# Making GDPR Usable: A Model to Support Usability Evaluations of Privacy* **

Johanna Johansen*** [1][0000−0003−4908−9045] and Simone Fischer-Hübner[2]

[1] Department of Informatics, University of Oslo.
johanna@johansenresearch.info
[2] Department of Mathematics and Computer Science, Karlstad University.
simone.fischer-huebner@kau.se

**Abstract.** We introduce a new model for evaluating privacy that builds on the criteria proposed by the EuroPriSe certification scheme by adding usability criteria. Our model is visually represented through a cube, called Usable Privacy Cube (or UP Cube), where each of its three axes of variability captures, respectively: rights of the data subjects, privacy principles, and *usable privacy criteria*. We slightly reorganize the criteria of EuroPriSe to fit with the UP Cube model, i.e., we show how EuroPriSe can be viewed as a combination of only *rights* and *principles*, forming the two axes at the basis of our UP Cube. In this way we also want to bring out two perspectives on privacy: that of the data subjects and, respectively, that of the controllers/processors. We define usable privacy criteria based on usability goals that we have extracted from the whole text of the General Data Protection Regulation. The criteria are designed to produce measurements of the level of usability with which the goals are reached. Precisely, we measure effectiveness, efficiency, and satisfaction, considering both the objective and the perceived usability outcomes, producing measures of accuracy and completeness, of resource utilization (e.g., time, effort, financial), and measures resulting from satisfaction scales. In the long run, the UP Cube is meant to be the model behind a new certification methodology capable of evaluating the *usability of privacy*, to the benefit of common users. For industries, considering also the usability of privacy would allow for greater business differentiation, beyond GDPR compliance.

**Keywords:** usable privacy · Human-Computer Interaction · usability goals · usable privacy criteria · privacy certification · GDPR.

## 1 Introduction

The complexity of the privacy concept as such and of digital data and technology, make it difficult for one to evaluate the privacy properties of a specific

* A long version of this paper is available as [17].

** We would like to thank the anonymous reviewers for helping improve the paper.

*** The first author was partially supported by the project IoTSec – Security in IoT for Smart Grids, with nr. 248113. Thanks go also to Josef Noll for introducing me to the topic of privacy evaluations and labeling.

piece of technology (e.g., web service, Internet of Things (IoT) product, or communication device). The difficulty is not only for average people, but also for regulators to check compliance, and for developers to be able to provide privacy-aware digital services/products/systems.[3] Indeed, there are multiple concepts involved in digital privacy, like data sharing (which for normal business practices nowadays can form a highly intricate network of relationships), ownership and control of data, accountability or transparency (both towards the regulators as well as the users). Many of the privacy concepts are even a challenge by themselves, when it comes to their evaluation, since they are difficult to measure or to present/explain.

For explaining the intricacies of privacy, besides research articles and books [13], there are several legislative texts adopted in different jurisdictions. The General Data Protection Regulation (GDPR)[4] in Europe makes a good effort in clarifying many aspects of data privacy, providing the legislative support to enforce better data protection practices on anyone (within its jurisdiction) collecting and processing personal data. However, these regulations only specify the requirements on the data controllers in the form of basic principles, and the rights of the data subjects, but do not make any strict claims about the extent to which a controller (or processor) should go about implementing these requirements so that they are beneficial for the user, and to what degree.

As such, one motivation for usability evaluations of privacy is the fact that usability goals of GDPR, s.a. "... any information ... and communication ... relating to processing [to be provided] to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, ..." (Article 12 (1) of GDPR), are left open to the subjective interpretation of both evaluators and controllers. The provisions of GDPR regarding usability are too general and high-level to be suitable for a certification process [18]. To remedy this, we propose a set of criteria thought to produce measurable evaluations of the usability with which privacy goals of data protection are reached.

For evaluating privacy we take as starting point the methodology developed by EuroPriSe [3] that has as purpose to evaluate compliance with GDPR. We are guided by the EuroPriSe criteria when eliciting, what we call, *principles* and *rights*, which form the two variability axes at the basis of our model, i.e., which principles are followed and which rights are respected. However, EuroPriSe does not consider usability, which is the main focus of our work here. As such, one contribution of this paper is to show how to add usability aspects to the existing evaluation criteria of EuroPriSe.

Unlike EuroPriSe (and other existing certification schemes) that provides a seal showing compliance with data protection regulations (or industry standards), our evaluation measures on a scale how well data protection obligations are respected and how easy it is for a user to understand that. The measurements can be presented to the user in different ways, e.g., using "traffic light" scales, showing which level of usability has been reached by the privacy of a certain

[3] Note that system/product/service are used interchangeably throughout the paper.
[4] GDPR – General Data Protection Regulation from European Union [1].

technological product. A "traffic light" presentation of privacy is recommended by [2, Chapter 6(235)] as a way to "foster competition" and "show good practice on privacy policies".

