Privacy Icons:

A Risk-Based Approach to Visualisation of Data Processing

*Zohar Efroni, Jakob Metzger, Lena Mischau and Marie Schirmbeck**

Although the institution of consent within the General Data Protection Regulation intends to facilitate the exercise of personal autonomy, reality paints a different picture. Due to a host of structural and psychological deficits, the process of giving consent is often neither informed nor does it foster self-determination. One key element in addressing this shortcoming is the visualisation of relevant information through icons. This article outlines a risk-based methodology for the selection, design and implementation of such privacy icons. It lays the groundwork for identifying risky data processing aspects as a first step in a larger project of creating a privacy icons set to accompany privacy policies. The ultimate goal of the privacy icons is to assist users in making better informed consent decisions through the visualisation of data processing aspects based on their inherent risks.

Keywords: Privacy Icons, Consent, Risk-Based Approach, Private Autonomy, Legal Design

I. Introduction

1. The Problem

Internet users are being routinely asked to grant their consent to the collection and use of personal information in connection with gaining access to goods and services. Very often, 'data subjects' in terms of data protection law are at the same time 'consumers' in terms of consumer protection law. In many cases, obtaining consent is necessary for legitimising the use of personal data.[1] In order to be valid, the consent must be 'informed'.[2] Many studies have shown, however, that users often do not read privacy policies they grant their consent to. Due to a host of structural conditions and cognitive deficiencies,[3] the consent granted by checking a box that merely provides a link to the full text of the privacy policy might not qualify as informed. One of the key reasons for the lack of informed consent is that users fail to properly evaluate or even recognise the risks (or the potential negative consequences)[4] involved in the processing of their data.

2. Motivation and Structure of the Article

This article is part of a five-phased privacy icons project in which we inquire whether visualisation of

DOI: 10.21552/edpl/2019/3/9

[*] Dr Zohar Efroni, LLM, Research Group Lead at the Weizenbaum Institute for the Networked Society in Berlin; Humboldt University Law Faculty, Berlin. Jakob Metzger, Research Associate at the Weizenbaum Institute for the Networked Society in Berlin; Doctoral Candidate, Humboldt University Law Faculty, Berlin. Lena Mischau, Research Associate at the Weizenbaum Institute for the Networked Society in Berlin; Doctoral Candidate, Humboldt University Law Faculty, Berlin. Marie Schirmbeck, MSc Psychology, Research Associate at the Weizenbaum Institute for the Networked Society in Berlin; Humboldt University Law Faculty, Berlin. This work has been funded by the Federal Ministry of Education and Research of Germany (BMBF) under grant no 16DII111 ('Deutsches Internet-Institut'). For correspondence: <zohar.efroni@rewi.hu-berlin.de>.

[1] Alongside consent, which is at the focus of this article, alternative legal grounds (such as the legitimate interests of the controller or complying with legal obligations) may justify data processing independently of the individual wish of the data subject.

[2] art 4(11) GDPR (''consent' of the data subject means 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').

[3] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv L Rev 1880.

[4] In this article, we use the terms 'risk' and 'possible negative consequences' interchangeably while keeping in mind that negative consequence to the interests of a given user in a given consent situation are very hard to predict and estimate ex ante. We elaborate on the notion of risk in the context of data protection law in s V. below.

data processing aspects, specifically via risk-based icons, can contribute to a more informed consent. As part of the first phase of the project, this article outlines the risk-based approach we intend to apply in developing such icons, and it lays down the psychological and legal groundwork necessary for our future work.

In detail, this article starts by highlighting the importance of self-determination and its interrelation with consent as well as data protection law in general (Section II). After explaining the structural and psychological deficiencies of consent that hinder the enforcement of self-determination (Section III), we continue by highlighting visualisation as a possible solution for those deficiencies (Section IV). Based on these findings, we explain our methodology and present the first results of our risk-based approach consisting of a comprehensive analysis of the concept of risk in the General Data Protection Regulation (GDPR) (Section V). Finally, we give an outlook on some of the most important design guidelines and enforcement strategies for privacy icons (Section VI).

