


How does GDPR (General Data Protection Regulation) affect persuasive system design: Design requirements and cost implications

Xiuyan Shao  [0000-0001-6550-9025] and Harri Oinas-Kukkonen

Oulu Advanced Research on Service and Information Systems,
University of Oulu, P.O. Box 3000, 90014 Oulu, Finland
{xiuyan.shao,harri.oinas-kukkonen}@oulu.fi

Abstract. In May 2018, GDPR came into effect in the European Union, placing additional requirements for data sensitive companies on data protection. For persuasive systems which deal with users' data, taking GDPR into consideration in the design phase is necessary. This paper analyzes and summarizes the requirements by GDPR and discusses how they affect persuasive systems design in terms of design requirements and cost implications.

Keywords: GDPR, data protection, Persuasive Systems Design, cost

1 Introduction

The European GDPR is new legislation on data protection in the European Union (EU). The GDPR strengthens the protection of personal data of individuals in the EU and improves the level of harmonization across the EU. The impact of the GDPR on European and non-European organizations is significant. However, many organizations are still unaware of the new legislation and its complexity, while others are still focusing on the first implementation stage. Non-compliance may expose these organizations to newly introduced high sanctions. Persuasive and behavior-change support systems, which aim to promote change in different domains (including health, safety and security, environmental sustainability, energy conservation, marketing, and education), are data-sensitive by definition [1]. For this reason, the GDPR should be taken into account in organizations which develop persuasive systems. This paper discusses the GDPR from the viewpoint of systems design and costs, and it suggests how development of persuasive systems should tackle these new challenges.

2 Data protection and essentials of GDPR

To harmonize data protection, Data Protection Directive 95/46/EC (hereafter DIR95) has been a central legislative instrument for personal data protection in the EU. DIR95 regulates the protection of individuals with regard to personal data processing and free movement within the EU. In 2002, Privacy and Electronic Communications (EC

Directive 2002/58/EC) [2] was introduced to DIR95, adding new concerns of the processing of personal data and the protection of privacy in the electronic communications sector. For example, the directive regulates confidentiality, unsolicited communications, and processing of billing, traffic, and location data [2].

After more than two decades, DIR95 no longer provided the degree of harmonization that is required among the EU member states or the efficiency to ensure the right to personal data protection in the present-day digital environment [3]. The inadequate harmonization put Europe at a disadvantage in the global competition with other countries, such as the United States and China [4]. The EU's data protection framework had a fundamental reform. The reform consisted of two instruments: the GDPR and the directive on protecting personal data processed for the purposes of prevention, detection, investigation, or prosecution of criminal offences and related judicial activities. The GDPR points out the role of the FIP (Fair Information Practices)-based Privacy by Design (PbD) principles [5] and obliges companies to integrate these principles into their business processes [6].

A major departure from current practices is embodied in the GDPR. The GDPR gives primacy to purpose: Data may be collected and stored only when (1) end-users have consented, often explicitly, to the purposes for which that data is collected and (2) the collected data is necessary for achieving these purposes, and the data must be deleted when those purposes are no longer applicable [7]. To highlight this, the GDPR emphasizes these requirements in its notions of purpose limitation and data minimization, its treatment of consent, and the right to be forgotten.

3 Impact of GDPR on persuasive systems design

The implementation of the GDPR indicates the needs for various actions, planning and assignment of new responsibilities, which may have significant impacts on companies in using their resources and may demand the acquisition of new expertise. Eleven requirements can be recognized and specified for persuasive systems design, and they can be categorized into: (1) design requirements, (2) cost implications. (See Table 1.)

Table 1. Impact of GDPR on persuasive system design

Impact categories	Explanation
Impact on design requirements	1. Privacy by design and default
	2. Providing information to data subjects
	3. Ensuring individuals' right to be forgotten
	4. Ensuring individuals' right to data portability
Impact on costs	1. Data minimization
	2. Obtaining consent
	3. Data processing in international contexts
	4. Demonstrating compliance
	5. Obligation to report breaches within 72 hours
	6. Profession of Data Protection Officer (DPO)
	7. Documentation of processing activities

3.1 Design requirements

(1) Privacy by design and default. To ensure compliance with the GDPR and protection of data subjects' rights, companies are obliged to implement technical and organizational measures and procedures. Privacy should be considered not only in the business processes, but also throughout systems development. The influence on persuasive systems design would be the implementation of technical measures to ensure compliance with the GDPR. Yet, the definition of technical measures is not fully clear in this context. It would be best to consider such technical measures already in the systems planning phase, rather than after the fact. Thus, in order to satisfy the "privacy by design and default" requirement, privacy-related software features may have to be carefully designed into the persuasive system under development.