Traditionally, usability is a quality related to the use of a product. In our case, we are not interested in the usability of a product per se, but only in those aspects of a product that concern privacy. Our conceptualization of usable privacy is based on the definition of usability as presented in the ISO 9241-11:2018 [4], which we adapt to include privacy as follows:

> *Usable privacy* refers to the extent to which a product or a service protects the privacy of the users in an efficient, effective and satisfactory way by taking into consideration the particular characteristics of the users, goals, tasks, resources, and the technical, physical, social, cultural, and organizational environments in which the product/service is used.

Our long term goal is to create a methodology to support service providers to make the privacy of their products more usable. The Usable Privacy Cube (UP Cube) described in Section 3 and the usable privacy criteria introduced in Section 6 are the first building blocks of the methodology we are aiming for. They are meant as tools, for both usability engineering experts and certification bodies, to evaluate if a product was designed to respect and protect the privacy of its users in an usable way. Once privacy measures and privacy enhancing technologies are integrated into the design of a product, it still remains to find out if (and how much or to what extent) those measures empower and respect the rights of their particular user as intended. In Human-Computer Interaction (HCI) this is determined based on user testing and usability evaluations. The criteria we propose presume the use of such established HCI methods for usability evaluations (e.g., [12]).

The legislation does not directly refer to usability goals and context of use as known in the ergonomics/human factors or human-centered design. However, requirements as the one in the Recital (39) of GDPR asking for the information addressed to the data subject to be "easily accessible and easy to understand" are categorized in this paper as usability goals, for which we create usable privacy criteria meant to measure effectiveness, efficiency and satisfaction – as usability outcomes – with regard to privacy aspects (we henceforth call these *Usable Privacy criteria*, and abbreviated it as UP criteria).

After a short digression into Related Work in Section 2, we introduce in Section 3 the UP Cube model, which is the main contribution of this work. We then continue to detail the UP Cube in the rest of the paper. Section 4 presents the EuroPriSe in the new light of the UP Cube, forming the two axes of criteria at its basis. The third vertical axis of the UP Cube, a genuine contribution of this paper, is formed of the UP criteria detailed in Section 6. To the best of our knowledge, there is not other work that extends privacy certification schemes with usability criteria. Section 5 presents usable privacy goals that the criteria are meant to measure. The UP Cube naturally captures Interactions between all the axes, which we talk about in Section 7. We conclude in Section 8, presenting also some avenues for further work.

## 2 Putting the work into context

*Usable privacy and security.* The present work can be placed in the research field called *usable privacy and security*, with seminal works s.a. [6,14,27,10] and conference series s.a. the Symposium On Usable Privacy and Security (SOUPS). We consider that research on privacy requires, even more than security, an interdisciplinary approach (encompassing the expertise coming from research fields such as Psychology, Law or Human-Computer Interaction). As [5] points out, privacy has its meaning rooted in larger cultural and social practices and has political, ethical as well as personal connotations.

Regarding the relation between security and privacy, in this paper we consider security as one integral aspect of privacy, where privacy implies security but not the other way around. We consider such a clarification necessary, as we have seen a tendency in the general public to equalize the meanings of the two terms in favor of security. In computer science, privacy research has been closely intertwined with security research, reflected e.g. in the contents and the structure of the book [11]. However, in this paper, we favor the term "usable privacy", as it includes by default security, which is in accordance with the data protection legislation, where security (integrity and confidentiality) is specified as one of the several principles to abide by in order to assure the privacy of users' data.

*Human-Computer Interaction.* Having the goal to evaluate the usability of privacy in technological systems and products, makes our work part of the larger HCI research on privacy [5,20,19,23]. Following the classifications made by Iachello and Hong in their review [16], we approach privacy from a "data protection" perspective by extracting usability related goals from the GDPR. A similar approach is taken in [23], which translates legislative clauses of the Directive 95/46/EC (now replaced by GDPR) into interaction implications and interface specifications.

For evaluating how well a product meets privacy requirements, context of use variables s.a. user capabilities, tasks, the field where the technology is going to be deployed (e.g., healthcare, industrial facilities), should be defined. We thus adopt the ergonomic approach from ISO 9241-11:2018 where *usability is always considered in a specified context of use*, since the usability to be applied to a certain technology can be significantly different for varied combinations of users, goals, tasks and their respective contexts.

## 3 The Usable Privacy Cube model

We devise a model for organizing the criteria to use in privacy evaluations and measurements, and represent it as a cube with three axes of variability (see Fig. 1), which we call the Usable Privacy Cube (UP Cube). The two axes found at the base of the UP Cube are composed of the existing EuroPriSe criteria, which we slightly reorganize in the Section 4 to fit in one of the two categories: data protection principles or rights of the data subjects.

