International Journal of
Geo-Information

MDPI

Article

Complying with Privacy Legislation: From Legal Text to Implementation of Privacy-Aware Location-Based Services

Mehrnaz Ataei [1,*], Auriol Degbelo [1], Christian Kray [1] and Vitor Santos [2]

[1] Institute for Geoinformatics, University of Muenster, Heisenbergstrasse 2, 48161 Muenster, Germany; degbelo@uni-muenster.de (A.D.); c.kray@uni-muenster.de (C.K.)

[2] NOVA IMS Information Management School, University Nova Lisboa, 1070-312 Lisbon, Portugal; vsantos@novaims.unl.pt

* Correspondence: m.ataei@uni-muenster.de; Tel.: +49-251-83-30097; Fax: +49-251-83-39763

Received: 12 October 2018; Accepted: 7 November 2018; Published: 13 November 2018

Abstract: An individual's location data is very sensitive geoinformation. While its disclosure is necessary, e.g., to provide location-based services (LBS), it also facilitates deep insights into the lives of LBS users as well as various attacks on these users. Location privacy threats can be mitigated through privacy regulations such as the General Data Protection Regulation (GDPR), which was introduced recently and harmonises data privacy laws across Europe. While the GDPR is meant to protect users' privacy, the main problem is that it does not provide explicit guidelines for designers and developers about how to build systems that comply with it. In order to bridge this gap, we systematically analysed the legal text, carried out expert interviews, and ran a nine-week-long take-home study with four developers. We particularly focused on user-facing issues, as these have received little attention compared to technical issues. Our main contributions are a list of aspects from the legal text of the GDPR that can be tackled at the user interface level and a set of guidelines on how to realise this. Our results can help service providers, designers and developers of applications dealing with location information from human users to comply with the GDPR.

Keywords: geographical information; location privacy; geoprivacy; general data protection regulation (GDPR); location-based services; privacy-aware systems

1. Introduction

Many services routinely collect location data from human users for various reasons. While there are many benefits of the ready availability of personal location data (e.g., better personalisation, location-based services), this type of geoinformation is particularly sensitive, as it allows for deep inferences about the person who produced it. For example, location data can be used to find out where a person lives, whom they interact with and what their daily routine is [1]. In addition, even very few data points can be exploited for attacks such as stalking or breaking into someone's home while they are away [2]. Recently disclosed privacy violations have led to further increasing worries regarding surveillance [3,4]. It thus makes sense that technical as well as legal measures are being developed to ensure the safety of service users as well as their basic civil rights and freedoms.

The General Data Protection Regulation (GDPR) [5] is one such legal safeguard that harmonises data privacy laws across Europe. It was introduced by the European Parliament and the Council of the European Union (EU) to strengthen the protection of people with respect to the processing of their personal data. The GDPR was first published in April 2016 and has been applied from 25 May 2018 onwards. It includes far-reaching measures to protect privacy and is widely expected to be a game changer for the design of computing systems in general—including those that specifically function using location data of their users, i.e., location-based services (LBS). Given that in the digital age "privacy goes global" [6], the impacts of the GDPR will be felt far beyond the boundaries of Europe.

While this new law promises to strengthen the rights of individuals, it also poses challenges to the designers and developers of systems that process personal data (e.g., location data). On the legal level, there are questions as to how compliance can be demonstrated. On a technical level, the law introduces new requirements regarding how data is stored, processed and deleted. While these two perspectives already introduce many challenges, it is also not clear how to realise various requirements that the GDPR formulates with respect to what users should be able to control and regarding how and when certain types of information should be presented to them. Providing material to support developers implementing GDPR is critical, as non-compliant companies could be fined with up to (the greater of) 20 million Euro or 4% of their global annual turnover.

Location-based services (LBS) are increasingly ubiquitous systems that deal with geo-information and process the location data of their users. In this paper, we aim to address challenges resulting from the introduction of the GDPR that relate to user interfaces of LBS. Our main contributions are as follows: (1) We systematically analysed the legal text to identify a list of aspects that can be tackled at the user interface level (UI) (Section 3); (2) In addition, we carried out interviews with experts to gain further insights into challenges arising from having to comply with the GDPR as well as into ways of addressing them (Section 4); (3) Based on the outcome of both activities, we compiled a set of guidelines for developers and designers to help them design LBS that comply with the GDPR (Section 5). Finally, these guidelines were evaluated in a take-home study with four developers. The participants developed two fully functioning LBS prototypes while using the guidelines (Section 6). Our contributions can benefit designers and developers who need to create services that meet requirements related to location data defined by the GDPR.

2. Related Work

In this section, we briefly summarise key related work by first reviewing various concepts and definitions of privacy and location privacy. We then provide a short overview of the GDPR (the next chapter will give an in-depth analysis of the legislation) and outline how location data privacy and LBS are connected. This is followed by a brief review of the existing approaches used to tackle location privacy issues in LBS. A short summary concludes the section. LBS research may be viewed as covering the seven areas listed in [7]: positioning, modelling, communication, evaluation, applications, analysis of LBS-generated data, as well as social and behavioural implications of LBS. This review of previous work does intend to cover all these areas. Instead, the works presented next touch primarily on communication aspects as well as social and behavioural implications of location privacy because these themes are the most closely related to the main focus of the article.

2.1. Location Privacy: Definitions and Concepts

Although there is no single and simple definition for privacy, it is important to describe the facets that define and shape it in order to build privacy-aware technologies.

According to Westin [8], privacy is "the claim of an individual to determine what information about himself or herself should be known to others". In addition, it also makes a difference how such information is obtained by others and what it is then used for. Westin further defines three levels on which privacy issues can be addressed: at the political level, the socio-cultural level and the individual level. Obviously, different political systems and philosophies will vary regarding how much they value individual freedom from surveillance versus maintaining public order. Legal frameworks, such as the GDPR, are means by which these different values can be expressed. Privacy at the socio-cultural level relates to individuals' practices and experiences in their everyday lives, or as Westin puts it, "the real opportunities people have to claim freedom from the observation of others. [..] In this sense, privacy is frequently determined by the individual's power and social status [8]". At the individual level, Westin [8] distinguishes four basic states: solitude, intimacy, anonymity and reserve. Solitude refers to the right to not be observed by other parties. Intimacy refers to the right to entertain a close, honest and relaxed relationship with one or more people (a small group). Anonymity refers to being free from surveillance in public. Finally, reserve denotes the right to limit what information about oneself is disclosed to other parties.

While privacy thus is an important and complex concept in our everyday lives, this is especially true in the context of our digital endeavours. Solove [9] confirms this by stating that: "privacy is a plurality of different things and that the quest for a singular essence of privacy leads to a dead end". Solove [10] argues that conceptualising privacy can be achieved by discussing six general headings: "(1) the right to be let alone; (2) limited access to the self, the ability to shield oneself from unwanted access by others; (3) secrecy, the concealment of certain matters from others; (4) control over personal information, the ability to exercise control over information about oneself; (5) personhood, the protection of one's personality, individuality, and dignity; and (6) intimacy, control over, or limited access to, one's intimate relationships or aspects of life. Some of the conceptions concentrate on means to achieve privacy; others focus on the ends or goals of privacy" [10].

The importance of data privacy becomes more clear when specific kind of data can pose substantial risk to individuals' safety and privacy, sometimes even without their knowledge. Information about an individual's location is one type of data that not only has a great potential to personally identify users, but, when it is combined with other types of data such as financial or health data, can also reveal sensitive information about individuals. Location data is used in most services that provide users with relevant information about their geographical positions (i.e., LBS). The presence of "ubiquitous positioning devices and easy-to use application programming interfaces (APIs) make information about an individual's location much easier to capture than other kinds of personally identifiable information" [11].

Protecting location data is important due to the increasing number of technologies that collect, process and store users' location data and the nature of this data is highly sensitive. Even if users do not explicitly share their geographic coordinates, their location can be probabilistically determined based on the words that they write (e.g., on Twitter), the time stamps that they make public, and the spatial properties of a city (see [12]). In general (and as indicated in [13]), a location privacy threat is a function of the current location along with previously released locations.

In order to design a GDPR-compliant UI for LBS, the first step is to understand LBS, location privacy, and the importance of protecting personally identifiable information (PII) including location data. Duckham and Kulik [14] define location privacy as "a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others". Personally identifiable information (PII), which includes location data, is one of the key factors related to privacy in the digital realm. PII refers to any information that can be linked back to a natural person and therefore provides a third party with a potential vector of attack. For example, knowing a person's current location might enable a third party to threaten or expose that person. Since such information is very sensitive and potentially dangerous in the wrong hands, laws are put in place to protect it and regulate its use.

2.2. Location Data Privacy Issues in LBS and the Role of the General Data Protection Regulation (GDPR)

The European Commission has issued the General Data Protection Regulation (GDPR) [5], which is an expanded and harmonised version of the Directive 95/46/EC (Data Protection Directive or DPD). The GDPR defines far-reaching rights for individuals with respect to PII that relates to them, and it applies to any company that processes or collects personally identifiable information of an individual in the E.U., e.g., in the context of providing services or selling products. It applies also to companies based outside the E.U. if they process or collect such data. The many requirements set out by the GDPR are predominately focused on the way companies handle PII (which in some cases may require substantial changes in order to become GDPR-compliant). While some of these changes will affect behind-the-scenes data management or data processing, other aspects will require direct user interaction, i.e., changes at the UI level. A detailed analysis of the latter is the topic of Section 3.

The GDPR has a very broad definition of processing information, which includes "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" [5]. Consequently, almost any system that allows users to register or personalise its appearance or functioning would fall under the GDPR. For example, personalization of a Web application can affect links that users see when they interact with the system, the content that they are presented with, and the overall structure of the Web application (see [15]). In earlier work, Kobsa [16], providing an introduction to the field of privacy-enhanced personalization, pointed out that online users value personalization, and at the same time, personalization of websites seems profitable for web vendors. Therefore, automatic content customisation creates a win–win situation for both. Nevertheless, since users need to give up some data in exchange for tailored content, there is always a privacy threat associated with personalization on the web. The risk of privacy breach mentioned above is one of the ethical dilemmas of LBS [17]. A second ethical dilemma of LBS is the possibility of increased monitoring leading to unwarranted surveillance by institutions and individuals [17]. Abbas et al. [17] proposed therefore to explore the social implications of LBS based on these two factors. They observed that inextricable linkages exist between the four themes of control, trust, privacy and security. Put differently, "privacy protection requires security to be maintained, which in turn results in enhanced levels of control, leading to decreased levels of trust, which is a supplement to privacy" (see also [18]). Few social/behavioural implications of LBS were mentioned in [4]: location data collection impacts employer/employee, customer/vendor relationships and marital relationships; it has probative value (i.e., has been used by courts to convict criminals); and constant location monitoring could ultimately impact on our own ability to be creative, be different, be diverse and be our own person. Ensuring data privacy of LBS users will require a coordination of legal, industry-based and technological approaches (see [17]). The need to move beyond technology-centric approach to embrace a more holistic approach to location privacy (including ethical, economical, legal, and educational aspects) was also recently stressed by Keßler and McKenzie [11] in their "manifesto" on Geoprivacy (i.e., location privacy).

