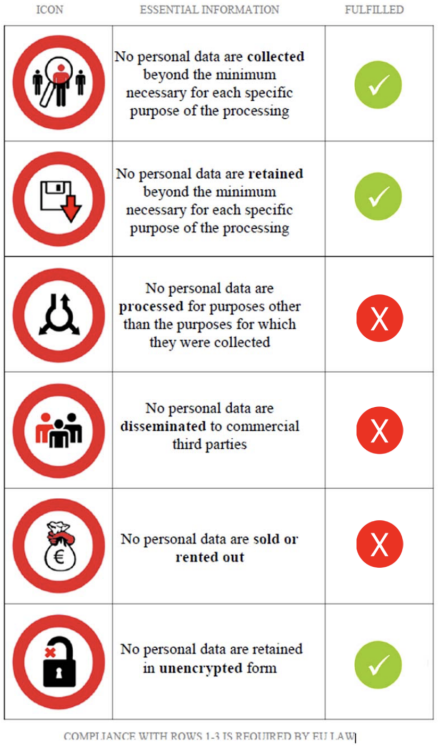
Designing Privacy Icons & Testing for its Effectiveness by an Interdisciplinary Research Methodology

Combining Research Methods from the Areas of Law, Behavioural Economics and UX Design as an Element of Data Protection by Design (GDPR)

Problem and research goal: How to design and test privacy icons *and its effectiveness*

The European General Data Protection Regulation (GDPR) can certainly be regarded as a milestone for the civil rights movement in our digital society. The GDPR establishes several innovative approaches (such as the data protection by design approach). However, despite its ambition, there are several challenges that hinder the protected individuals (so-called data subjects) to fully profit from the GDPR's protective power. An example are the extensive information duties requiring controllers to inform the data subjects about the data processing (see, in particular, the transparency principle under Art. 5 sect. 1 lit. a and, more specifically, the information duties under Art. 12 to 14 GDPR). Many studies illustrate that data subjects barely take notice of the provided information, let alone understanding them.[1] Since the information shall help individuals to understand which risks the processing causes to them and, on this basis, to properly adapt to the risky situation, the actual effects of the law prove it, so far, a paper tiger. This is a painful result as this effectless protection creates, nonetheless, enormous legal uncertainty amongst controllers.



The legislator saw this challenge and clarified in Art. 12 sect. 7 GDPR that "*the information to be provided to 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.*" Sect. 8 also states that the European Commission can enact an act "*for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.*" Indeed, the Commission has not yet started to elaborate on such an act but observes the situation.[2] The European Data Protection Board states, at least, that "*the development of a code of icons should be centred upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.*"[3]

In fact, within the industry and wider public, there are already several attempts to create privacy icons to make lengthy privacy statements more intelligible for data subjects. For example, in 2007, Mathias

[1] See, instead of many others, Arnold, René, et alt., Personal Data and Privacy.
[2] This statement is based on an email exchange with Olivier Micol from the EU Commission (10th October 2018).
[3] See European Data Protection Board, Guidelines on Transparency (17/EN - WP260), referring to recital 166 GDPR, p. 23.

Mehldau from the German blog Netzpolitik.org developed and published such a set;[4] just as Ben Moskowitz and Aza Raskin from Mozilla did in 2011;[5] and even the EU Parliament tried, in 2014, to develop the set visible on the right sight of this page.[6] Of course, since the GDPR has become applicable, there are also current initiatives.[7] However, despite these good intentions, their common problem is, so far, that they are lacking an appropriate methodology. The icons are mind experiments without integration of the user (taking age, experience, capabilities and so on into account). The goal of the present research project is to develop and apply such a methodology.

Method: Combining legal research with behavioral economic and UX design research

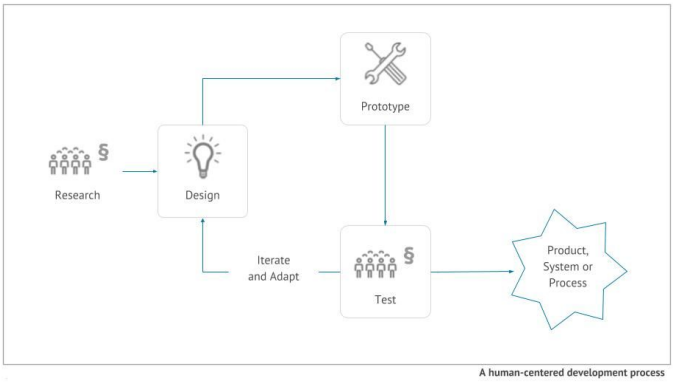
In order to develop and apply an appropriate methodology to design privacy icons and evaluate their effectiveness, the present research project refers to the data protection by design approach as established under Art. 25 GDPR. Art. 25 GDPR requires data controllers to implement data protection principles by technical and organisational measures to *effectively* meet the GDPR requirements *and* protect the fundamental rights of the data subjects. When doing so, the controller has to take into account, amongst other aspects, the processing purposes and the risk for the data subjects' fundamental rights. The data protection principles are listed under Art. 5 GDPR, such as the principles of transparency and purpose limitation (including the requirement to specify the processing purpose). Thus, the essential question is how a controller has to implement the information duties with respect to the principles of transparency and purpose limitation so that they effectively protect the data subject's fundamental rights. An answer to this question requires combining three research areas:

Since privacy icons are intended to implement the law, one must firstly find out how a controller has to specify its processing purpose from a legal point of view. From a legal perspective, the specification of the purpose shall enable data subjects to foresee the consequences of the data processing.[8] In fact, not informing data subjects about such risks is an essential shortcoming in the aforementioned approaches to iconise privacy information. This becomes particularly apparent regarding the icons proposed by the EU Parliament. When looking at these icons, it remains rather vague what the consequences for the data subjects are. For example, the privacy icons do not specify the consequences for the data subject if the data is used for other purposes than for which it has originally been collected or if the data is shared with commercial partners or if it is even rented out. In all these cases – which means, in most cases, realistically – the *specific* risks remain unnamed, which means, the consequences remain *abstract*.