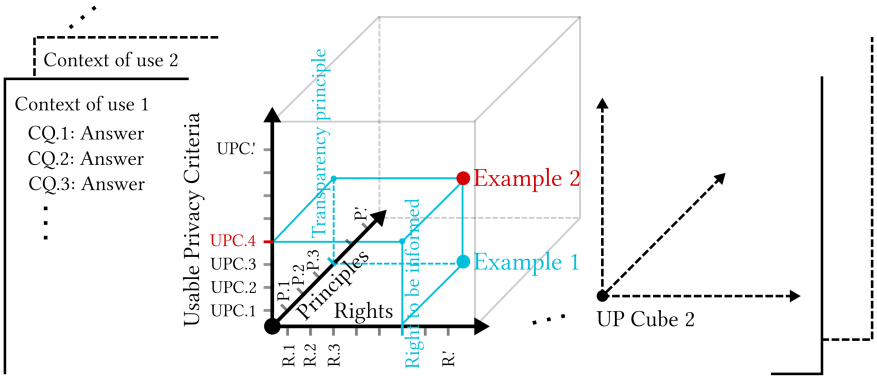


**Fig. 1.** A generic version of the cube with the three axes of variability: data protection principles, the rights of the data subjects, and usable privacy criteria.

We want to emphasize *two perspectives on privacy* that the UP Cube represents (hence our restructuring of the EuroPriSe criteria): the perspective of the controllers and of the data subjects. The controllers are thus given an overview of the principles that they are obliged to follow, whereas the data subjects are offered an overview of their rights.

The UP Cube allows to visualize interactions between the axes, made easier by our separation of the criteria into the three categories. Each such intersection has its specifics and could be studied in itself; we identify a few exemplary points of intersection between the axes in Section 7.

*Example 1.* The intersection between the transparency principle and the right to be informed is identified in Article 12 of GDPR. The controllers are obliged to provide the data subject information that should be concise, transparent, intelligible and in easily accessible form, using clear and plain language.

The third vertical axis of the cube is composed of our UP criteria, presented in Section 6. The UP criteria are determined based on usable privacy goals and are evaluated considering the context of use by following the guidelines in the ISO 9241-11:2018 standard. Interactions exist also with this third axis.

*Example 2.* For the case presented in Example 1, in order to establish how easily accessible or clear the information is, we must measure the level of efficiency, effectiveness and satisfaction in a specific context of use. Efficiency implies measuring the time and effort spent by a specific user for finding the information needed and for understanding it. Effectiveness measures the completeness with which a goal was achieved. In this case we would like to know how much of the needed information was the specific user able to access and understand. At the same time, what a certain type of user perceives as intelligible information, might be perceived by another as difficult to comprehend. Establishing the perceived characteristics of information is an activity categorized under the satisfaction usability outcome.

The UP Cube also brings the idea of *orderings* on each axis, hence the arrows. Such orderings are important for several reasons, e.g., UP criteria can be ordered based on "how little effort is required to evaluate it compared to how much overall evaluation outcome it entails" or "covers most technologies". Usual for certification methods is to use a decision tree order to capture the impact of each criterion (e.g., choosing the most discriminating first), thus which to prioritize in the evaluation.

Judging from practice, one is inclined to think that an ordering is not always possible to find as some principles are equally important, therefore the orders are not necessarily strict. Moreover, one can even see one principle as more important than another only in some industry or context, whereas in a different industry the same two principles would be ordered the other way, therefore one may think that the orders are only partial (i.e., not total). However, in a specific cube (i.e., used in a specific methodology by a specific authority for privacy usability evaluations in a specific industry and context) there must always be an ordering in which the criteria should be applied. One can always generate a strict and total order from a partial order by just taking a random decision on ordering two criteria when no reasonable order exists. For example, one can any time pick as default order the one arising from the textual placement of the criteria in the data protection legislation texts (maybe considering content from articles as more general than content from recitals), or in the EuroPriSe (or the regulator/company) catalogs. What is certain is that each use case or industry has its specific requirements from which a meaningful ordering would be created.

Forming a specific UP Cube, i.e., deciding on the precise details of each criteria on the three axes and the orderings, is to some degree dependent on the specific context of use for the respective product to be evaluated. Therefore, one can think of *infinitely many cubes*, one for each different context. The criteria will not be different between the cubes, but their scope, depth, and evaluation might be different, depending on the context.

## 4 EuroPriSe

EuroPriSe originated from the Schleswig-Holstein Data Protection Seal, which was led by the Schleswig-Holstein Data Protection Authority (DPA) from ca. 2001 until the end of 2013, when it was transferred to a company, EuroPriSe GmbH. The scheme has a history of eighteen years [15] and is one of the oldest privacy and data protection seals based on a law, i.e., the State Data Protection Act of the German federal State Schleswig-Holstein. The role of the seal is to help the vendors of IT products and services to comply with the data protection requirements derived from the applicable law in Europe [7,9,22]. EuroPriSe criteria are already updated to consider the fairly new GDPR.