The critical need for law enforcement becomes clear when [19] presents the result of the three recently conducted European surveys. They indicate that "EU citizens have a good opinion about their technological skills, but this opinion has little correspondence with reality: their online behaviours suggests that they are not smart users; they have no clear idea of how to protect their privacy and safety. They are cynical about who they could trust to make a fair use of their personal data (basically, only the actors that are legally bound to, or those that lose money if they don't) and they think that the first actors who should protect users' privacy and data are users themselves, but they have little (and often misguided) idea on how to do it. Their greatest fears are based on classic frauds, not on fraudulent misuse of their personal data; they are generally poorly afraid for their reputations or that data on online activity can be used to discriminate against them". A practical example of implementing GDPR has been done by Raschke et al. [20] who designed a GDPR-compliant Dashboard to protect privacy. Challenges that controllers and processors of personal data might face dealing with the obligation of GDPR in the context of the internet of things have been listed in Lindqvist [21]'s work. For example, Lindqvist pointed out that "both controllers and processors are obliged directly by law to ensure the security of personal data processing".

A large body of work exists discussing various technical ways to protect location privacy as well as various key concepts such as k-anonymity [22], mix zones [23] or the Casper system [24]. In addition, recent work is exploring the possibilities of combining various techniques such as pseudonym change strategy with multiple mix zones to protect privacy [25]. Such works also adjust existing technologies such as mix zones to protect the location privacy of vehicles (which can also reveal confidential information about their drivers through the trajectory of their location information [26]). Beyond approaches that focus on technical issues, there are also some more general proposals about how to make LBS more privacy aware. Langheinrich [27] specifically looked at ubiquitous systems and proposed an approach to ensure accountability regarding PII. His approach can also be classified as following many of the guidelines laid out by Cavoukian [28], which defines seven basic principles that interactive systems should realise to protect users' privacy. While such technical advancements are necessary for improving the protection of location privacy, Keßler and McKenzie [11] reminded that "Preserving geoprivacy involves more than obfuscating geographic co-ordinates. Location can be inferred from non-explicitly geospatial information such as interests, activities and socio-demographics". One of the concerns in this regard is related to mobile operating systems that "lack fine-grained control mechanisms for location services, thus severely limiting the degree of control users have over their location information" [11]. Ataei et al. [29] recently proposed user interface elements for fine-grained management of location privacy settings, which help to specify who to share location information with, when to share it, and where to share it. A common sentiment among critics of LBS is that "the ethical ramifications of progresses in location-enabled technology are often viewed as an afterthought, and legal concerns over privacy aspects oftentimes lag behind technological advances" [11]. To address this issue, the GDPR has integrated privacy by design principles (e.g., privacy embedded into design, privacy as the default setting), and also aims to enforce greater visibility and transparency regarding data collection activities. However, addressing location privacy related issues are complex, and they need clarification, discussion and proper actions. To keep this work feasible, we will focus only on a few aspects of this process. As location privacy in LBS is a core area of focus, we reviewed and categorized the legal requirements that are addressable through UI.

2.3. Summary

From this brief review of related work, we can draw a number of conclusions. While privacy is a complex concept, it plays an essential role in everyday life, in particular in the digital realm. Many services process personally identifiable information such as location information for various reasons (e.g., service adaptation, personalisation, in-kind payments) and can thus cause different types of issues. One of the critical concerns regarding the default behaviour of such services is related to the lack of fine-grained controls for location privacy settings (sharing all or nothing). For most of these LBS, users are not provided with means to adjust the personal data collected about them. In addition, such services are subject to corresponding legislation such as GDPR. While various approaches have been proposed to tackle privacy issues in LBS, how exactly these could be used to make a system compliant with the GDPR is not clear. In the remainder of this paper, we look deeper into this issue.

3. Analysis of the GDPR

The compliance with GDPR may be viewed as a sequence of three iterative steps: (i) general understanding of the original GDPR text, and (ii) selection of pertinent concerns to be addressed, and (iii) development of strategies to tackle the concerns. The analysis documented in this section aimed at extracting aspects of the GDPR that are pertinent to UI design in the context of LBS. The rationale for focusing on UI design for LBS in this work was twofold. First, GDPR puts a strong emphasis on data subjects rights. UI, as fundamental ways of communicating various matters to users, are thus instrumental in realising the goal of the regulation. Second (and as briefly discussed in Section 2), in the area of developing privacy-aware LBS, there has been more advancement on the back end (i.e., technical) level than the front end (i.e., presentation or UI) level. That is, more work is currently needed in LBS research in general to better communicate location privacy subtleties to users. To keep the scope of this work manageable, we focused on the following three aspects of GDPR: notice, consent, and control (Aspects such as Data security (Art 5), data minimisation (Art 5), Appointment of a data privacy officer (DPO) (Art 37), or Impact assessment (Art 35) are equally relevant but could be the subject of follow-up analyses). We will discuss the legal requirements for each of these factors in the next sections.

The GDPR [5] consists of 99 articles and 173 recitals, including principles such as the conditions for lawful processing, the rights of data subject, and the responsibilities of the controllers and processors, to name a few. Among many aspects presented in the GDPR, there is an emphasis on transparency, providing ways for individuals to control their data, and the principle of Privacy by Design. We explored various strategies for interpreting the text of the GDPR from the perspective of developers and designers. We eventually developed a strategy for understanding the legal requirements and assigning them to the responsible individuals. The strategy involves six iterative steps: (1) scanning the legal content thoroughly; (2) extracting the requirements; (3) clarifying the expectations of the legal text; (4) clustering the expectations into categories; (5) relating or connecting them into understandable terms for developers; and (6) assigning the requirements to responsible individuals. With regard to these aspects, we compiled the most relevant set of provisions for designing LBS in GDPR, and we categorised them into two groups: (1) *data management*, which includes minimising data collection, secure storage, and keeping the data accountable (i.e., updated and correct); and (2) *communication of data management with data subjects*, which includes notifying data subjects about collected personal data and conditions for consent and providing controls (e.g., access, rectification, and restriction based on the rights of data subjects).

For the purpose of this paper (inferring concepts and principles), we are using the same terms and definitions that are presented in Art 4 definitions of GDPR [5]. The following terms (and their respective definitions) are relevant in the context of this work:

- "Personal data" means any information relating to an identified or identifiable natural person.
- "Data subject" is a natural person 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.
- "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

One of the GDPR's major concerns is related to the data subjects' rights. Compliance with GDPR requires understanding these rights and also building services with respect to these rights. GDPR requires service providers (i.e., data controllers and processors) to support transparent communication (Article 5). In this context, the GDPR requires respecting data subjects' rights and communicating the processing activities to data subjects. Thus, our analysis of GDPR has focused on data subjects' rights and the aspects that are addressable at the UI level. This analysis resulted in three primary categories: notice, consent and control. A short explanation for each of the factors is presented in the following sections. A more detailed version of the analysis including all relevant Articles and Recitals from GDPR is included in Appendix A.

3.1. Notice

GDPR requires the ensuring of lawful, fair and transparent processing of personal data. According to Recital 60 of GDPR [5], the processing is fair and transparent if the data subject is given notice of the existence of the processing and its purposes. The controller should provide data subjects with the information that is listed in Art 13 of GDPR, which includes (a) the identity and the contact details of the controller; (b) the contact details of the data protection officer; (c) the purposes of the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; and (e) the recipients of the personal data. In addition to the list, data subjects should also be informed about (a) the period for which their personal data will be stored; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; ... (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 13 [5]).

Ensuring fairness and transparency regarding the lawfulness of the processing is thus achieved by informing data subjects about their rights, the consequences of their decisions, and the activities of the controller. GDPR considers the processing lawful if “the data subject has given consent to the processing of his or her personal data for one or more specific purposes” or processing is necessary for various reasons such as “compliance with legal obligation” or “for the performance of a task carried out in the public interest”, according to Recital 60 [5].

3.2. Consent

According to the GDPR, consent is one of the fundamental principles to make data processing activities lawful. Article 4 defines consent of data subjects as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” [5]. Article 7 defines the conditions for the consent such as follows: (1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. (2) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Recital 42 also lists some requirements for consent: “for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment”. Similar to the concept of notice, consent should communicate the processing activities with data subjects, but the primary difference is that the consent requires active approval and confirmation from data subjects. Consent also needs to be flexible to support the features of withdrawal (i.e., the right of opting out from data processing), renewal (i.e., receiving an updated consent when the purpose of the processing has changed), renewal is needed in the case of multiple purposes processing, according to Recital 32 “when the processing has multiple purposes, consent should be given for all of them”.

3.3. Control

GDPR stresses the importance of providing data subjects with control over their personal data. Control includes various principles such as the right to access, the right to rectification and erasure, the right to restriction, the right to data portability and the right to object. We will briefly explain the legal requirements for each.

- Access—according to Art 15: *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed* (see Appendix A for the listed conditions according to Art 15).
- Rectification—Art 16:*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her*.
- Erasure (right to be forgotten): *The controller shall have the obligation to erase personal data without undue delay where one of the following grounds* listed in Appendix A applies.
- Restriction of processing—Art 18: *The data subject shall have the right to obtain from the controller restriction of processing where one of the following grounds* listed in Appendix A applies.
- Data portability—Art 19: *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided—Art 20.*
- Object—Art 21: *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1)*. See Appendix A for the details.

3.4. Summary

The previous three sections have presented the provisions of GDPR with respect to data management and the communication of data management to data subjects. The terms "data subject" and "controller" appear repeatedly, and they stress the importance of both parties for the law giver (see also Figure 1 for a visualisation of the most frequently mentioned terms in the regulation). GDPR emphasises primarily the processing of personal data and the interaction between controllers and data subjects. Note that interaction is used here in line with [30], who argued that "interaction concerns two entities that determine each other's behavior over time". GDPR-compliant interactive systems are therefore mediums which support that mutual determination between the controller and the data subject. The regulation puts a clear emphasis on the role of controllers, but the processor is also a third important actor, an actor that was previously identified by Conger et al. [31] in their model of personal information privacy (There are some parallels between the roles listed above and the roles listed by Conger et al. [31] in their model of personal information privacy. The "individual" of [31] is equivalent to the "data subject" of GDPR; the "vendor/providers of services" from [31] are akin to "controllers" of GDPR; the term "processor" from GDPR includes both the "third party" (i.e., data sharing partners) and the fourth party (i.e., illegal hackers, thieves and third party employees who violate company policy) from [31]). That is, in the digital age, GDPR-compliant systems are systems which support the mutual determination between the controller (i.e., the entity which requests personal data), the data subject (i.e., the entity which gives personal data away), and the data processor (i.e., the entity which processes personal data).