(2) Providing information to data subjects. The information that companies need to provide to data subjects includes processing operations, data security measures, the legal basis for processing, the data subjects' rights, and the companies' legitimate interests. The way of providing such data should be transparent, easily accessible, and understandable, especially when the data subject is a child. Procedures and mechanisms for exercising the data subjects' rights are also required, i.e. companies have to arrange for the means of responding to information requests according to GDPR requirements. There can be two ways to meet this requirement. First, information provision can be embedded in the information system, i.e. introducing a new software feature that communicates with data subjects about processing operations, data security measures, and so on. Another option is to have other channels (such as emails) to communicate with data subjects about the required items. Adding a software feature requires more planning in the design phase, while the email or other extra communication channel option are likely to cost more in the long run.

(3) Ensuring individuals' right to be forgotten. Companies are obliged to delete data subjects' personal data anytime they request it, which demands implementing processes and technical means for the deletion within time limits. These include ways of informing third parties about the deletion request, while processing personal data. Ensuring the right to be forgotten requires documentation of the data, how it is stored and with which parties it is shared. A software feature embedded in the system, which erases users' data per user request, could be developed. If the data has been shared with third party, making sure that third party deletes the data would require communication and coordination, which takes time and expense.

(4) Ensuring individuals' right to data portability. Companies are obliged to provide data subjects with an electronic copy of their data upon request. They must ensure that the personal data collected for processing is in a consistent format to facilitate its further use by the data subject and its transmission to other service providers' processing systems. A software functionality could be developed that would be embedded in the persuasive system. This could be implemented in such a way that when data subjects request to have an electronic copy of their data, the persuasive system generates the copy so that data subjects can download it by themselves. The format of data ought to match existing standards.

3.2 Cost implications

(1) Data minimization. The principle of limiting data usage requires limiting personal data processing to the absolute minimum necessary. Profiling customers' needs to inform data subjects about the reasons and the need for profiling would add more documentation and communication work with customers, which would not necessarily influence persuasive systems design. However, this influences the cost of developing persuasive systems. New obligations may also be introduced when planning data collection and processing. For example, collecting data from children needs verification of age and consent from parents or custodians.

(2) Obtaining consent. The data subject's consent is required for utilizing personal data. Demonstrating that the data subject has consented to the processing is important. All relevant information about the processing should be contained and presented clearly when requesting for consent. The request should be clearly distinguishable from other information, such as contracts. To obtain consent, a software functionality could be developed so that when users start to use the system, the system pops out a consent letter on which users must choose "yes" or "no." To have this functionality doesn't increase the cost much, but handling the consent will increase the cost. Namely, at any given time, a service provider has to be informed when someone has withdrawn their consent and thus not utilize their data.

(3) Data processing in international contexts. With cloud service and other modern software infrastructures, personal data may transfer to a third country or an international organization. Companies need to make sure that their current safeguards for personal data transfers comply with the GDPR conditions and, when necessary, put into practice new safeguards. Companies outside the EU must comply with both their own national legislation and the GDPR when handling EU residents' personal data or monitoring data subjects' behavior within the EU. A non-EU established controller will need a representative in the EU. This is about understanding other organizations' practices; therefore, it is not directly linked to persuasive software features. But this involves personnel designation and communication, and these will end up with more costs.

(4) Demonstrating compliance. The GDPR obliges controllers to be able to demonstrate that their personal data processing complies with the regulation. To show compliance with GDPR requirements, getting data protection certifications, seals, and marks is recommended, which increases the cost.

(5) Obligation to report breaches within 72 hours. Controllers should notify data protection authorities and data subjects about data breaches as early as possible. A possible software feature could be an automatic notification or warning for data subjects about possible data breaches. This has already been manifested in persuasive systems design through reminder features [8], which can take care of automatic notifications and/or warnings. In general, clearly defined and well-practiced procedures (because of the requirement to act within a very limited time) are needed in organizations to deal with possible breaches and related reporting. These support activities increase costs.