We have chosen EuroPriSe as the basis for our UP Cube because of its long history, its continuous improvement, strong list of well-developed criteria, being led in the past by a DPA, and being based on the European data protection

| **EuroPriSe Criteria:** We list the names of (sub)sections as appearing in the EuroPriSe document [3], which has two parts, the second being subdivided into four *sets* of criteria, whereas the first contains preliminary issues, from where only section C is relevant for us. | Principles | Rights | Context |
|---|---|---|---|
| C. Target of Evaluation (ToE) | ✓ | | ✓ |
| 1.1.1 Processing Operations; Purpose(s) | ✓ | | ✓ |
| 1.1.2 Processed Personal Data | | | ✓ |
| 1.1.3 Controller | | | ✓ |
| 1.1.4 Transnational Operations | | | ✓ |
| 1.2.1 Data Protection by Design and by Default | ✓ | | |
| 1.2.2 Transparency | ✓ | | |
| 2.1 Legal Basis for the Processing of Personal Data | ✓ | | |
| 2.2 General Requirements | ✓ | | |
| 2.3.1 Data Collection (Information Duties) | | ✓ | |
| 2.3.2 Internal Data Disclosure | ✓ | ✓ | |
| 2.3.3 Disclosure of Data to Third Parties | ✓ | ✓ | |
| 2.3.4 Erasure of Data after Cessation of Requirement | | ✓ | |
| 2.4.1 Processing of Data by Joint Controllers | ✓ | | |
| 2.4.2 Processing of Data by a Processor | ✓ | | |
| 2.4.3 Transfer to the Third Countries | ✓ | | |
| 2.4.4 Automated Individual Decisions | ✓ | | |
| 2.4.5 Processing of Personal Data Relating to Children | | | ✓ |
| 2.5 Compliance with General Data Protection Principles | ✓ | | |
| Set 3: Technical-Organisational Measures | ✓ | | |
| Set 4: Data Subjects' Rights | | ✓ | |

**Table 1.** Overview of the the EuroPriSe criteria categorized to fit into our UP Cube model, i.e., as the two axes with Principles and Rights, as well as Context of use.

legislation. EuroPriSe also integrates with widely acknowledged IT security certification methods s.a. ISO 27000 and the The Standard Data Protection Model[5].

The way the criteria are formulated, as questions, also fits with the form of our usable privacy evaluation criteria. In addition, the existing EuroPriSe evaluation, which is at the basis of our model, assures that the GDPR legal grounds are covered, including data protection principles and duties and data subject rights. The UP criteria evaluations come on top, fine-graining the EuroPriSe evaluation with usability measurements, showing how well the legislation is respected.

Another feature that is relevant for our user-centered approach is that the EuroPriSe criteria catalog has been updated to include the data protection by de-

[5] Following the requirement for a consistency mechanism set out in the Article 63 of GDPR, the work of the certifications bodies and DPAs in Germany is coordinated and made consistent through *The Standard Data Protection Model* (https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/), issued by the Conference of the Independent Data Protection Authorities of the Bund and the Länder on 9-10 November 2016. This document is a good reference for methods and guidance for implementing the data protection principles.

fault paradigm, promoting built-in data protection and privacy-friendly default settings. Moreover, EuroPriSe takes into account the technical, organizational and legal framework within which the product or service is operated and asks for considering the requirements of all the parties involved in the system, aiming at strengthening the position of the data subjects. Our work shares with EuroPriSe its high-level goal of making transparent for the general public how companies are managing data protection in their products and services.

In order to build on EuroPriSe, we first look into how its methodology fits with our UP Cube model. We show how EuroPriSe criteria can be redistributed into one of the two axes at the basis, i.e., as either rights of the data subjects or as privacy principles, or otherwise as a context of use criterion. Table 1 gives an overview of this redistribution. The distinction between principles and rights is inspired by the structure in [13], where principles and rights represent the core of this handbook. One purpose of the principles, mentioned in [13], is to serve as the starting point when interpreting the more detailed provisions in the subsequent articles of data protection law. The law also requires that these principles should correspond to the rights presented in the articles 12 to 22. This correspondence can be visualized through the intersection between the respective rights and principles axes of the UP Cube.

## 5 Usable Privacy Goals

We identify usable privacy goals (henceforth called *Usable Privacy goals*, and abbreviated as UP goals) that appear in the GDPR text. These guide the work in Section 6 where we present the UP criteria meant to measure to what extent these goals are being achieved. We give here only some examples of goals, numbered as in the long version [17], where the full list of 30 UP goals can be found. The goals are listed in the order they appear in the legislation. The words ***emphasized*** in each goal relate to usability. The chosen words are those that can be interpreted differently based on the context they are used in, and can result in objective and perceived measurements when evaluated in usability tests. These words also capture goals that can be achieved up to certain degrees, and thus can be translated into a level in a evaluation scale. In addition to the GDPR, there are more specific data protection laws, such as the proposed ePrivacy Regulation that have implication for usability, from where one could eventually extract additional usability goals.