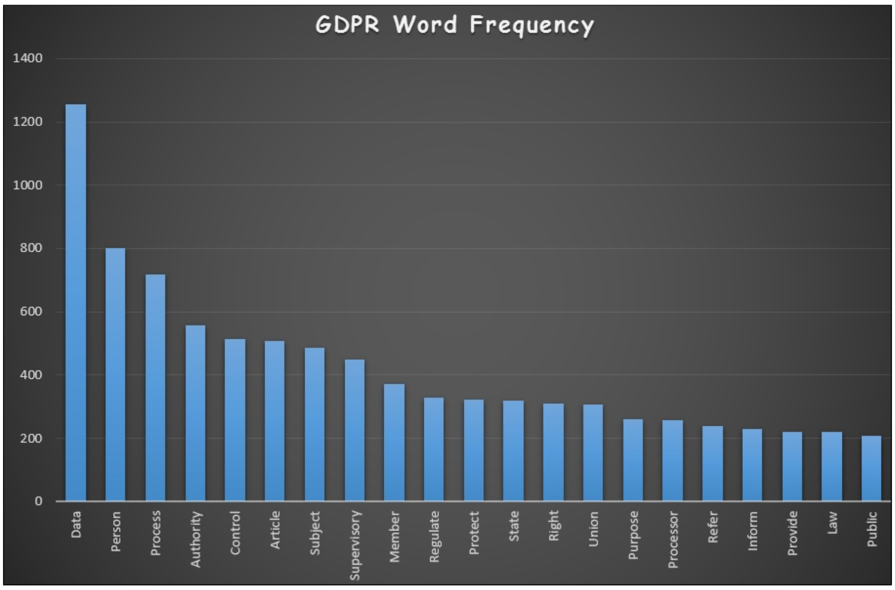


Figure 1. Words mentioned at least 200 times in the GDPR reference document [5] (stopwords removed). It helps see most prominent concepts of the regulation: personal data, the processing of it, and the interaction between controllers and (data) subjects. Word frequencies were obtained by using Wordart [32].

4. Expert Interviews

As mentioned in the previous section, the compliance with GDPR may be viewed as a sequence of three iterative steps: (i) general understanding of the original GDPR text, and (ii) selection of pertinent concerns to be addressed, and (iii) development of strategies to tackle the concerns. The primary goal of Section 3 was to extract relevant points from the GDPR and help to better grasp the requirements to comply with regarding the tasks of notice, consent and control. This section points out some of the challenges (viewed through the lenses of experts) with implementing GDPR-compliant systems and possible ways of addressing them. A set of interviews was conducted to explore challenges and solutions regarding the implementation of GDPR. We started the process with a planning phase including few research questions (see Appendix B), and we gathered reflections from experts in three main areas: general challenges, possible solutions, and specific requirements for notice, consent and control (i.e., NCC factors). The specific requirements touched upon what to include in each NCC factor, how to communicate it to users, and the phase of system development where they should be considered.

4.1. Participants

The participants were domain experts who were directly involved with implementing GDPR in an academic or industry environment. Besides GDPR involvement as the main requirement for recruitment, experts were also recruited based on their experience in the field of data privacy, data ethics and security in information systems. Six experts—two from industry, three from academia and one from both—participated in our study. Detailed biographies can be found in Table 1.

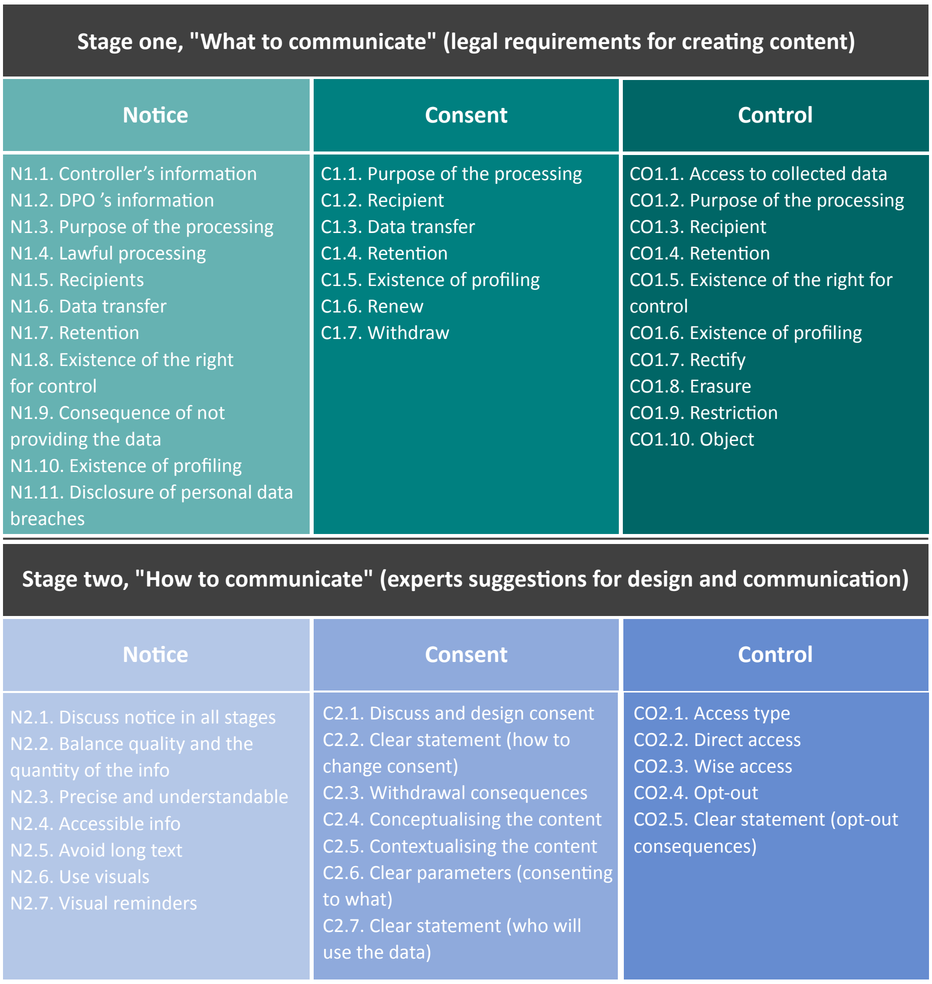
Table 1. Brief biographies of the experts interviewed.

Participant ID	Brief Biography
E1	Professor and consultant working on design ethics
E2	E-Governance evangelist, currently part of an expert group advising a European city council on matters related to the implementation of GDPR in relation with government and public services
E3	Assistant professor working on projects related to data justice, and in particular data ethics
E4	Lawyer, currently advises companies in different sectors such as banking, insurance, transportation on how to implement GDPR
E5	Professor and co-Founder of an IOT (Internet of Things) company, which develops solutions for smart cities
E6	Professor, currently working closely with municipalities on the implementation of smart cities initiatives

4.2. Procedure

We conducted semi-structured interviews through video calls (via Skype). We found semi-structured interviews appropriate, as our goal was to gather deep insights and receive critical comments about the topic.

We divided the questions into three levels. Level one included the intro question (i.e., participants' role in and experience with data privacy or GDPR), which was followed by questions regarding the general aspects of the topic, including challenges regarding the implementation of GDPR and possible ways of addressing such challenges. Level two consisted of a more specific set of questions including some that targeted difficulties which developers and designers could encounter while developing GDPR-compliant interactive systems. Level three was a focused inquiry on particular questions regarding the NCC factors, including the phase of system development in which one should consider the NCC factors, what to include in each phase and how to communicate the relevant information to end users at the UI level (see Figure 2 for details). The lead author carried out all the interviews, provided verbal explanations, received digitally signed consent forms from participants, and took notes during the sessions. All of the sessions were audio recorded after participants had consented. The institutional ethics review board approved the study prior to its execution.



Stage one, "What to communicate" (legal requirements for creating content)

Notice	Consent	Control
N1.1. Controller's information N1.2. DPO 's information N1.3. Purpose of the processing N1.4. Lawful processing N1.5. Recipients N1.6. Data transfer N1.7. Retention N1.8. Existence of the right for control N1.9. Consequence of not providing the data N1.10. Existence of profiling N1.11. Disclosure of personal data breaches	C1.1. Purpose of the processing C1.2. Recipient C1.3. Data transfer C1.4. Retention C1.5. Existence of profiling C1.6. Renew C1.7. Withdraw	CO1.1. Access to collected data CO1.2. Purpose of the processing CO1.3. Recipient CO1.4. Retention CO1.5. Existence of the right for control CO1.6. Existence of profiling CO1.7. Rectify CO1.8. Erasure CO1.9. Restriction CO1.10. Object

Stage two, "How to communicate" (experts suggestions for design and communication)

Notice	Consent	Control
N2.1. Discuss notice in all stages N2.2. Balance quality and the quantity of the info N2.3. Precise and understandable N2.4. Accessible info N2.5. Avoid long text N2.6. Use visuals N2.7. Visual reminders	C2.1. Discuss and design consent C2.2. Clear statement (how to change consent) C2.3. Withdrawal consequences C2.4. Conceptualising the content C2.5. Contextualising the content C2.6. Clear parameters (consenting to what) C2.7. Clear statement (who will use the data)	CO2.1. Access type CO2.2. Direct access CO2.3. Wise access CO2.4. Opt-out CO2.5. Clear statement (opt-out consequences)

Figure 2. Recommended guidelines based on legal requirements and expert suggestions.

4.3. Results

The analysis of data started by transcribing the audio recording and the notes taken by the interviewer. We used directed content analysis to analyse the data. Directed content analysis involves the use of categories or codes defined by the researcher prior to analysis, and it may lead to the definition of some further (sub)categories during the analysis (see [33]). We used MAXQDA 2018 (VERBI Software, Berlin, Germany) as a tool to code and analyse the data. The codes were specified at the beginning of the analysis based on the questions that we asked about (1) the challenges regarding the implementation of GDPR (i.e., including particular difficulties for developers and designers in the context of GDPR implementation); (2) the suggested solutions by the experts to tackle the challenges; (3) when (during interactive system development) the experts thought GDPR should be addressed and who should be responsible for the GDPR implementation; and (4) the specific recommendations from the experts for the implementation of notice, consent and control at the UI level.

The answers that emerged from each category are reported in the following sections. Since it is well known that experts often disagree among themselves, a (sub)category related to one of the codes defined above was created only if at least two different people referred to the topic of the category.

4.3.1. Challenges Regarding the Implementation of GDPR

The following challenges and how to address them were mentioned by the participating experts:

User-friendliness: Not surprisingly, implementing GDPR in a way that does not place some unmanageable burden on users was mentioned by the participants as an issue. Implementing GDPR while avoiding complexity in interaction or overwhelming numbers of alerts or notifications was mentioned by E1 and E6. In addition, the importance of communicating privacy-related issues to end users in a simple way was mentioned by E1, E2 and E5.

Awareness: Another challenge that experts considered important was raising awareness about the need to think about data protection early during application development. E4 believed that start-ups and some business do not have enough resources to consider privacy-related issues from the beginning stages of system development. E1′s thoughts regarding the prioritising of privacy-related issues are in line with E4.

Technical considerations: Technically realising the requirements of the regulations is a further challenge. Guaranteeing anonymisation is difficult due to the currently available technology options, according to E5 and E6.

Regarding specific challenges for developers and designers, the participants highlighted the following problems:

Lack of specific guidelines: E5, who is a founder of a company developing IOT devices, said, "In my company, we have developers and we are trying to develop software solutions and we have not found any guidelines that we can use". A similar concern was raised by all other participants.