II. Autonomy, Self-Determination and Consent

Consent in data protection law as a manifestation of self-determination builds on the notion of autonomy. While thinking about consent as an instrument that promotes self-determination and about its connection to personal autonomy, it should be helpful to briefly explain what these concepts generally mean and how they interrelate.

1. A Brief Introduction to the Notion of Autonomy

The notion of personal autonomy captures centre stage in the fabric of liberal-democratic societies. Political, societal and economic structures in liberal democracies are premised on the ideal and actual freedom of persons to make individual choices in various fields of their lives and with regard to a broad range of matters. The notion of autonomy traces back even to a more fundamental aspect of human existence, as human beings are commonly considered autonomous creatures: Their autonomy consists in the ability to choose whether to think in a certain way, their freedom from obligations in some spheres of life and their moral individuality.[5] The literature emphasises that the notion of autonomy and the way in which it is applied is context-related. Essentially an abstract concept, the notion of autonomy may function as a moral, political and social ideal, to which multiple philosophical traditions attached their respective conceptions.

Personal autonomy, generally speaking, is a situation, in which the agent has an authority over herself simply since the agent can initiate her actions.[6] In this sense, the authority we have over ourselves and over our actions is intrinsic to our person, that is, to our 'self'. Having authority to initiate our actions, however, does not mean that when we act, we always exercise that authority. Powers that move us to act, which can be considered 'external' to the self, such as desires, urges or compulsions, can be at odds with our authority to act as agents, and in this sense, those powers can be considered as external to ourselves.[7] This observation leads to the distinction between actions that are self-governed and actions that are subject to autonomy-undermining influences on the decision, intention or even will of the agent, for example, in situations of brainwashing, dependency or addiction.

Within the more specific framework of moral and political philosophy, the discussion on autonomy begins with the moral capacity of a person to be herself, her own, authentic person, and to live her life according to her own reasons and motives. This capacity, which entails under most autonomy conceptions also a moral responsibility, contrasts with a situation of the agent being guided by manipulative or distorting external forces. Viewed through this prism, autonomy underpins some moral and political rights and freedoms emanating from the capacity to self-reflect and endorse one's own values via choices and actions. Autonomy, hence, correlates to

[5] Gerald Dworkins, *The Theory and Practice of Autonomy* (Cambridge University Press 1988) 6.

[6] Sarah Buss and Andrea Westlund, 'Personal Autonomy' in Edward N. Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition) <https://plato.stanford.edu/archives/spr2018/entries/personal-autonomy>.

[7] ibid.

some degree with notions of authenticity, independence and freedom.[8]

Ben Colburn suggested to classify autonomy conceptions as falling under one of three families: reason-based theories, motivation-based approaches and autonomy conceptions building on Joseph Raz's scholarship that place individuality at their centre of gravity and are constructed around the ideal of self-creation.[9] As one common thread running through all these theoretical approaches to autonomy, Colburn identified at their core something that can generally be referred to as self-governance or control of one's commitments.[10] The idea of autonomy as self-rule, indicated already by its Latin etymology, 'autos'=self, and 'nomos'=rule, accommodates alongside independence also the components of deliberation and choice of an agent having the intrinsic capacity to rule herself.[11]

Deliberation and choice are key for understanding the connection between these theoretical principles and consent in data protection law. Conceptually, notions of individual autonomy and a personal interest in informational self-determination are intimately related, and it is hard to speak of a meaningful actualisation of autonomy if the agent has little or no idea about the implications of the decision to grant consent for herself and her environment.

2. Data Protection Law

The ideal of individual autonomy is manifested in various branches of the law. In the area of relationships between private parties, the request for consent is usually connected to some sort of a bargain. Setting aside for the moment the public policy question about the adequacy and validity of personal data as subject matter of a binding contract,[12] there is a common basic element present in both, namely, the power of the individual to alter legal positions via a declaration of intention to be bound by the agreement. This power emanates from the recognition of the legal system in the authority of the individual as an autonomous agent while exercising this power.