**UPG.3** *Consent should be given by a* ***clear*** *affirmative act establishing a* ***freely given***, ***specific***, ***informed*** *and* ***unambiguous*** *indication of the data subject's agreement to the processing of personal data relating to him or her. [Recital (32) of GDPR]*

**UPG.8** *Make the natural persons* ***aware*** *of how to exercise their rights in relation to processing of personal data. [Recital (39) of GDPR]*

**UPG.18** *Any information addressed to the public or to the data subject to be* ***concise****,* ***easily accessible*** *and* ***easy to understand****. [Article 12 (1) and Recital (58) of GDPR]*

**UPG.19** *Any information addressed to the public or to the data subject to use* ***clear and plain language****. [Article 12 (1) and Recital (58) of GDPR]*

**UPG.21** *Provide information of the intended processing in an* ***easily visible****,* ***intelligible*** *and* ***clearly legible*** *manner. [Article 12 (7) and Recital (60) of GDPR]*

**UPG.24** *Allow the data subjects to* ***quickly assess*** *the level of data protection of relevant products and services. [Recital (100) linking to Article 42 of GDPR]*

## 6 Usable Privacy Criteria

The proposed criteria are always measurable, which makes the results of a privacy evaluation easier to present visually through the use of a *privacy labeling* scheme. The use of privacy labels will then fulfill the goal UPG.24. This goal has a special significance from a usability point of view as it reduces considerably the effort spent by the data subject for evaluating privacy, which for most users is not the primary task [5] and it gets in the way of buying or using a product or service.

For generic goals like [17, UPG.1] that regards protection of personal data in general, we formulate a criterion that considers usability as follows:

> What is the level of the *usability* of the personal data protection / privacy that the product or service ensures?

For being able to establish a level of how usable the privacy protection is, the evaluation needs to produce *measurable* outcomes. The structure that we follow is the one proposed in the ISO 9241-11:2018 where the measures consider both the objective and the perceived outcomes of usability (the UP criteria are labeled accordingly). The measurements will produce *counts* or *frequencies* (e.g., how many errors the user does when probed to do certain privacy related tasks) and *continuous data* (e.g., how much time does the user spend on completing a task related to privacy). The evaluation based on the UP criteria proposed below will produce three *main categories of measures*:

1. measures of accuracy and completeness,
2. resource utilization (time, effort, financial, and material resources), and
3. measures resulting from satisfaction scales.

The score for a main UP criterion is established based on evaluations of more specific UP criteria, called subcriteria. In order to reach a *high level* of "control of their own personal data" (Recital (7) of GDPR) the scores from evaluations

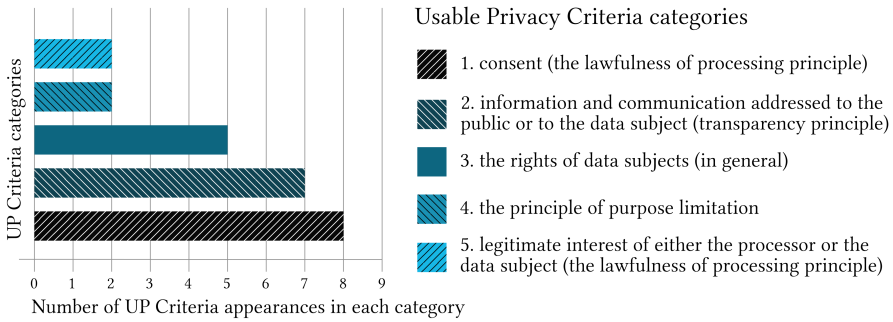


**Fig. 2.** An overview of the distribution of usable privacy criteria in each category.

of the subcriteria should also be high. The resources used to achieve a criterion, i.e., *time, effort, financial, and material* (which we abbreviate TEFM), should be measured to be able to determine the efficiency with which a specific criterion was reached. In addition, the results from the evaluations should show the level of perception that the data subjects have about their data being protected. The data subjects need to be highly satisfied with the offered privacy protection. The "high satisfaction" level is defined based on the user satisfaction evaluation of the respective subcriteria, and is also later important for the adoption of privacy technologies.

The UP criteria are categorized based on their area of application from the GDPR text. Figure 2 gives an overview of the number of criteria in each category.

A high-level UP criterion, like UPC.2, is labeled with the goal that it is related to, UPG.18. We then classify each UP subcriterion (e.g., from UPC.2.1 to UPC.2.9) into either effectiveness, efficiency, or satisfaction, and label it accordingly. We try to be exhaustive in our UP subcriteria and to give enough questions to cover all major aspects that need to be measured to achieve the respective goal that the high-level UP criterion relates to. The UP subcriteria are labeled with sublabels representing various specific measures of usability for the above three general categories, e.g.: *[Effectiveness:Completeness]*.

### 6.1 List of UP criteria

We give few examples of the usable privacy criteria, while the full list of all 24 UP criteria can be found in the long version [17]. Since our criteria are modular (i.e., each high-level criterion is thought independent of the other) and can be ordered based on their importance for different application cases, they could be introduced gradually and selectively. It can be that certification bodies (like EuroPriSe) would start to include our UP criteria in their future test catalogs on an article-basis, e.g., a good candidate is Article 12 of GDPR (referring to rights that intersect with the transparency principle) as it contains five UP goals.