Reasons for compliance with GDPR: This was another challenge, mentioned from different perspectives. Participants also raised concerns about the need of proper education regarding the importance of complying with GDPR (similar statements by E1, E3 and E5). E1, for example, stated that "designers need to be told clearly ... about compliance with GDPR..., designers ought to know the purpose of compliance, designers should know the context and reasons". E3 also said that "we can explain to designers what kind of value they think they should include or how to include those values" to comply with GDPR. The overall difficulty was to find a way to provide developers and designers with explanations and reasons beyond avoiding fine and punishment.

4.3.2. Approaches to Address Implementation Challenges

Participants suggested some approaches to address the challenges presented in the previous section, based on the area of their work and their expertise. Some of the suggestions are very specific and we try to explain them in the context of the discussion.

A group of experts: Building a group consisting of legal and technical experts was suggested by E3 and E4. Both argued that addressing GDPR-related challenges is not simple and therefore cannot be expected to be done by single individuals alone. E4 suggested to include "lawyers, data processors, those who are aware about how information flows in a company, IT people, data ethics experts, those with humanistic training, or philosophers, or those who have legal ethics as their main concern, so this should be a multidisciplinary discussion". The communication among members of such a group can be also challenging, and E3 suggested that assigning one individual with knowledge in both legal and technical aspects of development process could be a way to facilitate the communication.

Customised guidelines: All experts agreed on the importance of developing specific guidelines for each company or service provider. E1 said: "there has to be a guideline for designing interactive systems, that is fundamental, this is technical, then it is the discussion of system requirements that must be designed with features supporting the implementation of GDPR, then you need certain visual and graphical palettes based on a company's visual brand, that is related to the company's design guidelines".

Contextualisation: The best way to communicate concepts related to privacy to users is through simplified but tangible methods (i.e., mentioned by E1, E2, E3 and E5). E1 calls it "wise notification", and E3 believes that if the consent is not fully understandable for users, then it can turn into a tool for service providers to obtain permission for processing user data without protecting the users' privacy.

4.3.3. Integrating GDPR Considerations into the Development Process

Regarding the phase in which one should consider GDPR compliance factors, all experts agreed on the importance of considering GDPR compliance factors at the requirement gathering and analysis stage or even prior to that. E1 said: "it should definitely be discussed at requirement analysis and design but it should also stay through the other stages". This is in line with the GDPR suggestions which encourage service providers to follow Privacy by Design principles and include privacy considerations early and in all stages of system development [34]. While all expert agreed that assigning a group of individuals with various expertise as being responsible for GDPR implementation is the best strategy, a few believed that the implementation is the service providers' responsibility rather than developers' and designers' (i.e., mentioned by E1, E2 and E3).

5. Guidelines for Realising GDPR-Compliant Implementations

As mentioned in Section 1, the GDPR does not come with explicit guidelines for developers and designers to help them implement its requirements. This need for guidelines was confirmed during the expert interviews (see Section 4.3.1). With focus on notice, consent, and control (NCC) factors from GDPR, presented in Section 3, we developed a set of guidelines. In order to construct guidelines that are easy to follow, we defined two primary stages for developers (Figure 2); the content stage, which refers to the body of the material that should be included for addressing each of the factors (e.g., the purpose of processing should be stated when designing for notice); and the communication stage which includes suggestions about how to communicate the content to users (e.g., text or icon).

The content stage is about "what" to include, and it covers a few aspects. First, developers and designers should understand what each of these factors mean. Second, they should understand what to include when designing for notice, consent, or control. The content stage is designed based on GDPR's main document [5] to cover the list of requirements for addressing NCC factors. This stage provides a list of required information that should be provided to users.

The communication stage is about "how" to communicate, and it focuses on the aspects regarding the communication of the body of material produced in the content stage. This stage addresses aspects such as appearance and characteristics of the NCC factors (e.g., when to ask for users' consent and how that should look). The communication stage includes the suggestions from experts for designing the content and appearance of NCC factors.

The guidelines listed in Figure 2 should be used together with the explanations for each factor presented in Sections 5.1–5.3. Regarding the content that one should create for addressing the GDPR requirements, there are repeated items for all NCC factors which include are the purpose of processing, recipients, retention, and existence of profiling. Both the notice and consent factors include data transfer, and both notice and control include the existence of the right for control for notice and control. The reason we did not present them all together is to emphasise the legal requirements for each, and also to highlight that although the content we describe for each one could be reused; it needs to be adjusted for each factor. For instance, the content described for notice does not require the confirmation from data subjects as does consent; therefore, despite the similarity of the content, the way of rephrasing and presenting might be different.

In the following subsections, we describe all the factors incorporated in the guidelines. We start by introducing those relating to notice, then move on to those connected to consent and finally to the factors linked to control. Each subsection is split into the two stages we described above. Figure 2 provides an overview of all factors and stages.

5.1. Notice

5.1.1. Content Stage—Notice (N1)

Users should be informed about all activities related to personal data processing such as data collection, its purposes and data breaches. When creating the content for notice, developers and designers should include the information listed in the first column of Figure 2.

Controller's information (N1.1) refers to the identity and the contact details of the data controller. *DPO 's information* (N1.2) refers to the contact details of the data protection officer. *Purpose of the processing* (N1.3) explains why personal data is collected and what is being done with it. It should also be made clear that the processing is lawful, meaning that it should meet the requirements explained in Art. 6 for *Lawful processing* (N1.4). Another crucial aspect to communicate to users is to whom the personal data is going to be disclosed—its *Recipients* (N1.5). These can be, for example, a natural or legal person, public authority, agency or another body (who is going to see the collected data or have access to it). *Data transfer* (N1.6) refers to whether any personal data is transferred to a third country or international organisation (where it is going to be sent). *Retention* (N1.7) describes the period of time for which the personal data will be stored, or, if that is not possible, the criteria that will be used to determine that period (for how long the collected personal data will be kept). A further important piece of information is the *Existence of the right for control* (N1.8). This relates to the right to request from the controller all aspects of control, meaning the right to access, rectify or erase personal data as well as to restrict processing or to move data to another provider. Data subjects also have to be informed after such a request has been processed (what rights data subjects have about their personal data). *Consequence of not providing the data* (N1.9) refers to whether data subjects are obliged to provide personal data, and of the possible consequences of the failure to provide such data (does the data subject have to provide personal data? What will happen otherwise?). *Existence of profiling* (N1.10) relates to the existence of automated decision-making, including profiling. The information should clearly explain the logic underpinning the decision-making, as well as the significance and the envisaged consequences of such processing for the data subject (Is there any profiling activity involved? Why? What does that mean?). *Disclosure of personal data breaches* (N.11) refers to communicating personal data breaches to the data subject in particular when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons [5].

5.1.2. Communication Stage—Notice (N2)

After creating the content for notice, it is important to decide how to communicate it to users. Recital 60 of GDPR [5] states that the information provided for data subjects "may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing". The recital's description can be interpreted differently in various contexts. During the expert interviews, we asked about the best time and the most appropriate way to notify users. A list of keywords regarding expert opinions are presented in Figure 2. *Discuss notice in all stages* (N2.1) suggests that designing the notice should be discussed and addressed throughout the requirement gathering, design and development phases. *Balance quality and the quantity of the info* (N2.2) proposes to pay attention to the importance of balancing the quality and the quantity of the information presented in notice, such that developers and designers should decide how much information must be shown so that it gives a profound overview but is still concise. *Precise and understandable* (N2.3) refers to the need to use simple, understandable and relevant terms instead of complicated, legal or technical ones. *Accessible info* (N2.4) suggests that the information presented in the notice should be accessible later (e.g., through setting), and it should not be ephemeral (e.g., to be shown only when installing the application). *Avoid long text* (N2.5) suggests that the message should be communicated through a short and wise text. *Use visuals* (N2.6) proposes to prioritise the use of visual means and relevant icons over using text. *Visual reminders* (N2.7) refers to not only presenting the information through visual means but also encouraging the use of visual reminders to fully communicate the information to users.

5.2. Consent

5.2.1. Content Stage—Consent (C1)

The GDPR requires users' consent to data processing activities. Those who collect and process the data must be able to prove that consent was given. What the user will consent to should be provided in an intelligible and easily accessible form using clear and plain language, and it should not contain unfair terms—Recital 42. Regarding the content of the consent, there are a number of items that overlap with the items presented for notice, as the focus is on the data processing activities. *Purpose of processing* (C1.1), *Recipient* (C1.2), *Data transfer* (C1.3), *Retention* (C1.4), and *Existence of profiling* (C1.5), correspond to (N1.3), (N1.5), (N1.6), (N1.7), (N1.10) from Section 5.1.1. The key difference is related to formulating the content: for notice, the purpose was only to inform users but for consent, the goal is to ask for the explicit agreement to data processing activities. Besides consenting to the data processing activities, consent also has two other specific conditions. GDPR requires to *Renew* (C1.6) the consent if the purpose of the data processing changes, the consent must be renewed and information should be presented to users accordingly. In addition, users shall have the right to *Withdraw* (C1.7) their consent at any time and through easy means, per Art. 7 [5]. It is important that users have been informed about the right of withdrawal prior to consenting.

5.2.2. Communication Stage—Consent (C2)

We discussed consent during the expert interviews. The main concern, which was raised by all experts, was the challenge of assuring that the presented information (e.g., text or image) in consent is understandable for non-technical users. In other words, how to make sure that users know what are they consenting to and that they are aware of the consequences of such consent. Experts suggest that, for designing a consent that conveys a comprehensible message to users, it is important to *Discuss and design consent* (C2.1) throughout various development stages such as requirement gathering, design and evaluation. They also suggest that the developers and designers should provide a *Clear statement (how to change consent)* (C2.2), explaining that the user will have the opportunity to change her/his decision regarding consent later, also and explaining how and through what steps one can make such changes (i.e., withdrawal right). Additional important information that consent should include, according to the experts, is the consequences of withdrawing consent: *Withdrawal consequences* (C2.3) should clearly states the outcome of a user's decision to withdrawal. The experts suggested that *Conceptualising the content* (C2.4) for users by telling them how developers will use their data rather than how they will *not* use the data, might have better results. Furthermore, *Contextualising the content* (C2.5) through everyday life events of users can also be a way to make it understandable. Experts also encourage designers and developers to use *Clear parameters (consenting to what)* (C2.6) explaining to users what they are consenting to, and a *Clear statement (who will use the data)* (C2.7) explaining who their data will be marketed to.

5.3. Control

5.3.1. Content Stage—Control (CO1)

Control consists of the factors described in the GDPR that give users control over their personal data. These factors are access, rectification, erasure, restriction of processing and object (i.e., explained in detail in Section 3). In a nutshell, Control should provide users access to the collected data, the possibility of updating the collected data, and also an option to opt-out from data collection activities.

Regarding the content of the control, the same as consent, many of the items here also overlap with those listed for the notice, but the key difference is the way they are provided to users. For example, providing the information about the collection of data will not be sufficient; it should be followed by the possibility of opting out of data collection. Similar content from notice includes *Purpose of the processing* (CO1.2), *Recipient* (CO1.3), *Retention* (CO1.4), *Existence of the right for control* (CO1.5), and *Existence of profiling* (CO1.6), which correspond to (N1.3), (N1.5), (N1.7), (N1.8), (N1.10) from Section 5.1.1. In addition to the listed information, there are a few controls that are explicitly required by GDPR to be provided to users. *Access to collected data* (CO1.1) gives users the right to access the collected personal data and also to obtain a copy of the collected information from data controllers. In addition, users have the right to *Rectify* (CO1.7) or *Erasure* (CO1.8), which means the personal data collected about them can be rectified or erased and no longer processed, particularly when the data is no longer necessary for the functionality of the service or users have withdrawn their consent. In addition, users have the right to ask for the *Restriction* (CO1.9) of the processing and the right to *Object* (CO1.10) to processing in the case of direct marketing including profiling.

