in his/her personal area. This was an area of application modelling that had to be reformulated. Li et al. (2019) advocate that the global design culture is being changed motivated by the emergence of the GDPR with a more user data privacy-focused approach. Users should also be able to revoke consent from their personal area. As Politou et al. (2018) point out, revoking consent should be as easy as granting it. Therefore, options for revoking consent should not be hidden or difficult to find.

Historical data shall be kept in accordance with the proportionality of their necessity. Regardless of the personal data collected, it shall be kept for as short a time as possible. In this period, the time necessary for any legal obligations determined by natural law or legal or fiscal matter shall be considered. Furthermore, both companies have stated the importance of setting deadlines for erasing or reviewing the stored personal data. CS4 highlights this approach allows them to increase user reliability for their applications, as "just-in-time" alerts are issued when it is necessary to collect personal data. This approach implements the granularity principle as advocated by Barrett (2019), and Hallinan (2020), where personal data should be requested only when necessary.

CONCLUSIONS

In designing an interface to ensure compliance with the GDPR, pragmatic and hedonic aspects must be simultaneously considered, due to the high interconnection and dependence between them. Together with clarity in the interface, the consequences of users' actions should be fully explicit, and the benefits brought by providing their personal data should be explained. It is also essential that the user has control over his data, which will contribute to an increase in user confidence.

The consent and agreement must be separated. Explicit consent is required for the processing of any personal data. Consent to the use of personal data needs to be informed, specific, and unambiguous. To this end, the description of the scope and purposes of personal data must be short and direct. There are several ways to request this consent, namely by combining the adoption of cookies, subscription forms, and checkboxes. The means used to collect this information are typically not mapped in a good practice manual but are obtained informally by looking up the most commonly used standards in the field.

The application access device is not a determining factor in defining the type of personal data required for the operation of applications. It is essential to follow the principles of minimization and proportionality to ensure that the minimum amount of data necessary for the operation of the application is collected. The definition of personal data to be collected is a strategic decision that must be taken in the early stages of project development. Interdisciplinary teams with competence in the legal, technical, and cybersecurity areas must participate in this process. Finally, access to personal data must be intuitive, to enable the user to know its purpose, when it has been used, and to revoke his/her consent when requested. Meanwhile, the data must be kept in the application as minimal time as possible.

This study offers essentially practical contributions by exploring the models and good practices that should be adopted in the development of interfaces that follow the GDPR principles. This information is particularly relevant for the business sector, especially for UX designers and CIOs facing the challenges of building interfaces that comply with the rules established by the GDPR and the need to establish policies for personal data management that allow the control over their personal data. This study also has some limitations. Firstly, the approach adopted to case studies is interesting to know in-depth the challenges of each organization but brings more limitations in the generalization of its results. Therefore, and as future work, and after this exploratory study in the area, it becomes pertinent to carry out a complementary quantitative study that allows us to have a more comprehensive view of the practices adopted by the organizations. Another limitation is that the study did not intend to focus on the challenges posed to organizations according to the sector of activity. In this sense, it is expected that the challenges posed to organizations according to their sector of activity will be different. For example, a professional training company will have different challenges from a company offering an e-commerce platform. Exploring the specific challenges in the design of interfaces considering the sector of activity of these companies is another relevant topic for future work.

REFERENCES

Almeida, F. And Lourenço, J. (2020). Privacy and Security Challenges in the Internet of Things. In Khosrow-Pour D.B.A., M. (Ed.), *Encyclopedia of Criminal Activities and the Deep Web* (pp. 749-762). IGI Global. https://doi.org/10.4018/978-1-5225-9715-5.ch051

Auka (2018). *Best UX practices for GDPR compliance*. Available at: https://medium.com/@AukaPay/best-ux-practices-for-gdpr-compliance-563b73362095

Bakker, S. and Niemantsverdriet, K. (2016). The Interaction-Attention Continuum: Considering Various Levels of Human Attention in Interaction Design. *International Journal of Design*, *10*(2), 1-21.

Barrett, C. (2019). *What does GDPR mean for UX?* Available at: https://uxdesign.cc/what-does-gdpr-mean-for-ux-9b5ecbc51a43

Chiosa, A. R. and Anastasiei, B. (2017). Negative word-of-mouth: exploring the impact of adverse meassages on consumers' reactions on facebook. *Review of Economic & Business Studies*, *10*(2), 157-173. https://doi.org/10.1515/rebs-2017-0059

Cooper, A., Reimann, R. and Cronin, D. (2007). *About Face 3: The Essentials of Interaction Design*. Michigan, Wiley.