**UPC.2** Is any information and communication addressed to the public or to the data subjects related to the processing of personal data concise, easily accessible and easy to understand? *[UPG.18][Type of criteria: Information and communication addressed to the public or to the data subjects]*

> How much [Time / Effort / Financial / Material resources] do the data subjects need to invest in order to [ **UPC.2.1** access, **UPC.2.2** read through, **UPC.2.3** understand] the information? *[Efficiency:Time used, Human effort expanded, financial resources expanded, materials expanded] [Measure:Objective]*
> How much of the information were the data subjects able to [ **UPC.2.4** access, **UPC.2.5** understand, **UPC.2.6** read through]? *[Measure:Objective] [Effectiveness:Completeness]*
>
> **UPC.2.7** To what degree the data subjects perceive the information as concise? *[Satisfaction:Cognitive responses] [Measure:Perceived]*
>
> To what degree the data subjects perceive the information as easy to [ **UPC.2.8** access, **UPC.2.9** understand]? *[Satisfaction:Cognitive responses] [Measure:Perceived]*

*Remark 1.* The subcriteria in UPC.2 refer to cognition and understanding, while the subcriteria in UPC.3 refer to visual aspects of the information presented.

*Remark 2.* In different HCI works one can find different formulations that could seem related to how we formulate the subcriteria, e.g.: "Can the data subjects make sense of the information at all?"; "What is the extent to which the data subjects make sense of the information?". However, we intend to measure the proportion of the information that is made sense of. Therefore we use formulations that give a statistically measurable outcome, such as "How much?", "What is the percentage?", "What is the degree?".

**UPC.3** Is the information about the intended processing provided in an easily visible, intelligible and clearly legible manner? *[UPG.21][Type: Info]*

> How much TEFM do the data subjects need to invest in order to [ **UPC.3.1** see/locate, and **UPC.3.2** distinguish] the information? *[Ey:Time used, Human effort expanded, Financial resources expanded, Materials expanded]*
>
> How well were the data subjects able to [ **UPC.3.3** visually locate and **UPC.3.4** distinguish] the information? *[Es:Accuracy]*
>
> How much of the information were the data subjects able to [ **UPC.3.5** visually locate and **UPC.3.6** distinguish]? *[Es:Completeness]*
>
> To what degree the data subjects perceive the information as [ **UPC.3.7** easily visible, **UPC.3.8** intelligible, and **UPC.3.9** clearly legible]? *[S:Cognitive responses]*

*Remark 3.* Poor visibility can affect the perception of trust, as information that has low visibility can appear to be hidden with a purpose. Poor legibility can

reflect sloppiness in the way the content is produced, which again can give an impression of lack of professionalism. Poor visibility and legibility affects the satisfaction of the data subjects and it can cause physical discomfort (e.g., to the eyes, by having to read a text written in a very small font).

**UPC.4** Is any information and communication addressed to the public or to the data subjects related to the processing of personal data using clear and plain language? *[UPG.19][Type: Info]*

> What is the level of [ **UPC.4.1** clearness and **UPC.4.2** plainness] of the language? *[Es:Accuracy]*
>
> **UPC.4.3** What is the percentage of the data subjects that understand the language? *[Es:Completeness]*
>
> What is the percentage of the language considered [ **UPC.4.4** plain and **UPC.4.5** clear]? *[Es:Completeness]*
>
> How [ **UPC.4.6** clear and **UPC.4.7** plain] do the data subjects perceive the language to be? *[S:Cognitive responses]*

Several usability goals are found in the consent related provisions. These provisions are evaluated in detail in the EuroPriSe sections *2.1.1.1 Processing on the Basis of Consent* and *2.1.1.2 Processing on the Basis of a Contract*. The criteria we generate here are meant to complement the ones in the EuroPriSe through bringing in usability concerns. Marc Langheinrich presents several of the problems with how consent can be misused [21]. One of these is the "take it or leave it" dualism where the person does not have a real choice and thus getting consent comes very closed to blackmailing. This problem has been ameliorated in the GDPR law by asking the controllers to allow for separate consent for different data processing operations. A usability evaluation could help further by revealing how the data subjects perceive the consenting act, as well as whether the data subjects consider consent a real choice and if the options to consent to some of the processing operations only, are satisfactory.

**UPC.8** Is consent given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subjects' agreement to the processing of personal data relating to them? *[UPG.3][Type: Consent]*

> **UPC.8.1** How much of the consent text do the data subjects understand? *[Es:Completeness]*
>
> **UPC.8.2** How much of the implications of consenting do the data subjects understand? *[Es:Completeness]*
>
> To what degree the data subjects perceive the agreement to be [ **UPC.8.3** freely given, **UPC.8.4** informed, and **UPC.8.5** unambiguous]? *[S:Cognitive responses]*

## 7 Interactions between the three axes

Characteristic to the data legislation text is that it always refers to how principles and rights intersect and depend on each other. In this section, we give examples of such references found in the recitals of GDPR, relevant for some of the identified usability goals. The recitals, though not legally biding, are meant to provide more details to the GDPR's articles. The lawfulness, fairness, and transparency of processing principles, and the right to be informed appear to be closely interrelated, having also the highest occurrence of usability goals.