5.3.2. Communication Stage—Control (CO2)

This section summarises the experts' opinions on how to address control. The main concern when discussing the control was related to the possibility of increased interaction complexity for users, which could arise after providing controls over their personal data. Thus, experts suggested avoiding such complexities by explaining the *Access type* (CO2.1) to users, meaning the kind and degree of the access should be communicated to users through notice and consent. In addition, *Direct access* (CO2.2) should be given to users, with easy possibilities of updating and observing the collected data about them. In addition, users should be notified about the consequences of erasing the data (e.g., erasing the data can influence the functionality of the service they use)—*Wise access* (CO2.3). If users request to *Opt-out* (CO2.4), the collection process has to be stopped, and this change should be communicated to them. The success of this operation has to be reported back to the users so that they can confirm that their data is no longer being collected. The opt-out option should be directly accessible through the application but similar to other decisions like erasing the data, there is a need for *clear statement (opt-out consequences)* (CO2.5) about the consequences of enabling the opt-out.

5.4. Applying the Guidelines during Development

The software engineering lifecycle for developing products includes requirement analysis, design, development, test, implementation, and maintenance [35]. The majority of the experts stated that while it is essential to consider addressing privacy-related issues in all stages of the service development, there should be more attention on addressing these issues during the requirement analysis, design, and development stages (i.e., in line with Privacy by Design principles [28]). The following is a summary of suggestions that each of these stages can include for addressing GDPR requirements at the UI level.

Requirement analysis stage: This stage could include *awareness and education*, which refers to the need of educational programmes for designers, developers and everyone in the development team who is involved in the collection, use or the processing of personal data. These programmes should involve three subjects: (1) GDPR regulations, particularly data subjects' rights, (2) the ethical and philosophical reasoning of protecting individuals' data privacy, and (3) the consequences of not complying with the regulations. It is also essential to perform *information flow inspection* during the requirement analysis stage for understanding how the data flow works, mainly for finding gaps (i.e., which part of the information flow requires GDPR compliance) and then designing solutions.

Design stage: From the activities and findings of the requirement analysis stage, the design stage could identify the moments of the development cycle when GDPR requirements should be addressed. When these moments are clear, it would be helpful to map the requirements to tasks and assign them to a group of individuals with various expertise, such as developers, designers, DPOs, lawyers, and ethics advisers. This stage could also develop an action plan connecting GDPR requirements to the system development life cycle based on every particular product's goal.

Development stage: While the initial design ideas are developed in the design stage, the development stage is where the full content (i.e., the information that should be included in the body of the solutions) and design (i.e., the way that solutions should be communicated to users) of the NCC should be finalised.

6. Guidelines in Practice: A Take-Home Study

In order to evaluate the use of the guidelines during actual software development, we asked developers to use it during a development project. Our main evaluation goal was to see whether developers could use the guidelines to incorporate (location) privacy features into newly developed location-based services. We were also interested in any problems they encountered and what they thought about the guidelines. For this purpose, we tasked four participants with a nine-week-long project course at our department (i.e., student developers) with the design and development of an LBS.

6.1. Participants

All participants were students on one of the two master's programmes offered by our institute. Programming skills varied amongst the participants, with three being quite experienced and one having of intermediate skills. The four students had between 3 and 20 years of programming experience, had participated in up to ten programming courses, and rated their own experience between 4 and 10 (10 being the highest mark). Regarding the concerns about location privacy, two participants were quite concerned about sharing location information (scoring 20 and 18 out of a maximum of 30). The two other students were less concerned (scoring seven and nine out of a maximum of 30).

6.2. Materials and Procedure

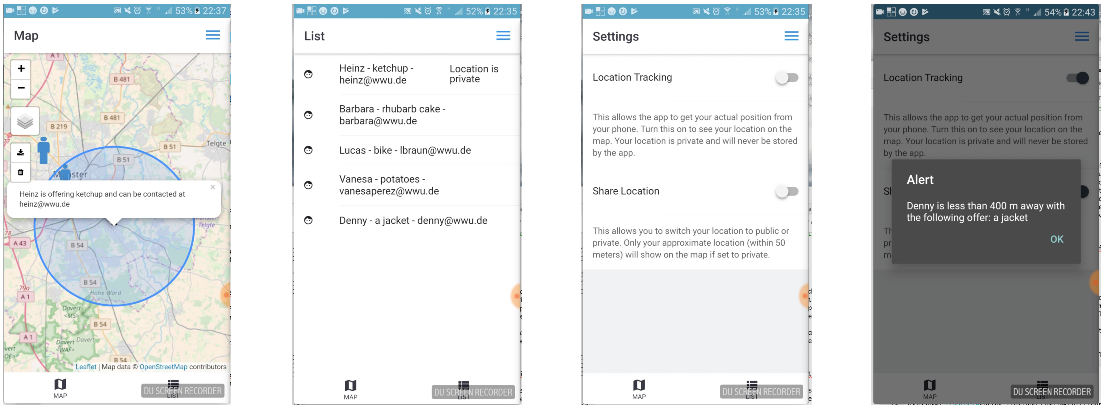
Over a period of nine weeks, the four student developers were split into two teams. The student developers were instructed to use an existing framework (LBS engine (https://github.com/LEinfeldt/LBS-Engine)) together with the guidelines introduced in Section 5 to build an example LBS of their own choice that complies with GDPR. The LBS engine is a toolkit in the sense of [36], as it provides a template which helps design location-based services. Asking participants to create example apps within about three months is a strategy for toolkit evaluation and is generally called a take-home study [37]. This approach is useful to gather some evidence on the external validity of the used tools (LBS engine and guidelines). The student developers received short introductory lectures about both tools at the beginning of the course, before starting the implementation work. We used the System Usability Questionnaire (SUS; see [38] for a recent review of its properties) to evaluate the usability of the LBS engine and the guidelines. In order to assess the effectiveness of the guidelines, we also analysed the privacy-preserving features of the developed LBS by examining the final submitted products as well as their weekly progress reports.

6.3. Results

In the following, we summarise key results of the take-home study: we describe the implementations that were produced, the privacy features that were implemented, insights into how the guidelines were perceived and used, as well as challenges and limitations we observed. While all developers received the same information, the systems and features implemented to address location privacy varied considerably between the two teams.

6.3.1. Implementations

The two teams of two students each developed two very different LBS: GeoFreebie and TourChamp. GeoFreebie (https://github.com/lbraun/geofreebie) is a location-based mobile application that helps users find and donate gifts by visualising items on a map. It is based on the idea of freecycling—recycling by giving unneeded items away to other people for free. The app provides a spatially ordered list for users to search for free items. Furthermore, GeoFreebie can notify users about gifts in their current vicinity (see Figure 3). Gifters can upload their donation data without giving their exact location in order to protect their privacy. TourChamp (https://github.com/TeKraft/TourChamp) is an LBS for newcomers to a city to find tourist spots and then test their knowledge about the new places they visit. The users can use the application map to identify tourist spots in a city and they have the possibility to take part in a multiple-choice quiz about these spots (see Figure 4). Both applications were implemented using existing open source web technologies and libraries, primarily Node.js (https://nodejs.org/en/), Apache Cordova (https://cordova.apache.org/) and Leaflet (https://leafletjs.com/).



Heinz is offering ketchup and can be contacted at heinz@wwu.de

Heinz - ketchup - heinz@wwu.de Location is private

Barbara - rhubarb cake - barbara@wwu.de

Lucas - bike - lbraun@wwu.de

Vanesa - potatoes - vanesaperez@wwu.de

Denny - a jacket - denny@wwu.de

Location Tracking

This allows the app to get your actual position from your phone. Turn this on to see your location on the map. Your location is private and will never be stored by the app.

Share Location

This allows you to switch your location to public or private. Only your approximate location (within 50 meters) will show on the map if set to private.

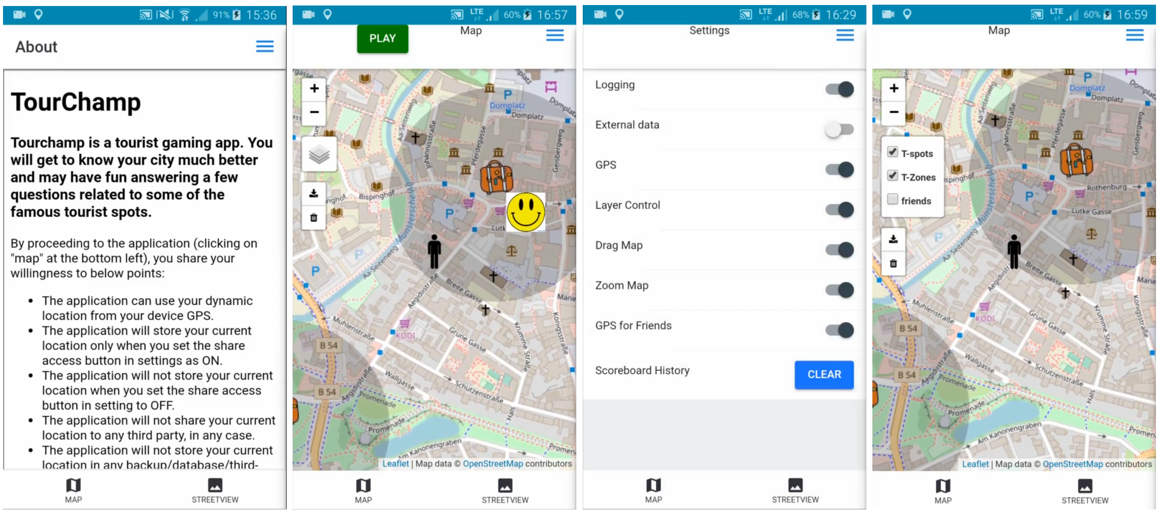
Location Tracking

This allows the app to get your actual position from your phone. Turn this on to see your location on the map. Your location is private and will never be stored by the app.

Alert

Denny is less than 400 m away with the following offer: a jacket

Figure 3. GeoFreebie (left to right): (**a**) approximate location of the users shown in a blue circle; (**b**) marked location info as private; (**c**) setting options to adjust location tracking and location sharing; (**d**) notification pop-up if the location sharing and tracking are enabled.



About

TourChamp

Tourchamp is a tourist gaming app. You will get to know your city much better and may have fun answering a few questions related to some of the famous tourist spots.

By proceeding to the application (clicking on "map" at the bottom left), you share your willingness to below points:

- The application can use your dynamic location from your device GPS.
- The application will store your current location only when you set the share access button in settings as ON.
- The application will not store your current location when you set the share access button in setting to OFF.
- The application will not share your current location to any third party, in any case.
- The application will not store your current location in any backup/database/third-

Settings

Logging	● ON
External data	○ OFF
GPS	● ON
Layer Control	● ON
Drag Map	● ON
Zoom Map	● ON
GPS for Friends	● ON
Scoreboard History	CLEAR

☑ T-spots
☑ T-Zones
□ friends

Figure 4. TourChamp (left to right): (**a**) notice; (**b**) visual indications of friends' presence when location sharing is enabled; (**c**) setting options to adjust location sharing (GPS) for public or only friends; (**d**) layered setting adjustment to enable/disable location sharing.