Moving now to examine positive privacy/data protection law,[13] a cursory glance at the GDPR reveals numerous provisions that manifest the rights and entitlements of natural persons to determine the use of personal data. Alongside the power to extend their consent with respect to certain usage of their personal data by others,[14] data subjects have entitlements to withdraw consent at any time[15] or control in various ways data usage once in the hands of third parties.[16]

The great importance attributed to individual decisions can be linked to the underlying theory that conceptualises privacy law as protecting the right of individuals to exercise control over the communication of personal information concerning them by determining when, how and to what extent such information can be communicated to others.[17] Control-based conceptions of privacy law as well as related data protection doctrines developed in Germany, which uphold the right to informational self-determination,[18] exemplify an approach of general prohibition unless a legal ground for data processing is established.[19] This approach

[8] On the distinctions between 'autonomy' on the one hand, and 'freedom' or 'liberty' on the other hand, *see* John Christman, 'Autonomy in Moral and Political Philosophy' in Edward N Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition) <https://plato.stanford.edu/archives/spr2018/entries/autonomy-moral/>. *See also*, Dworkin (n 5) 14.

[9] Ben Colburn, *Autonomy and Liberalism* (Routledge 2010) 5-6.

[10] ibid 4 (citing John Christman, 'Constructing the Inner Citadel', Ethics 101 (1988) 505-520).

[11] Dworkins (n 5) 12-15.

[12] For a view that categorically denies the application of contractual freedom to personal data, *see* European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' (14 March 2017) 7. *Cf* Axel Metzger et al, 'Data-Related Aspects of the Digital Content Directive' (2018) 9(1) JIPITEC <https://www.jipitec.eu/issues/jipitec-9-1-2018/4682> (supporting a more market-oriented approach to personal data as counter-performance in contractual situations online).

[13] Being mindful of the distinction between privacy and data protection interests and regulations, we use the terms 'privacy' and 'data protection' for the sake of the discussion interchangeably, as the relevant role of informed consent discussed here applies in a similar way to both types of interests.

[14] art 6(1)(a) GDPR.

[15] art 7(3) GDPR.

[16] For instance, art 15 (right of access by data subject), art 17 (right to erasure), art 18 (right to restriction of processing) and art 20 GDPR (right to data portability).

[17] Alan Westin, *Privacy and Freedom* (first published 1967, Ig Publishing 2015) 5.

[18] For a historical overview on the development of data protection law in Germany, *see* Kai v Lewinski, 'Zur Geschichte von Privatsphäre und Datenschutz - Eine Rechtshistorische Perspektive' in Jan-Hinrik Schmidt and Thilo Weichert (eds), *Datenschutz – Grundlagen, Entwicklungen und Kontroversen* (bpb 2012).

[19] *see* Dagmar Hartge, 'Erlaubnisse und Verbote im Datenschutzrecht' in Jan-Hinrik Schmidt and Thilo Weichert (eds), *Datenschutz – Grundlagen, Entwicklungen und Kontroversen* (bpb 2012) 281-282. (explaining the general principle in German data protection law, still under the former Federal Data Protection Law, according to which every processing of personal data is firstly prohibited unless specifically permitted under law or the data subject has consented).

also significantly underlies current EU data protection law.[20]

One of the most cited sources in this context is the seminal decision of the German Federal Constitutional Court on the 1983 census (*Volkszählungsurteil*), where the fundamental right to informational self-determination has been explicitly recognised and formulated. Specifically, the constitutional right guarantees the power of individuals, in principle and to some degree, to determine how personal data is to be used.[21] Such self-determination is significantly achieved via the instrument of consent.

Nevertheless, consent currently struggles to fulfil this role. On the one hand, consent competes with other statutory alternatives that provide valid justifications to processing personal data.[22] On the other hand, also within the instrument consent itself, there are various deficiencies hindering it from fostering self-determination as intended.

III. The Troubles with Consent

After briefly discussing below some of those deficiencies, we will take a closer look at the underlying psychological factors.