In contrast to such vague approaches, the present project will focus on how to make the *specific* risks to data subjects clear. To answer the question about which *concrete* consequences the controller has to inform the subjects, the present research project can build on several already accomplished research projects.

[4] See under https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf (11th December 2018).
[5] See under https://wiki.mozilla.org/Privacy_Icons (11th December 2018).
[6] See the evaluation at Pettersson, S., A brief evaluation of icons suggested for use in standardised information policies.
[7] For example, by the Bitkom, according to Rebekka Weiß from Bitkom (April 2018).
[8] See European Data Protection Board, Opinion on the Principle of Purpose Limitation (00569/13/EN - WP203), p. 11.

According to previous legal research, for example, the controller has to discover and disclose the specific risks that the processing causes to the data subjects' fundamental rights through specifying the purpose of its data processing. If an intended data processing causes a specific risk to a fundamental right, such as to privacy, freedom or equality, the controller must make this clear specifying its processing purpose, correspondingly.[9] Thus, if a controller wants to make its processing that causes a specific risk legally compliant, it *must* inform the subject about that risk. The following example shall illustrate this concept: A mobile app provider collects personal data to provide, originally, its service and improve the user's experience. So far, we assume that the data processing reveals personal information about the users' private life (e.g. how they behave when using the app) and, thus, causes a specific risk to their right to privacy. However, at a later stage, the controller decides to also use the data for personalised advertising and shares, to reach that purpose, the data with commercial partners. In the moment of that decision, this new purpose does not only extend the users' risk to privacy because more entities know something about their private lives. Rather, the new purpose causes an additional risk to the users' right to make autonomous purchasing decisions. Therefore, if the new processing operations cause such an additional risk, the controller must inform the users about that additional risk to be legally compliant.



A human-centered development process

Against this background, the present project asks how privacy icons should be designed so that the data subjects understand the risks against their rights to privacy, freedom, and/or equality. The project seeks to answer the question by building on previous UX design projects. Applying an iterative research methodology, the project will focus on a set of typical scenarios that cause a specific data protection risk (e.g. the risks caused by personalised advertising). The empirical user testing shall be carried out in the Berlin Open Lab. For the expert workshops, the research team can build upon its extensive network to researchers, data protection authorities, and the industry.

[9] See v. Grafenstein, M., The Principle of Purpose Limitation in Data Protection Laws, pp. 325 et subs. and pp. 483 et subs.

About the Institutions

The **University of the Arts Berlin (UdK)** is one of the largest and most diversified universities of the arts in the world. The teaching offered mostly in traditional formats in the four colleges of Fine Arts, Architecture, Media and Design, Music and Performing Arts as well as at the Central Institute for Continued Education/ Berlin Career College encompasses the full spectrum of the arts and related academic studies in more than 70 courses. With the right to confer doctorates and post-doctoral qualifications, Berlin University of the Arts is also one of the few art colleges in Germany with full university status. Teachers in art and music are also educated at Berlin University of the Arts, the only university in Berlin and Brandenburg where these subjects can be studied.

The **Einstein Center Digital Future (ECDF)** is an inter-university nucleus for research on the digitalization of our society. Its aim is to foster innovative, cutting-edge interdisciplinary research, and to provide outstanding training for talented young scholars. The ECDF is a public-private partnership, initiating around 50 new professorships, and bringing together universities, non-university research institutes, and industrial enterprises, as well as regional and federal ministries. The scale of this alliance between public entities, sponsors and supporters is unique in Berlin's history as a center of academic endeavor.

The **University of Siegen (USI)** has established with the Master Human Computer Interaction in 2010 one of the first German courses of study in the field of human-centered development of application systems. The research group "Usable IT Security and Privacy" around Prof. Dr. Stevens at the has already carried out many research projects on user-centered security research as well as the ergonomic design of data protection and information system solutions for the IoT sector and especially for the automotive industry. These include, among others, participation and project lead in the calls in the funding lines of Smart Services (www.Car-bits.de), Mittelstand Digital (www.Smart-Life.info) as well as currently ongoing projects in the competence centers Usability (www.kompetenzzentrum-usability.de) and Siegen (www.kompetenzzentrum-siegen.de). In this context, legal analyses have already been developed in cooperation with other institutes. Numerous international publications at top conferences and high-ranking periods also attest to the groups research excellence.

For further information

Prof. Dr. Max von Grafenstein, LL.M. (ECDF / UdK) · m.von-grafenstein@udk-berlin.de
Timo Jakobi (Universität Siegen) · timo.jakobi@uni-siegen.de
Keevin Klug (ECDF / UdK) · kevin.klug@hiig.de

Einstein Center Digital Future - Robert Koch Forum
Wilhelmstr. 67 · 10117 Berlin · www.digital-future.berlin/