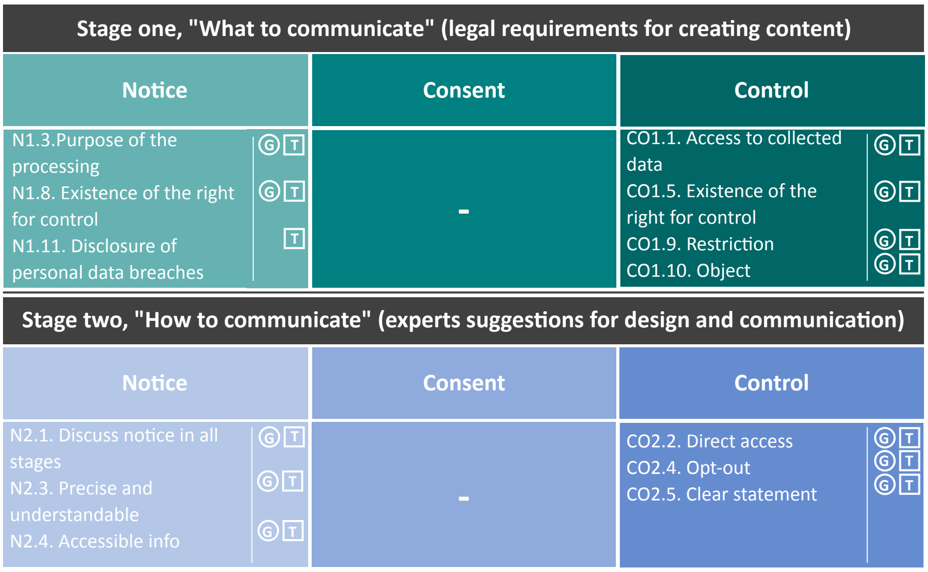
6.3.2. Location Privacy Features

Both teams were encouraged to discuss location privacy from the beginning of the process. They reported on such discussions during their progress meetings. At the beginning of the course, they believed their applications could not harm users' privacy in any way. They changed their minds after learning about the possibility of extracting personal information from location data combined with other types of data. Both teams implemented some privacy-preserving measures while developing the architecture, but they were finalised during the development and UI design stages.

GeoFreebie's developers hid the current user location by default. In the list view, the location information of users who are not willing to share their location is marked as private. Even when this option is enabled, only an approximate location of users in a zone (i.e., buffer) is shown, therefore avoiding giving the exact location of users (The technical term for this technique is obfuscation (see e.g., [14]).). The app settings screen provides users with two specific options, one for location data tracking and one for location data sharing. There are further means for users to communicate with each other (e.g., a phone number or an email address). Application users can thus reach their goal without disclosing their location data. However, enabling location sharing and tracking benefits users because the app provides pop-up notifications when they are close to a gift that is ready to be given away (Figure 3). GeoFreebie's developers designed a notice explaining how the app works and also explaining that users are in control of sharing their location. The notice implements features N1.3 and N1.8 of the guidelines. They also provide controls for users, giving them the possibility of an opt-out from location tracking and data sharing. Their implementation covers CO1.2, CO1.9, and CO1.10 of the guidelines provided in Figure 2. GeoFreebie's developers also explicitly avoided making users' exact location publicly visible. These features were implemented to build a GDPR-compliant LBS prototype.

TourChamp's developers designed a notice in the form of text explaining that location privacy can be adjusted through the settings (i.e., N1.3 and N1.8). The setting screen provides options for users to enable or disable the GPS, which will impact the location sharing directly (i.e., CO1.2, CO1.5, CO1.9, and CO1.10). Another feature in the setting is GPS for a friend. Disabling this option will stop sending users' locations to the server, and will also influence the social aspect of the game, meaning that the users will no longer be able to see other players (i.e., yellow happy faces) and they will have to continue the game individually. To adjust location privacy and stop location sharing, users are provided with an option in the main screen of the app, namely the layers button. Unchecking the friend layer (see Figure 4d) disables the location sharing of the users with others, similar to the controls available in the setting menu (i.e., fine-grained adjustment for enabling and disabling GPS for public and friends or based on different zones) (see Figure 4c).

In addition to these features for complying with GDPR, TourChamp's developers also designed and answered a set of questions for addressing location data privacy. The questions were: "What data do we collect from users?—How do we store it?—Is it prone to a breach?—Is the user aware of the data collection and storage?—Can the user withdraw/delete the shared data?—Is a user's consent taken while getting data?". Through these questions, the developers discussed (i.e., did not implemented as features) a number of items from the guidelines, such as N1.7, CO1.7, and CO1.8. Figure 5 shows each application and the features from the guidelines implemented.



Stage one, "What to communicate" (legal requirements for creating content)

Notice	Consent	Control
N1.3.Purpose of the processing G T N1.8. Existence of the right for control G T N1.11. Disclosure of personal data breaches T	-	CO1.1. Access to collected data G T CO1.5. Existence of the right for control G T CO1.9. Restriction G T CO1.10. Object G T

Stage two, "How to communicate" (experts suggestions for design and communication)

Notice	Consent	Control
N2.1. Discuss notice in all stages G T N2.3. Precise and understandable G T N2.4. Accessible info G T	-	CO2.2. Direct access G T CO2.4. Opt-out G T CO2.5. Clear statement G T

Figure 5. Recommended guidelines reflected in the two LBS developed during the take-home study: "G" and "T" indicate factors that were realised in the GeoFreebie and TourChamp LBS, respectively.

We found this technique an interesting interpretation of the proposed guidelines and in general a useful strategy to consider location privacy during the process of developing a privacy-aware and GDPR-compliant LBS. We expected that the implementation of the guidelines would be very different for both teams, leading us to conclude that some level of flexibility is needed while developing such guidelines. The features that none of the teams addressed were related to consent. The reason for this could be that the developers assumed consent should be addressed during the installation process (e.g., end user agreement). Although GDPR explicitly requires consent to be an active part of the app, the developers' decision in this study could indicate that the matter of addressing Consent needs further exploration (i.e., when and how to ask for a user's consent).

6.3.3. Usability Guidelines

We used the System Usability Scale (SUS) [39] for measuring usability of both the LBS engine and the guidelines. In order to clearly distinguish what was being evaluated, we replaced the word "system" with "GDPR guidelines" in the SUS form. We are presenting only the results for the guidelines here due to the overall focus of this article on location privacy rather than rapid prototyping of LBS.

The SUS results show that the perceived usability of the guidelines varied between developers: the SUS score [40] of the participants ranged from 35 (P2) to 55 (P1) and 65 (P4) to 72.5 (P3). The Mean SUS score was 56.9 for our study.

According to the adjective rating scale proposed by Bangor et al. [41]'s (with a SUS score lower than 12.5 corresponding to "the worst imaginable" usability and a SUS score higher than 85 representing "the best imaginable" usability), we can conclude that the overall perception of the guidelines was "Good" (i.e., higher than 50.9). Due to the low number of respondents, individual scores (e.g., the rating P2 gave) had a disproportionate impact on the mean score. While this result thus provides initial evidence that developers can use the guidelines, it also indicates the need to run further usability tests (involving higher number of developers) in order to spot usability issues as well as to refine the guidelines and their presentation.

6.3.4. Limitations and Challenges

The take-home study provides some initial insights into how the guidelines can be used to work towards GDPR compliance during LBS development. However, this study only involved four developers were involved in an academic setting. Using more developers in a commercial setting over a longer period of time would have led to deeper insights regarding trade-offs between privacy and other constraints. Nevertheless, the study showed that developers can use the guidelines during the development of a location-based service that incorporates (location) privacy-preserving features.

The study also revealed some challenges for the guidelines. The relatively low SUS scores and informal feedback indicate that the developers struggled with the guidelines. We attribute this to the overall complexity of the legal framework as well as its generality. However, the diversity of the two developed systems also highlights the need for this generality. One way to address the issues mentioned above could be to develop an interactive toolkit (or wizard) that makes it easier to identify relevant factors and potential solutions at specific points during the development process.

7. Discussion

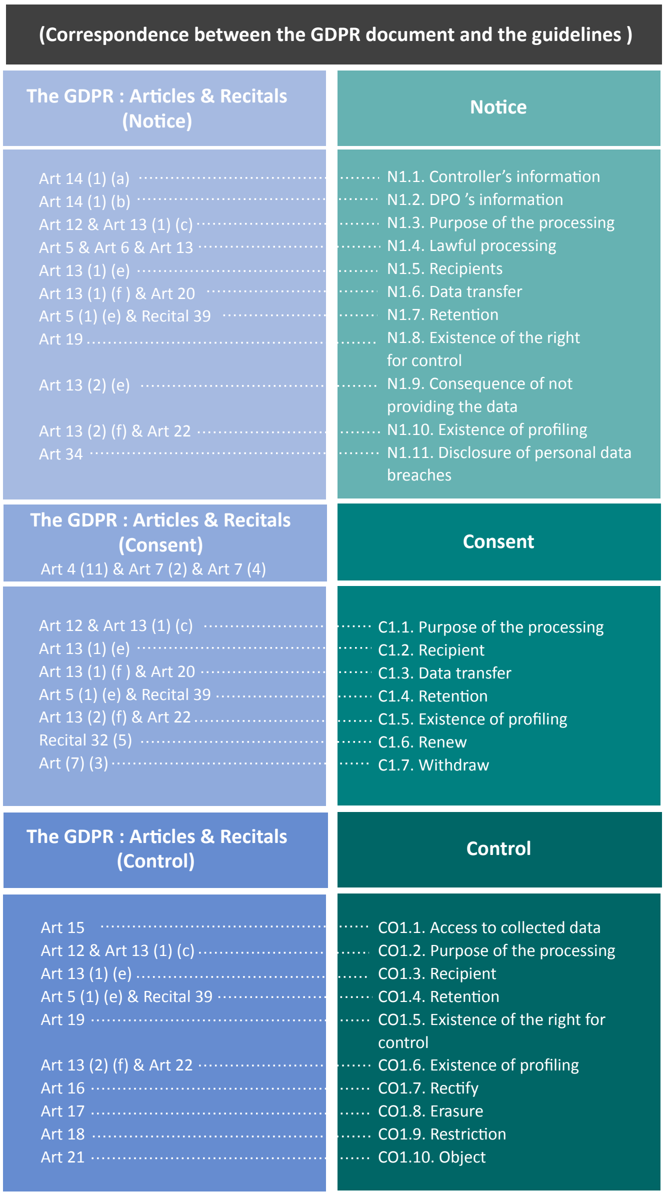
In the following, we briefly discuss key aspects relating to the GDPR and our guidelines, point out opportunities for future work, and review the limitations of our work.

7.1. Implications and Observations

The guidelines described above are based on a thorough analysis of the legal text as well as on input from experts. Our take-home study provides initial evidence that these guidelines can help designers and developers in designing UIs that provide information and interaction along the lines of what the GDPR requires. The LBS that were produced by the developers participating in our study all included features to improve the location privacy of their users (see Figure 5). While the guidelines were effective in this respect, we also found that their usability leaves room for improvements.

