The EU General Data Protection Regulation and its Effects on Designing Assistive Environments

Erik Krempel
Fraunhofer IOSB
Karlsruhe, Germany
erik.krempel@iosb.fraunhofer.de

Jürgen Beyerer
Fraunhofer IOSB
Karlsruhe, Germany
juergen.beyerer@iosb.fraunhofer.de

ABSTRACT
On the 25th of May 2018 the EU will start to enforce the General Data Protection Regulation (EU-GDPR)[3]. This new regulation will replace the old Data Protection Act from 1998 and will disrupt common data processing practices. While the new regulation will make it easier to develop systems that comply with data protection laws all over Europe, it will change the way we design technology. With data protection a much more important factor and huge fines for data protection violations, technology vendors will demand systems where data protection was already considered during development. This will force the research community to broaden their perspective and consider how to develop and design systems in a way, that complies with data protection. This paper focuses on some of the more important parts of the GDPR for Assistive Environments. Reading the paper will not solve all your privacy related challenges but will help you to know which questions to ask.

CCS CONCEPTS
• Security and privacy → Privacy protections; Social aspects of security and privacy; Usability in security and privacy;

KEYWORDS
privacy, GDPR, privacy by design, data protection

1 INTRODUCTION
Privacy by Design, the engineering discipline of designing a system in a way that allows it to fulfill some user’s demands combined with a high level of data protection, has only sparked little interest outside the privacy community. With the GDPR regulation, this will have to change.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2018 Copyright held by the owner/author(s). Publication rights licensed to Association for Computing Machinery.
ACM ISBN 978-1-4503-6390-7/18/06...
https://doi.org/10.1145/3197768.3201567
See this paper as a summary of privacy requirements you will have to keep in mind in the near future. Whenever processing personal information consult a legal expert for the legal requirements applicable to your situation.

2 DEFINING AN ABSTRACT ASSISTIVE ENVIRONMENT

Before we start going into the finer details of the GDPR let us introduce what we understand as Assistive Environment and its data processing [6]. We assume that an Assistive Environment will have one or many sensors that will collect real-time information of a user. The sensors could be cameras, wireless connected tools or any other kind of sensor. The data collected by this sensors will be processed in real-time and give the system some information about the users, their location and actions. Additionally, we assume that a typical Assistive Environment will have some persistent user profile. Depending on the use case, the system might need to know if its users are left or right handed or what qualifications they have.

As a concrete example of an abstract Assistive Environment we introduce the heavily simplified manufacturing system tight screw. In a production process, a worker has to check multiple fittings on a piece of equipment using a wireless torque tester (sensor). The different fittings require different maximum torques and every fitting has to be tested. A camera (sensor) registers the user’s position, which fitting is tested and what the current torque of the tester is. As the equipment is of high relevance for safety, think of a jet turbine, only specific workers are certified (user profile) to perform this final test. The system uses a face identification to check if the current user has a valid certification. Once all fittings are tested successfully, the next piece of equipment is presented for testing.

2.1 Definitions in the GDPR

Not all data is protected by the GDPR, it is only applicable for personal data. This is defined in Article 4 as follows:

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

Considering this definition, it is reasonable to assume, that every Assistive Environment imaginable in manufacturing will process personal data and therefore will have to comply with the GDPR. If, for example, a shift plan lets you know which employee operated a machine at a given time, all data from this interaction has to be considered personal data.

Whenever we speak of personal data, this data belongs to a user, called data subject in the GDPR. The legal entity processing data is called a controller and is in charge to meet the requirements defined by the GDPR. Many of the rights and obligations in the GDPR only exist between the data subject of a piece of personal data and the controller. When we write that a subject has the right to understand how personal data is processed, this is only true for the data concerning this subject. A controller has to explain what he is going to do with your data, not the data of all other users of a service.

3 THE GDPR AND ITS MEANING FOR ASSISTIVE ENVIRONMENTS

In the following section we will have a closer look on a small number of selected Articles with high relevance for Assistive Environments.

3.1 Lawful data processing and consent

One of the key aspects ofdata processing in general and the GDPR in particular is that processing of personal data is prohibited until otherwise legalized. The GDPR Article 6 sees six different reasons that allow the processing of personal data:

- Consent: The data subject has given consent to the data processing.
- Contract: The data processing is necessary for the performance of a contract of which the data subject is party.
- Legal obligation: The data processing is necessary for compliance with legal obligations.
- Vital interests: The data processing is necessary to protect vital interests of the data subject or of another natural person.
- Public interest: The data processing is necessary for the public interest or in the exercise of public authorities vested in the controller.
- Legitimate interest of the controller: The data processing is necessary for a legitimate interest of the controller and not challenged by the interests or fundamental rights and freedoms of the data subject.