Crutzen, R., Peters, G. Y. and Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health*, *34*(11), 1347-1357. https://doi.org/10.1080/08870446.2019.1606222

Denning, S. (2018). *GDPR & the User Experience*. Available at: https://uservision.co.uk/thoughts/gdpr-the-user-experience/

Distler, V., Lallemand, C. and Koenig, V. (2020). How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior*, *106*, 106227. https://doi.org/10.1016/j.chb.2019.106227

Hallinan, D. (2020). Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sciences, Society and Policy*, *16*(1), 1-18. https://doi.org/10.1186/s40504-019-0096-3

Hassenzahl, M., Diefenbach, S., e Göritz, A. (2010). Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers*, *22*(5), 353-362. https://doi.org/10.1016/j.intcom.2010.04.002

Hoofnagle, C. J., Van der Sloot, B. and Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 69-98. https://doi.org/10.1080/13600834.2019.1573501

Hu, X. and Sastry, N. (2019). Characterising third party cookie usage in the EU after GDPR. *WebSci '19: Proceedings of the 10th ACM Conference on Web Science*, 137-141. https://doi.org/10.1145/3292522.3326039

ICO (2017). *Consultation: GDPR consent guidance*. Available at: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Irwin, L. (2017). *GDPR: When do you need to seek consent?* Available at: https://www.itgovernance.eu/blog/en/gdpr-when-do-you-need-to-seek-consent

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, *5*(4), 87-88. https://doi.org/10.4103/0976-0105.141942

Karray, F., Alemzadeh, M., Saleh, J. A. and Arab, M. N. (2008). Human-Computer Interaction: Overview on State of the Ar. *International Journal on Smart Sensing and Intelligent Systems*, *1*(1), 137-159. https://doi.org/10.21307/ijssis-2017-283

Kujala, S., Roto, V., Väänänen-Vainio-Mattila, K. and Sinnelä, A. (2011). Identifying Hedonic Factors in Long-Term User Experience. In *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces*, Milano, Italy, 1-8. https://doi.org/10.1145/2347504.2347523

Lee, H. J., Lee, K. K. and Choi, J. (2018). A Structural Model for Unity of Experience: Connecting User Experience, Customer Experience, and Brand Experience. *Journal of Usability Studies*, *14*(1), 8-34.

Li, H., Yu, L. and He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1-6. https://doi.org/10.1080/1097198X.2019.1569186

Lomas, N. (2019). *Europe's top court says active consent is needed for tracking cookies*. Available at: https://techcrunch.com/2019/10/01/europes-top-court-says-active-consent-is-needed-for-tracking-cookies/

Machuletz, D. and Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. In *Proceedings on Privacy Enhancing Technologies, Virtual*, 481-498. https://doi.org/10.2478/popets-2020-0037

Marsh, S. (2018). *User Research: A Practical Guide to Designing Better Products and Services*. London, UK: Kogan Page.

Morville, P. (2004). *User Experience Design*. Available at: https://semanticstudios.com/user_experience_design/

Mulder, T. and Tudorica, M. (2019). Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law*, *28*(3), 261-274. https://doi.org/10.1080/13600834.2019.1644068

Newman, D. (2017). *Improving Customer Experience Through Customer Data*. Available at: https://www.forbes.com/sites/danielnewman/2017/04/04/improving-customer-experience-through-customer-data/#4e497f144e64

Politou, E., Alepis, E. and Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), 1-20. https://doi.org/10.1093/cybsec/tyy001

Poritskiy, N., Oliveira, F. and Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, *21*(5), 510-524. https://doi.org/10.1108/DPRG-05-2019-0039

Queirós, A., Faria, D. and Almeida, F. (2017). Strengths and Limitation of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*, *3*(9), 369-387.

Rostama, G., Bekhradi, A. and Yannou, B. (2017). From privacy by design to design for privacy. In *Proceedings of the International Conference on Engineering Design (ICED)*, Vancouver, Canada, 1-11.

Saariluoma, P. and Jokinen, J. P. (2014). Emotional Dimensions of User Experience: A User Psychological Analysis. *International Journal of Human-Computer Interaction*, *30*(4), 303-320. https://doi.org/10.1080/10447318.2013.858460

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N. and Diakopoulos, N. (2016). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. London, UK: Pearson.

Thew, S. and Sutcliffe, A. (2018). Value-based requirements engineering: method and experience. *Requirements Engineering*, *23*, 443-464. https://doi.org/10.1007/s00766-017-0273-y

Thüring, M. and Mahlke, S. (2007). Usability, aesthetics and emotions in human–technology interaction. *International Journal of Psychology*, *42*(4), 253-264. https://doi.org/10.1080/00207590701396674

Todorovic, I., Komazec, S., Krivokapic, D. and Krivokapic, D. (2018). Project Management in the Implementation of General Data Protection Regulation (GDPR). *European Project Management Journal*, *8*(1), 55-64. https://doi.org/10.18485/epmj.2018.8.1.7

Utz, C., Degeling, M., Fahl, S., Schaub, F. and Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, UK, 973-990. https://doi.org/10.1145/3319535.3354212

Van Ooijen, I. and Vrabec, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*, 91-107. https://doi.org/10.1007/s10603-018-9399-7

Yin, R. (2017). *Case Study Research and Applications: Design and Methods*. Thousand Oaks, California: SAGE Publications. https://doi.org/10.1002/col.22052

Yu, E. (2018). Designing for Value: Insights from the Emotional Appraisal Approach to Understanding User Value. *The Design Journal*, *21*(2), 185-207. https://doi.org/10.1080/14606925.2018.1407540