Many of the technical aspects included in the GDPR are more familiar to developers and are more easily mapped to technical solutions (such as using strong encryption). By separating user-facing from technical requirements (such as secure storage of personal data), these guidelines have the potential to make it easier for developers to create LBS that comply with GDPR. Though both types of requirements need to be tackled for full compliance, we only evaluated one type (user-facing requirements) in this article.

In addition, the guidelines can serve as a way to communicate between different stakeholders in the development process (designers, developers, data protection officers, legal experts, users). The guidelines are in line with Privacy by Design principles [28] and support the paradigm shift that GDPR is trying to enforce, namely pro-activeness with respect to privacy protection (rather than re-activeness). Since GDPR redefines the context for interactive development and use the discussion provided in this article helps make the peculiarities of this context explicit. In particular, the guidelines can be viewed as one way of further specifying the activity context dimension of Döweling et al. [42]'s model of interactive system design. They can be seen as rules to be followed by GDPR-compliant LBS, and could be a starting point for developing a formal model [43] that encodes specific aspects of the GDPR and then facilitates (semi-)automatic proofs of compliance. The correspondence between the guidelines and the original GDPR document are presented in Figure 6. However, given the complexity of the legislation and the topic in general, realising a comprehensive and consistent formal model of the GDPR appears to be quite a challenging task. Creating an interactive tool for developers that provides guidelines and walks developers through them might be a promising (and complementary) alternative to a formal model.



(Correspondence between the GDPR document and the guidelines)

The GDPR : Articles & Recitals (Notice)	Notice
Art 14 (1) (a)	N1.1. Controller's information
Art 14 (1) (b)	N1.2. DPO 's information
Art 12 & Art 13 (1) (c)	N1.3. Purpose of the processing
Art 5 & Art 6 & Art 13	N1.4. Lawful processing
Art 13 (1) (e)	N1.5. Recipients
Art 13 (1) (f) & Art 20	N1.6. Data transfer
Art 5 (1) (e) & Recital 39	N1.7. Retention
Art 19	N1.8. Existence of the right for control
Art 13 (2) (e)	N1.9. Consequence of not providing the data
Art 13 (2) (f) & Art 22	N1.10. Existence of profiling
Art 34	N1.11. Disclosure of personal data breaches

The GDPR : Articles & Recitals (Consent) Art 4 (11) & Art 7 (2) & Art 7 (4)	Consent
Art 12 & Art 13 (1) (c)	C1.1. Purpose of the processing
Art 13 (1) (e)	C1.2. Recipient
Art 13 (1) (f) & Art 20	C1.3. Data transfer
Art 5 (1) (e) & Recital 39	C1.4. Retention
Art 13 (2) (f) & Art 22	C1.5. Existence of profiling
Recital 32 (5)	C1.6. Renew
Art (7) (3)	C1.7. Withdraw

The GDPR : Articles & Recitals (Control)	Control
Art 15	CO1.1. Access to collected data
Art 12 & Art 13 (1) (c)	CO1.2. Purpose of the processing
Art 13 (1) (e)	CO1.3. Recipient
Art 5 (1) (e) & Recital 39	CO1.4. Retention
Art 19	CO1.5. Existence of the right for control
Art 13 (2) (f) & Art 22	CO1.6. Existence of profiling
Art 16	CO1.7. Rectify
Art 17	CO1.8. Erasure
Art 18	CO1.9. Restriction
Art 21	CO1.10. Object

Figure 6. The correspondence between the guidelines and the original GDPR document.

7.2. Future Work

The analysis presented earlier and the proposed guidelines can serve as a basis for much future work on interactive system design, including for LBS. Our findings can inform future efforts that try to standardise UI designs relevant to the context of GDPR. For example, they could be used to design a standard user interface that controls how location information is shared in an LBS. In addition, the presented guidelines point at the need for further research into three areas: effective ways of communicating privacy notices, user-friendly techniques of getting privacy consent, and truly enabling user control over their data. Previous research has already produced a design space for effective privacy notices (see e.g., [44]), but more work is needed to articulate design spaces for UI elements that are the most suitable while requesting privacy consent and control in interactive systems. The work has used expert interviews as input for the development of the guidelines, but exploring the struggles faced by developers during GDPR-implementation (e.g., through surveys, interviews or focus group studies) might provide a completely different (but complementary) take on the elements to include in the next version of the guidelines. Finally, and as said above, investigating ways of generating GDPR-derived constraints for LBS (e.g., through formal models) presents some rich opportunities for further research, on the road towards GDPR-compliant LBS user interfaces.

7.3. Limitations

Our work is subject to several limitations. The most important one is arguably that the proposed guidelines cannot guarantee that the resulting interactive system will fully comply with the GDPR. This is mainly due to the guidelines only covering a subset of the GDPR (those aspects that can be addressed at the UI level). In addition, the guidelines are at a level of abstraction that allows broad application to different systems, but this prevents very specific instructions that could be unambiguously checked. Nevertheless, we argue that the guidelines are a useful abstraction of the legal text that provide designers and developers with guidance towards realising a GDPR-compliant system. Although our evaluation took place during the actual development of two LBS, it was clearly limited in terms of duration, number of participants, and the diversity of applications that were developed. Nevertheless, it provides initial insights into how the guidelines are used during development.

Furthermore, the article has not discussed responsibilities when it comes to actually realising these guidelines in practice. The challenge of who is responsible for implementing GDPR was also one of the discussion points in the interviews. E3 and E7 agreed on the strategy of bringing together a group of individuals, developers, designers, ethical advisers and service providers. On the other hand, E1 believed that "this (i.e., compliance with GDPR) is not designers' responsibility, the one who is responsible for the project is also the main responsible person for GDPR compliance first". In the view of E2, the government should take the responsibility for implementing GDPR in both the public and private sectors, while E3 had a different opinion, mentioning that GDPR implementation requires hiring data protection officers (DPO) and stressing that "they are going to be the main channel of communicating with data protection authorities...". It is acknowledged here that the question of who will implement the guidelines? is important for GDPR-compliant interactive systems, but that question is not discussed further in this article since it involves institutional concerns which are not the main focus of this work.

Finally, we have not discussed how technical solutions currently available (e.g., [45]) could be adapted to support the implementation of GDPR. Guidelines about technical solutions which are in line with GDPR's requirements (or strategies to fine-tune them for the goals of GDPR) are also an important aspect which could ease the life of developers but exploring them was beyond the scope of this study. As said at the outset of the article, one of the contributions of this study was to present a way for extracting relevant principles from GDPR for a specific purpose, which is UI design in LBS. Technical aspects of protecting location privacy of users were thus not explored in detail (even though the developed applications in Section 6 used a few of such technical measures).

8. Conclusions

Privacy legislation such as the General Data Protection Regulation (GDPR) can be a big challenge for developers who have to implement systems that comply with it. Understanding the legal text already requires a lot of effort, but legal frameworks also do not include specific instructions about how to realise compliant software. In this article, we report on work to address this gap between the legislation and the implementation, with a particular focus on location privacy and location-based services. We analysed the legal text of the GDPR and extracted key aspects (i.e., challenges and approaches) relating to creating compliant interactive systems. In addition, we carried out interviews with experts to identify key challenges and issues developers face when building privacy-aware software. Based on the outcomes of the analysis and the interviews, we formulated guidelines for designers and developers to help them create systems that comply with the GDPR. In our work, we focused on location data and legislation aspects that require user interaction (i.e., privacy regulations that relate to the user interface). The guidelines are grouped into two stages (what to communicate and how to communicate it) and into three groups (notice, consent, control) that are directly derived from the GDPR. The usefulness of these guidelines was demonstrated through their application to the development of an interactive location-based service in a take-home study. The guidelines can inform the standardisation of GDPR-compliant user interface (UI) designs, such as a dialogue for location sharing that includes all necessary functionality and visualises all legally required information. In addition, the guidelines can be used by interactive system developers as a starting point for their work on GDPR-compliant interactive systems.

Author Contributions: Conceptualization, M.A., A.D., C.K. and V.S.; Data Curation, M.A.; Investigation, M.A.; Methodology, M.A., A.D. and C.K.; Project Administration, C.K. and V.S.; Supervision, C.K.; Visualization, M.A.; Writing—Original Draft, M.A., A.D. and C.K.

Funding: European Union through the GEO-C project (H2020-MSCA-ITN-2014, Grant Agreement Number 642332, http://www.geo-c.eu/).

Acknowledgments: The authors gratefully acknowledge funding from the European Union through the GEO-C project (H2020-MSCA-ITN-2014, Grant Agreement Number 642332, http://www.geo-c.eu/). We also thank the participants in the interviews and the take-home study for their very useful input, and the anonymous reviewers for their constructive comments and suggestions.

Conflicts of Interest: No conflicts of interest to declare.

Abbreviations

The following abbreviations are used in this manuscript:

GDPR	General Data Protection Regulation
IS	Information Systems
LBS	Location Based Services
UI	User Interface
NCC	Notice, Consent, Control
DPO	Data Protection Officer

Appendix A. Summarised Analysis of NCC Factors

Appendix A.1. Notice

GDPR requires the ensuring of lawful, fair and transparent processing of personal data. According to the recital 60 of GDPR [5], the processing is fair and transparent if the data subject is informed of the existence of the processing and its purposes. The controller should provide data subjects with the information that is listed in Art. 13 of GDPR regarding personal data collection from the data subject: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second sub paragraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. In addition to the list, data subjects should also be informed about: (a) the period for which their personal data will be stored, or if that is impossible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject Art.13—[5].

As mentioned in the previous paragraph, data subjects should be informed in the case of profiling, but according to recital 60, data subjects should also be informed about the consequences of both accepting the processing and objecting to it in the case of profiling. Data subjects should be also informed if any data breach occurs, according to Art. 34: *"when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay"*. The subjects should also be instructed to take steps to mitigate the damage after the communication of the incident [5].

Informing data subjects about their rights, the consequences of their decisions, and the activities of the controller can ensure fairness and transparency regarding the lawfulness of the processing. GDPR considers the processing lawful if *"the data subject has given consent to the processing of his or her personal data for one or more specific purposes"* or processing is necessary for various reasons such as *"compliance with legal obligation"* or *"for the performance of a task carried out in the public interest"* Recital 60—[5].

Article 19 adds another aspect to the list of information that data subject should be informed about, namely *The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.*

Appendix A.2. Consent

According to the GDPR, consent is one of the fundamental principles to make data processing activities lawful. Article 4, defines consent of data subjects as *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her* [5]. Article 7 defines conditions for the consent such as (1) where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data and (2) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. Recital 42 also lists some requirements for consent: *for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*

The consent should communicate the processing activities with data subjects which is similar to notice, but the primary difference is that the consent requires active approval and confirmation from data subjects. It also needs to be flexible to support the features of withdrawal (i.e., the right of opting out from data processing) and renewal (i.e., receiving an updated consent when the purpose of the processing has changed).

Appendix A.3. Control

GDPR stresses the importance of providing data subjects with control over their personal data. Control includes various principles such as the right of access, the right to rectification and erasure, the right to restriction, the right to data portability and the right to object. We will briefly explain the legal requirements for each.