In this paper, we will focus on the first case, where a data subject has given explicit consent to the data processing. This is the most common case in Assistive Environment, be it a Smart Home application or in manufacturing. Before a user starts using your system and at the same time the system starts to process the user’s personal data, he or she has to understand what data is collected, processed for what purpose and give explicit consent to it. The regulations sets high demands on the information basis the subjects gets before and after giving his consent. The information provided has to be in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12). This will present a challenge on how to communicate with users what data is processed for what purpose. Currently it is unclear how to provide this level of detail without presenting the user with extensive privacy policies that will not meet the requirement of clear and plain language.

A second challenge with consent is that consent has to be given freely. Meaning that you are not allowed to force a user to share personal information that has no direct effect on your system. So far, we do not know if a user can still decide freely, i.e., in the legal definition without outside pressure, if he or she uses an Assistive Environment the workplace. The obligation to use a system, i.e., our example “tight screw” as a quality control system in a manufacturing environment, will most likely prevent a user to give consent freely. At the same time, the employer could argue, that the quality control system is important to guarantee safety and therefore important for vital interests of another legal person.
As already mentioned, the user has to give his or her consent for a specific purpose. This purpose should be defined as specific as possible, e.g., “using cameras to monitor user interaction in an assembly step for quality control” instead of “assistive functionality.” Keep in mind that this purpose is of high legal relevance. You are not allowed to use data outside the specific purpose presented to the user. So if you defined the purpose of the system as “quality control in an assembly step” you are not allowed to use the data for other purpose, e.g., compare the efficiency of different workers. While this seems trivial in the design of a system, we often see that once a system is installed other stakeholders show interest in the collected data. So you will either have to prevent them from accessing your data or you will have to adapt the information you provide your users. In any case, you have to delete the collected data once the purpose is fulfilled.

3.2 Transparency and Control
The GDPR puts a high focus on consent, transparency and control of the data subjects. As mentioned earlier (cf. section 3.1) this work will assume that the data subjects have given explicit consent to the data processing. Here we will give a short overview of data subjects’ rights and the controllers obligations defined in Article 12 - 23 of the GDPR.

As long as personal data is processed by a controller the data subject has a right to access this data (Article 15). Additionally the subject has a right to rectification of personal data (Art. 16) and the right to request a restriction of processing (Article 18) or deletion (Article 17). Last but not least the user has a right to data portability (Article 20), meaning he or she can request to receive all personal data in a structured, commonly used and machine-readable format.

Of course, all these rights come with certain requirements and balances where the rights of the controller and the subject are considered. A subject cannot demand deletion of a bill and thus escape payment or chance data in a way that prevents the controller from fulfilling his legal obligations.

Still the users have more rights and systems have to be designed in a way to allow a much higher level of transparency and control. Consider that you will have to communicate what data is processed, transmitted and stored. Have a concept how the subject can inspect, alter and export his or her personal data.

4 AUTOMATED INDIVIDUAL DECISION-MAKING
The aim of Article 22 is to prevent automated decisions and especially profiling that might have a negative effect on the subject. The article is motivated by the fear of systems that make unfair decisions that the subject can not protest. A good example for such a system is an biased automated credit scoring. A subject might not be able to receive a loan solely by living area, the credit rating of friends or his or her gender.

While profiling is mostly irrelevant for Assistive Systems the article still represents some design challenges. Systems have to meet certain criteria to make automated decisions legal. Here we assume that a subject has given his or her explicit consent into the data processing (compare section 3.1) and therefore the system fulfills Article 22 (2) c).

More important is Article 22 (3) and the right of the data subject. The data controller has to make sure, that the subjects’ rights and freedoms are protected by the design. This is especially important if the system comes to a decision that the subject might not like, e.g., giving a bad quality rating to a manufactured product. Here you will need to check if your design incorporates the users’ rights in an appropriate way. The subject must have the right to obtain human intervention on the part of the controller to contest the decision.