1. The UP criterion [17, UPC.1] refers to the control the data subjects have over their data. The criterion can be related to the *right to data portability*, through the Recital (68), where due to the aim of strengthening the control of the data subject, the "data subject should also be allowed to receive personal data concerning him or her, which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller ...". It can also be linked to *data security principle* through the provision in the Recital (75) where the "risk to the rights and freedoms of natural persons" can result in data subjects being deprived of their rights and freedoms or prevented from exercising control over their personal data. The "risk to the rights and freedoms of natural persons" is also mentioned by the [13, pp. 131, 134] in the context of *data security principle*.
2. The UP criteria UPC.2 and UPC.4 are related to the *transparency of processing principle*, which is referred to directly in the Recital (58), where the respective goals are extracted from – "The principle of transparency requires that any information and communication related to the processing of those personal data ..." – and *principles of lawfulness and fairness*, which are also directly referred to in the Recital (39) – "Any processing of the personal data should be lawful and fair".
3. The UPG.8 goal relates to the *fairness and transparency of processing principles*, and is placed under these respective categories, also by the [13, pp. 117, 120].
4. The goal UPG.19 is mentioned in the context of the transparency principle, in the Recital (39), where the information to be given to the data subject relates to the purpose of processing. This connects *the principle of transparency* with *the principle of data minimization*.
5. The UP criterion [17, UPC.22] about "the personal data [being] adequate, relevant and limited to what is necessary for the purposes for which they are processed", is based on the [17, UPG.10], extracted from the Recital (39) of GDPR. This criterion is mentioned in Recital (39) as one of the requirements for complying with *the transparency principle*, while also referring to the purpose of processing. This connects the present criterion also with the *principle of data minimization* and in addition with the *data protection by design principle*. The link between the last two principles can also be seen in EuroPriSe criteria catalog, where data minimization is the focus of the [3, 1.2.1 Data Protection by Design and by Default, p.18] section.

## 8 Conclusion and Further Work

The benefits of the UP Cube model are multiple: (i) emphasizing both the perspectives of data subjects and of controllers; (ii) representing visually on the three variability axes the existing rights and principles criteria from EuroPriSe, together with our new UP criteria; (iii) visualizing intersections between the three axes; (iv) allowing ordering of the criteria on each axis.

The theory behind our usability evaluation of privacy is based on the well established standards ISO/IEC29100:2011 and ISO 9241-11:2018. We worked directly with the GDPR text, guided by [13], which also inspired our structuring of the EuroPriSe criteria into rights and principles. Our HCI and usability perspective on privacy is influenced by the seminal works [6,14,5,20,19,23,10].

To build the UP Cube we have:

- identified from the GDPR text *30 UP goals*,
- created *24 UP criteria*, each with measurable subcriteria, and
- restructured the criteria of EuroPriSe, laid as the basis of the UP Cube.

**Further Work.** The UP Cube is meant as the groundwork for building a certification methodology, extending EuroPriSe to evaluate the usability of privacy. The proposed UP criteria are designed to produce measurable evaluations, useful for generating privacy labels in order to guide stakeholders when choosing technological products, by representing and visualizing the different levels of privacy. To achieve this larger goal, one needs to investigate which existing HCI methods for usability testing should be used for each of the UP criteria, and in what way.

One example of such a usability method for measuring the perceived usability of a system is the System Usability Scale (SUS) [8], a ten-item attitude Likert scale questionnaire. The standard [4, Annex B: Usability measurements] also gives examples of methods that produce measurements relevant for our UP criteria, s.a. observing the user behavior to identify the actual usability problems, or asking the users to carry out tasks in a real or simulated context of use and measuring the outcomes. The experts can also run heuristic evaluations following design principles, theories and standards from the design and cognitive fields. More concrete examples of HCI methods and how these could be used for privacy and security solutions can be found in [19].

Which methods are appropriate to use, the number of test persons, and other test related concerns, depend on contextual factors, s.a. the type of technology, users and industry. Defining the required context is what our model offers support for. However, more work (e.g., providing guidelines and examples) is needed on how the context of use can be established.

HCI practices conduct user studies throughout the whole lifecycle of a product. These studies are run by the company itself, with the help of HCI (User Experience or Interaction Design) experts. For certification, the accredited data protection assessors would be using the results provided by the company to answer the UP criteria questions. In the cases of not enough or not reliable results, the assessors can recommend/require further testing. It would be valuable

to have guidelines, e.g., in the form of a check-list, to help the assessors with establishing if the results from the company are reliable and sufficient. Recommendations for the businesses are useful as well, to guide how to conduct privacy related user testing, so that the results would be reliable later for certification.

With the same goal of achieving a complete methodology that can be taken in use by the accreditation bodies, building on the present model, one could create a visual representation of the evaluation, i.e., a translation of the measurements of usability of privacy provided by the UP criteria into a visually appealing privacy label. This should serve as a vertically graded scale to differentiate a customer product from another. According to ISO 9241-11:2018, "where usability is higher then expected, the system, product or service can have a competitive advantage (e.g. customer retention, or customers who are willing to pay a premium)". The visuals will be thought to come in addition to the GDPR compliance seal and reflect the usability of the privacy implemented. The purpose will be the same as for the methodology, to help the businesses that have already achieved GDPR compliance to further differentiate themselves on the market. From the point of view of the user of the product, the visual scale would offer support for choosing the service or product that best respects her privacy expectations.