- Access—according to Art. 15: The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Rectification—Art. 16: The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- Erasure ("right to be forgotten"): 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 without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
- Restriction of processing—Art 18: The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
- Data portability—Art 19: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided Art 20.
- Object—Art. 21: The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates

> compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Appendix B. Expert Interviews' Scripts

Hi. My name is .... I'm a researcher in a project called .... I'm mainly working with digital privacy—More specifically location privacy, so I'm working on how we can build services which function based on location information that give users service but at the same time protect their location privacy. What we are going to talk about today is more related to building interactive systems in general, by interactive systems I mean any system that its operation involves user interaction and also New "GDPR" General data protection regulation. These new regulations will come to action this May as you probably heard. Thus, developers and designers are developing and building systems and services, but then these new privacy related regulations are out there and companies expect them to be aware about them and avoid trouble of not complying with GDPR. Thus, the topic of this talk is exactly about this: New General Data Protection Regulations and developers challenges understanding and implementing them.

GDPR is a long document with so many aspects, I will focus on only a few aspects and we will go through the legal explanation of each together and then I will ask your opinion about each of them? My main concern is about location information and how we can manage that while designing a service.

Q1. What is your role? What do you do? And please let me know if you have any experience or ongoing project regarding GDPR? At the end of this interview, we will decide if you want this to be mentioned or not.

Q2. How do you see the challenge of complying with GDPR while developing interactive systems?

Q3. What do think the difficulties are for developers and designers in this context?

Q4. There are some guidelines out there. Do you know any material you could recommend to a developer trying to implement GDPR?

Q5. In which stage do you think a system designer or developer should address notice, consent and control? why?

Q6. What should be included in notice, consent and control?

Q7. What would you say is the best way to communicate notice, consent and control with end users?

References

1. Krumm, J. A survey of computational location privacy. *Personal Ubiquitous Comput.* **2009**, *13*, 391–399. [CrossRef]
2. Clarke, R.; Wigan, M. You are where you've been: The privacy implications of location and tracking technologies. *J. Locat. Based Serv.* **2011**, *5*, 138–155. [CrossRef]
3. Lin, Y.W. # DeleteFacebook is still feeding the beast–But there are ways to overcome surveillance capitalism. *The Conversation*, 26 March 2018.
4. Michael, K.; Michael, M.G. The social and behavioural implications of location-based services. *J. Locat. Based Serv.* **2011**, *5*, 121–137, doi:10.1080/17489725.2011.642820. [CrossRef]
5. European Union. *Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) (General Data Protection Regulation)*; European Union: Brussels, Belgium, 2016.
6. Newman, A.L. What the "right to be forgotten" means for privacy in a digital age. *Science* **2015**, *347*, 507–508. [CrossRef] [PubMed]

7. Huang, H.; Gartner, G.; Krisp, J.M.; Raubal, M.; Van de Weghe, N. Location based services: Ongoing evolution and research agenda. *J. Locat. Based Serv.* **2018**, 1–31. [CrossRef]
8. Westin, A.F. Social and political dimensions of privacy. *J. Soc. Issues* **2003**, *59*, 431–453. [CrossRef]
9. Solove, D. *Understanding Privacy*; Harvard University Press: Cambridge, MA, USA, 2008.
10. Solove, D.J. Conceptualizing privacy. *Cal. Law Rev.* **2002**, *90*, 1087. [CrossRef]
11. Keßler, C.; McKenzie, G. A geoprivacy manifesto. *Trans. GIS* **2018**, *22*, 3–19. [CrossRef]
12. McKenzie, G.; Janowicz, K.; Seidl, D. Geo-privacy beyond coordinates. In *Geospatial Data in a Changing World—Selected Papers of the 19th AGILE Conference on Geographic Information Science*; Sarjakoski, T., Santos, M.Y., Sarjakoski, L.T., Eds.; Springer: Helsinki, Finland, 2016; pp. 157–175. [CrossRef]
13. Fawaz, K.; Feng, H.; Shin, K.G. Anatomization and protection of mobile apps' location privacy threats. In Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), Washington, DC, USA, 12–14 August 2015; USENIX Association: Berkeley, CA, USA, 2015; pp. 753–768.
14. Duckham, M.; Kulik, L. Location privacy and location-aware computing. In *Dynamic and Mobile GIS: Investigating Changes in Space and Time*; Billen, R., Joao, E., Forrest, D., Eds.; CRC Press: Boca Raton, FL, USA, 2006; Chapter 3, pp. 35–51.
15. Danculovic, J.; Rossi, G.; Schwabe, D.; Miaton, L. Patterns for personalized web applications. In Proceedings of the 6th European Conference on Pattern Languages of Programms (EuroPLoP '2001), Irsee, Germany, 4–8 July 2001; Rüping, A., Eckstein, J., Schwanninger, C., Eds.; UVK—Universitaetsverlag Konstanz: Irsee, Germany, 2001; pp. 423–436.
16. Kobsa, A. Privacy-enhanced personalization. *Commun. ACM* **2007**, *50*, 24–33. [CrossRef]
17. Abbas, R.; Michael, K.; Michael, M. The regulatory considerations and ethical dilemmas of location-based services (LBS): A literature review. *Inf. Technol. People* **2014**, *27*, 2–20. [CrossRef]
18. Perusco, L.; Michael, K. Control, trust, privacy, and security: evaluating location-based services. *IEEE Technol. Soc. Mag.* **2007**, *26*, 4–16. [CrossRef]
19. Layton, R.; Celant, S. How the GDPR compares to best practices for privacy, accountability and trust. *SSRN Electron. J.* **2017**, 1–23. [CrossRef]
20. Raschke, P.; Axel, K.; Drozd, O.; Kirrane, S. *Designing a GDPR-Compliant and Usable Privacy Dashboard*; Springer: New York, NY, USA, 2017; pp. 1–13.
21. Lindqvist, J. New challenges to personal data processing agreements: Is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *Int. J. Law Inf. Technol.* **2017**, 45–63. [CrossRef]
22. Sweeney, L. k-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl. Based Syst.* **2002**, *10*, 557–570. [CrossRef]
23. Beresford, A.R.; Stajano, F. Location privacy in pervasive computing. *IEEE Pervasive Comput.* **2003**, *2*, 46–55. [CrossRef]
24. Mokbel, M.F.; Chow, C.Y.; Aref, W.G. The new casper: Query processing for location services without compromising privacy. In Proceedings of the 32nd International Conference on Very Large Data Bases, Seoul, Korea, 12–15 September 2006; pp. 763–774.
25. Memon, I.; Chen, L.; Arain, Q.A.; Memon, H.; Chen, G. Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks. *Int. J. Commun. Syst.* **2018**, *31*, e3437. [CrossRef]
26. Memon, I.; Arain, Q.A.; Memon, M.H.; Mangi, F.A.; Akhtar, R. Search me if you can: Multiple mix zones with location privacy protection for mapping services. *Int. J. Commun. Syst.* **2017**, *30*, e3312. [CrossRef]
27. Langheinrich, M. A privacy awareness system for ubiquitous computing environments. In Proceedings of the International Conference on Ubiquitous Computing, Göteborg, Sweden, 29 September–1 October 2002; Springer: Berlin, Springer, 2002; pp. 237–245.
28. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*; Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2009.
29. Ataei, M.; Degbelo, A.; Kray, C. Privacy theory in practice: Designing a user interface for managing location privacy on mobile devices. *J. Locat. Based Serv.* **2018**, 1–38. [CrossRef]
30. Hornbæk, K.; Oulasvirta, A. What is interaction? In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI'17), Denver, CO, USA, 6–11 May 2017; Mark, G., Fussell, S.R., Lampe, C., Schraefel, M.C., Hourcade, J.P., Appert, C., Wigdor, D., Eds.; ACM Press: Denver, CO, USA, 2017; pp. 5040–5052. [CrossRef]

31. Conger, S.; Pratt, J.H.; Loch, K.D. Personal information privacy and emerging technologies. *Inf. Syst. J.* **2013**, *23*, 401–417. [CrossRef]
32. Wordart. Available online: https://wordart.com/ (accessed on 10 October 2018).
33. Hsieh, H.F.; Shannon, S.E. Three approaches to qualitative content analysis. *Qual. Health Res.* **2005**, *15*, 1277–1288. [CrossRef] [PubMed]
34. Bargiotti, L.; Gielis, I.; Verdegem, B.; Breyne, P.; Pignatelli, F.; Smits, P.; Boguslawski, R. *Guidelines for Public Administrations on Location Privacy*; Technical Report; Publications Office of the European Union: Luxembourg, 2016.
35. Centers for Medicare & Medicaid Services. *Selecting a Development Approach*; Centers for Medicare & Medicaid Services: Baltimore County, MD, USA, 2008; pp. 1–10.
36. Olsen, D.R. Evaluating user interface systems research. In Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology (UIST'07), Newport, RI, USA, 7–10 October 2007; Shen, C., Jacob, R.J.K., Balakrishnan, R., Eds.; ACM Press: Newport, RI, USA, 2007; pp. 251–258. [CrossRef]
37. Ledo, D.; Houben, S.; Vermeulen, J.; Marquardt, N.; Oehlberg, L.; Greenberg, S. Evaluation strategies for HCI toolkit research. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI'18), Montreal, QC, Canada, 21–26 April 2018; Mandryk, R.L., Hancock, M., Perry, M., Cox, A.L., Eds.; ACM Press: Montreal, QC, Canada, 2018; pp. 1–17. [CrossRef]
38. Brooke, J. SUS: A Retrospective. *J. Usability Stud.* **2013**, *8*, 29–40.
39. Lewis, J.R.; Sauro, J. The factor structure of the system usability scale. In Proceedings of the International Conference on Human Centered Design, San Diego, CA, USA, 19–24 July 2009; Springer: Berlin, Springer, 2009; pp. 94–103.
40. Brooke, J. SUS-A quick and dirty usability scale. *Usability Eval. Ind.* **1996**, *189*, 4–7.
41. Bangor, A.; Kortum, P.; Miller, J. Determining what individual SUS scores mean: Adding an adjective rating scale. *J. Usability Stud.* **2009**, *4*, 114–123.
42. Döweling, S.; Schmidt, B.; Göb, A. A model for the design of interactive systems based on activity theory. In Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (CSCW'12), Seattle, WA, USA, 11–15 February 2012; Poltrock, S.E., Simone, C., Grudin, J., Mark, G., Riedl, J., Eds.; ACM Press: Seattle, WA, USA, 2012; pp. 539–548. [CrossRef]
43. Ivory, M.Y.; Hearst, M.A. The state of the art in automating usability evaluation of user interfaces. *ACM Comput. Surv. (CSUR)* **2001**, *33*, 470–516. [CrossRef]
44. Schaub, F.; Balebako, R.; Durity, A.L.; Cranor, L.F. A design space for effective privacy notices. In Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), Ottawa, ON, Canada, 22–24 July 2015; pp. 1–17.
45. Memon, I.; Mirza, H.T. MADPTM: Mix zones and dynamic pseudonym trust management system for location privacy. *Int. J. Commun. Syst.* **2018**, e3795. [CrossRef]