If a decision of your system has a broader influence on the right of the subject, i.e., the system declines payment due to low quality of a manufacturing step, an automated decision should be avoided altogether. A good solution in this cases could be to present available data to a third person and let them decide (a. k. a. human-in-the-loop).

4.1 Data Protection by Design and by Default
Article 25 of the GDPR demands a fundamental change in the design of technology. Instead of thinking about privacy after a product is developed, data protection should be considered early in the development. This again strengthens the demand for researches to think about data protection in the development of systems to enable latter usage of the designed technology with costly changes. Two concepts for development are named in the heading: “Data protection by design” and “data protection by default”. Interestingly, these concepts, while well known in the privacy community, represent the goal of a development and not how to reach it. The well-known publication from Ann Cavoukian “Privacy by Design: The 7 Foundational Principles” gives a good idea what the goal of the development should be [2]. Since the initial publication multiple research groups have done work on Privacy by Design an how to integrate it into an design process [1, 5, 7]. Here we are going to quote the original 7 Principles and give some context what they mean for system development.

4.1.1 Proactive not Reactice - Preventive not Remedial.
“The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen.”

The first principle is in strong consensus with the GDPR. Data protection should be a proactive measure. You should think about data protection before data is collected. Only this will allow you to anticipate problems before they occur and design your system in a way that will not require elaborate and most likely costly chances in the future.

4.1.2 Privacy as the Default Setting.
“We can all be certain of one thing - the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.”

The second principle represents “data protection by default” as demanded by the GDPR. Privacy should be your default setting. System or to be more precise their users are not prohibited to share their data. But if your system can operate in different modes, one
sharing a lot of data with other systems and the second mode not sharing at all, a new user should automatically start with the more privacy friendly setting.

4.1.3 Privacy Embedded into Design.

"Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact."

This principle emphasizes again, that data protection must be part of the initial design and not a feature that will be added later.

4.1.4 Full Functionality – Positive-Sum, not Zero-Sum.

"Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, [...] it is possible, and far more desirable, to have both [functionality and privacy]."

Principle number four is the most ambitious but at the same time challenging principles. Privacy, like many other “second level requirements” such as environment protection or safety, often is seen as added cost that will reduce the functionality of a product. In many cases this is the fault of a bad design or insufficient knowledge about the technology. In the past, environment protections has shown how, with enough motivation and research, you can have an environment friendly technology that is better and cheaper than the alternatives. The same should be possible in the field of data protection. In many applications, you can combine data protection with the intended functionality. If data protections minimizes the amount of data you have to collect, process and store, you system gets simpler and therefore cheaper to build. Of course, there are systems where functionality and privacy will not increase at the same time. Especially business cases that are based on the trading of personal data will not profit from more data protection. At the same time, this seems to be less important in the area of Assistive Environments. Thus, we will not try to solve this dilemma.

4.1.5 End-to-End Security – Full Lifecycle Protection.

"Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved - strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end:"

We completely agree with this principle and think that every designer should build systems that protect data all the way from collection to deletion.

4.1.6 Visibility and Transparency - Keep it Open.

"Knowing what is going on with one’s personal data is a fundamental precondition for using one’s legal right to informational self-determination. From a user’s perspective, without transparency any other privacy measures do not take effect."

Principle number six shows how strong the GDPR and most other data protection laws are focused on transparency. Data protection is not about preventing data processing but about control. A data subject must understand how personal data is processed and have control over this processing. This is best enabled by systems with a high level of transparency.

4.1.7 Respect for User Privacy - Keep it Individual and User-Centric.

“Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!”

Only if privacy features are easy to use, users are able to act in a consistent way. This also means that the needs of different users have to be considered. If the users have only limited time to understand and configure a system to their need, i.e., because it is installed at their workplace and they should work with it not spend their day configuring it, the system has to be much simpler than a system designed for a private area.

5 CONCLUSIONS

In this paper we introduced the European General Data Protection Regulation and its effects on Assistive Environments. While far from solving the upcoming privacy challenges, we hope that this work can help researches to understand the regulation and its basic workings. The paper gives a short introduction into transparency, control and consent as well as some of the more important user rights. Many advanced aspects, such as the right to be forgotten or Privacy Impact Assessments are also highly relevant for the field of manufacturing, but unfortunately out of the scope for this work.

ACKNOWLEDGMENTS

This work was partially funded by the KASTEL project (16KIS0521) and the GUIDE project (16SV7891) of German Federal Ministry of Education and Research, BMBF.

REFERENCES