To further validate our UP Cube model and for exemplification, we are applying the UP criteria to *three use cases* taken from pilots done in an ongoing European project called Secure COnnected Trustable Things (SCOTT): *(i)* Assisted Living and Community Care System, *(ii)* Air Quality Monitoring for healthy indoor environments, and *(iii)* Diabetes App. These are examples of IoT systems [26,25,24] for which our model is especially relevant, as the privacy protection is even more variable and context-dependent. IoT technologies, due to their nature (i.e., ubiquity, invisibility, and continuous sensing) [21], are able to generate granular and intimate data about people and everything or everyone in their surroundings, by that reducing privacy to zero.

## References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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. Official Journal of the European Union **L 119/1** (2016)
2. The House of Lords EU Committee, European Union Committees report on Online Platforms and the Digital Single Market (2016), https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/12909.htm#_idTextAnchor235
3. EuroPriSe Criteria for the certification of IT products and IT-based services – v201701. Tech. rep. (2017), https://www.european-privacy-seal.eu/AppFile/GetFile/6a29f2ca-f918-4fdf-a1a8-7ec186b2e78a
4. Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts. Standard ISO 9241-11:2018 (2018)
5. Ackerman, M.S., Mainwaring, S.D.: Privacy Issues and Human-Computer Interaction. In: Cranor, L., Garfinkel, S. (eds.) Security and usability: designing secure systems that people can use, pp. 381–399. O'Reilly (2005)

6. Adams, A., Sasse, M.A.: Users are not the enemy. Communications of the ACM **42**(12), 41–46 (1999)
7. Balboni, P., Dragan, T.: Controversies and challenges of trustmarks: Lessons for privacy and data protection seals. In: Privacy and Data Protection Seals, pp. 83–111. Springer (2018)
8. Brooke, J.: SUS – A quick and dirty usability scale. Usability evaluation in industry **189**(194), 4–7 (1996)
9. Cavoukian, A., Chibba, M.: Privacy seals in the USA, Europe, Japan, Canada and Australia. In: Privacy and Data Protection Seals, pp. 59–82. Springer (2018)
10. Cranor, L.F.: SIGCHI Social Impact Award Talk – Making Privacy and Security More Usable. CHI EA '18, ACM (2018). https://doi.org/10.1145/3170427.3185061
11. Cranor, L.F., Garfinkel, S.: Security and usability: designing secure systems that people can use. O'Reilly (2005)
12. Dumas, J.S., Redish, J.C.: A Practical Guide to Usability Testing. Intellect Books, Revised edn. (1999)
13. European Union Agency for Fundamental Rights: Handbook on European data protection law – 2018 edition. Luxembourg: Publications Office of the European Union (2018)
14. Good, N.S., Krekelberg, A.: Usability and privacy: a study of Kazaa P2P file-sharing. In: Proceedings of the SIGCHI conference on Human factors in computing systems. pp. 137–144. ACM (2003)
15. Hansen, M.: The Schleswig-Holstein data protection seal. In: Privacy and Data Protection Seals, pp. 35–48. Springer (2018)
16. Iachello, G., Hong, J.: End-user Privacy in Human-Computer Interaction. Foundations and Trends in Human-Computer Interaction **1**(1), 1–137 (2007)
17. Johansen, J., Fischer-Hübner, S.: Making GDPR Usable: A Model to Support Usability Evaluations of Privacy. Tech. rep., arXiv (Aug 2019), arxiv.org/abs/1908.03503
18. Kamara, I., De Hert, P.: Data protection certification in the EU: Possibilities, Actors and Building Blocks in a reformed landscape. In: Privacy and Data Protection Seals, pp. 7–34. Springer (2018)
19. Karat, C.M., Brodie, C., Karat, J.: Usability design and evaluation for privacy and security solutions. Security and usability pp. 47–74 (2005)
20. Karat, C.M., Karat, J., Brodie, C.: Privacy Security and Trust: Human-Computer Interaction Challenges and Opportunities at their Intersection. The Human-Computer Interaction Handbook pp. 669–700 (2012)
21. Langheinrich, M.: Privacy by design – Principles of privacy-aware ubiquitous systems. In: International Conference on Ubiquitous Computing. pp. 273–291. Springer (2001)
22. Papakonstantinou, V.: Introduction: Privacy and Data Protection Seals. In: Privacy and Data Protection Seals, pp. 1–6. Springer (2018)
23. Patrick, A.S., Kenny, S., Holmes, C., van Breukelen, M.: Human Computer Interaction. In: Handbook for Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents, chap. 12, pp. 249–290 (2003)
24. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: The road ahead. Computer networks **76**, 146–164 (2015)
25. Stankovic, J.A.: Research directions for the internet of things. IEEE Internet of Things Journal **1**(1), 3–9 (2014)
26. Weiser, M.: Ubiquitous computing. Computer (10), 71–72 (1993)
27. Whitten, A., Tygar, J.D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: USENIX Security Symposium. vol. 348 (1999)