1. Structural Deficiencies of Privacy Policies

Every privacy decision takes place within a given context and under conditions of uncertainty that ultimately influence behaviour. In the case of online consent, the user typically faces a window, frame or some other element on an electronic screen asking the user to check an 'I agree' box. The screen refers (typically by providing a hyperlink) to the full text of the privacy policy, but the substantive information provided by the privacy policy, and importantly, data processing aspects and their inherent risks, often go unnoticed by humans.[23]

Structural and cognitive deficiencies that influence online consent decisions have been extensively discussed and documented in literature. Textual complexity[24] and length[25] of privacy policies, language[26] and design manipulation[27], information asymmetries[28] and incomplete information,[29] all intensifying users' susceptibility towards heuristics and cognitive biases,[30] are some of the most frequently cited deficiencies. One result of these decisional factors is that while the advantages of consenting to data processing (=benefits) are mostly clear and explicit within the decision framework and context, possible negative consequences (=costs) remain obscure.

The choice architecture of many websites and applications present additional challenges. Companies sometimes design choice architectures that require multiple clicks and redirections to subpages, rendering the task of finding relevant privacy information more tedious.[31] The lack of structural standards of privacy policies, the use of multiple information hierarchies in building sites and the lack of knowledge about available options and tools and their functionality to protect online privacy have al-

[20] *cf* art 6(1) GDPR (providing that processing 'shall be lawful only if and to the extent that at least' one of the justification grounds specified in subsections (a) to (f) applies), with consent being one of them – as stated under subsection (a).

[21] BVerfG, Judgment of 15 December 1983 – 1 BvR 209/83.

[22] For example, processing that is necessary in order to protect the vital interests of the data subject or of another natural person (art 6(1)(d) GDPR) or processing that is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (art 6(1)(f) GDPR).

[23] Ross A Malaga, 'Do Web Privacy Policies Still Matter?' (2014) 17(1) Acad Inf Manage Sci J 95; Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2018) Information, Communication & Society 1.

[24] Eric Paolo S Capistrano and Jengchung Victor Chen, 'Information privacy policies: The Effects of Policy Characteristics and Online Experience' (2015) 42 Computer Standards & Interfaces 24; Mark A Graber, Donna M D'Alessandro and Jill Johnson-West, 'Reading Level of Privacy Policies on Internet Health Web Sites' (2002) 51(7) Journal of Family Practice 642.

[25] Aleecia M McDonald, and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) Information System: A Journal of Law and Policy for the Information Society 543.

[26] Irene Pollach, 'What's Wrong with Online Privacy Policies?' (2007) 50 Communications of the ACM archive 103.

[27] NOYB – European Center for Digital Rights, 'Complaint to the Austrian Data Protection Agency' (2018) 6 <https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf>.

[28] For further details about the issue of information asymmetry, *see* Masooda Bashir et al, 'Online privacy and informed consent: The dilemma of information asymmetry' (2015) in Proceedings of the 78th ASIS&T Annual Meeting 1.

[29] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347(6221) Science 509.

[30] *cf* Alessandro Acquisti et al, 'Nudges for Privacy and Security' (2017) 50 ACM Computing Surveys 1.

[31] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media' (2018) 4 (3) Social Media + Society 1.

so been identified as problematic aspects of online consent.[32]

2. Psychological Factors Influencing Privacy Related Decisions

A closer look at psychological processes underlying privacy-related behaviours may shed more light on the issues sketched above and explain the intentional use of certain design aspects in order to drive users into less deliberate, even misguided decisions. Research indicates that the majority of users are most likely not able to manage their online privacy in an adequate manner due to a variety of factors. One may view trade-offs such as disclosing personal information in exchange for the benefits of high-quality personalisation,[33] or ignoring complex and time-consuming security advices due to a low likelihood of severe consequences to occur,[34] as components of rational decisions. However, users who perform privacy-related decisions operate under conditions of privacy uncertainty,[35] for instance, due to incomplete and asymmetric information.[36] This means that privacy decisions' consequences and the probability of their occurrence are mostly unknown to users, which argues against the mere rational weighting of costs and benefits involved in the so-called privacy calculus.[37]