(6) Profession of Data Protection Officer (DPO). In some cases, an organization must designate a DPO of the organization. Conditions for organizations that must have

a DPO are as follows: if they are a public authority (except for courts acting in their judicial capacity); if they carry out large-scale processing of special categories of data or data relating to criminal convictions and offences; and last but not least, if they carry out large-scale systematic monitoring of individuals (for example, online behavior tracking). Those organizations may need to obtain new experts who understand both the GDPR and the persuasive systems design. Obtaining new expertise is directly linked with the cost of persuasive systems development.

(7) Documentation of processing activities. Processing activities need to be recorded and made available to the supervising authority upon request. Data-protection impact assessments are also required prior to possible risky processing operations. Maintaining the required documentation involves more work time and therefore increases costs.

4 Discussion and conclusion

Information provided by an information system will be more persuasive if it matches with the needs, interests, personal use and user context, and other factors relevant to a user or a user's group [8]. A critical question for persuasive systems design is: Could some persuasive software features be affected by the GDPR to such an extent they will not be able to function as planned, and therefore they would decrease the system's persuasive power?

The GDPR requires that the data subjects have the right to obtain from the controller the erasure of their personal data without undue delay. Suppose the following scenario: a personal trainer website provides different content for different user groups, e.g. beginners and professionals. When a user decides to erase data about one's user history or personal interests, the coaching system may end up providing general information and suggestions rather than personalized or tailored information.

Let's look at another example. Social learning is dependent on the fact that a person can observe others performing the same behavior. Social comparison is based on the fact that a person can compare his/her performance with the performance of others, and social facilitation is based on the idea that a system user can discern that others are performing the behavior along with them [8]. Principles under the social support category are based on the fact that the system has access to other users' data. Similar to personalization and tailoring, when users have no access to other users' data (since the GDPR provides the right to data subjects to erase their data), social support functionality could end up not working as planned because of users' erasure of data.

While the GDPR brings new design requirements and cost implications, naturally it also provides the field of persuasive system design with new research directions. A key question that will remain is, while system features may be affected, will this decrease the system's persuasive power? Future research could also study to what extent the GDPR would affect the selection of persuasive software features and to what extent those very features would influence users' actual behavioral change. As previously proposed by Shao and Oinas-Kukkonen [9], the cost of developing persuasive systems would also need more attention. For companies, compliance with GDPR requirements

is costly. Thus, the essential question is, to what extent does the compliance with the GDPR influence the costs of persuasive system development? Future research should also seek to help companies assess the cost of persuasive systems development under the requirements of the GDPR.

To conclude, this paper recognized two impact categories for how the GDPR affects persuasive systems design: design requirements and cost implications. The GDPR requires organizations to treat privacy by design and as default, especially when providing information for users and ensuring both their right to be forgotten and their right to data portability. Complying with the GDPR also implies costs with minimizing data, obtaining consent, data processing in international contexts, demonstrating GDPR compliance, reporting breaches quickly, starting a new position of Data Protection Officer, and documenting processing activities carefully. Future research on these design requirements and cost implications is needed.

References

1. Oinas-Kukkonen, H.: A foundation for the study of behavior change support systems. *Personal and Ubiquitous Computing*, **17**(6), 1223-1235 (2013).
2. European Commission. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications). *Official Journal L 201*, 0037–0047; 2002.
3. European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions – Safeguarding privacy in a connected world. A European data protection framework for the 21st century. COM (2012) 09 final; 2012a.
4. Dix A.: The commission’s data protection reform after Snowden’s summer. *Intereconomics* **48**(5), 268–71 (2013).
5. Cavoukian A. *Privacy by Design: The 7 foundational principles*. Ontario: Information and Privacy Commissioner of Ontario, Canada. (Revised version published in 2013); 2009.
6. European Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM (2012) 11 final; 2012b.
7. Basin, D., Debois, S., Hildebrandt, T.: On Purpose and by Necessity: Compliance under the GDPR. 22ed International Conference on Financial Cryptography and Data Security (2018)
8. Oinas-Kukkonen, H., Harjumaa, M.: Persuasive systems design: Key issues, process model, and system features. *Communications of the Association for Information Systems*. **24**, 485-500 (2009).
9. Shao, X. & Oinas-Kukkonen, H.: Thinking about persuasive technology from the strategic business perspective: a call for research on cost-based competitive advantage. In: *Proc. Persuasive 2018*, 3-15 (2018).