The rationality assumption of the privacy calculus has its limits and is just one explanation for the observed incongruence between privacy attitudes and behaviour – a phenomenon known as information privacy paradox.[38] Study results from research fields such as psychology and information systems indicate that privacy-related decisions heavily depend on the given context and are impacted by humans' innate bounded rationality[39] and incomplete or asymmetric information. Further influencing factors are, inter alia, affective states,[40] motivational aspects,[41] personality traits,[42] pre-existing awareness and knowledge, social norms,[43] and cultural[44] and generational[45] influences. This complexity of factors often leads to users leaning on heuristics. A heuristic is defined as 'a strategy that ignores part of the information, with the goal of making decisions more quickly, frugally, and/or accurately than more complex methods'.[46] Heuristics mostly result in efficient and acceptable judgments. At the same time, they might lead to systematic misjudgements, so-called cognitive biases.[47] In the context of privacy policies, the framing effect is just one example of cognitive bias-

[32] *cf* Acquisti et al (n 30); Lorrie F. Cranor, 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2012) 10 Journal on Telecommunications & High Technology Law 273.

[33] Ting Li and Till Unger, 'Willing to Pay for Quality Personalization? Trade-off between Quality and Privacy' (2012) 21(6) European Journal of Information Systems 621.

[34] Cormac Herley, 'So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users' (2009) Proceedings of the Workshop on New Security Paradigms (NSPW'09) ACM 133.

[35] We are aware that the definition of 'uncertainty' differs between or even within disciplines. *See, eg,* Alessandro Acquisti and Jens Grossklags, 'An Online Survey Experiment on Ambiguity and Privacy' (2012), 88 (4th Q) Digiworld Economic Journal 19.

[36] Acquisti, Brandimarte and Loewenstein (n 29).

[37] Mary J Culnan and Pamela K Armstrong, 'Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation' (1999) 10 Organization Science 104; Tamara Dinev and Paul Hart, 'An Extended Privacy Calculus Model for E-Commerce Transactions' (2006) 17 Information Systems Research 61.

[38] For further information about the privacy paradox research, *see* Spyros Kokolakis, 'Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon' (2017) 64 Computers & Security 122.

[39] *See* Herbert A Simon, 'The Scientist as Problem Solver' in David Klahr and Kenneth Kotovsky (eds), *Complex Information Processing: The Impact of Herbert A. Simon* (Erlbaum 1989) 373.

[40] Robin Wakefield, 'The Influence of User Affect in Online Information Disclosure' (2013) 22 The Journal of Strategic Information Systems 157; Flavius Kehr et al, 'Blissfully Ignorant: the Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus' (2015) 25 Information Systems Journal 607.

[41] Asimina Vasalou et al, 'Understanding Engagement With the Privacy Domain Through Design Research' (2015) 66 (6) Journal of the Association for Information Science & Technology 1263.

[42] Serge Egelman and Eyal Peer, 'The Myth of the Average User: Improving privacy and security systems through individualization' (2015) Proceedings of the New Security Paradigms Workshop on ACM - NSPW 15, 16.

[43] Alessandro Acquisti, Leslie K. John and George Loewenstein, 'The Impact of Relative Standards on the Propensity to Disclose' (2012) 49 Journal of Marketing Research 160.

[44] Acquisti, Brandimarte and Loewenstein (n 29).

[45] Caroline L Miltgen and Dominique Peyrat-Guillard, 'Cultural and Generational Influences on Privacy Concerns: a Qualitative Study in Seven European Countries' (2014) 23(2) European Journal of Information Systems 103.

[46] Gerd Gigerenzer and Wolfgang Gaissmaier, 'Heuristic Decision Making' (2011) 62 Annual Review of Psychology 451, 454.

[47] Amos Tversky and Daniel Kahneman, 'Judgment under Uncertainty: Heuristics and Biases' (1974) 185(4157) Science 1124.

es: privacy decisions are affected by the way in which various choices are framed, for example, through wording, settings or situations. Often, options that are less sensitive to privacy considerations are framed solely in a positive manner, while intentionally leaving out possible adverse implications for users. Sometimes, such framing may present consequences that intend to intimidate the user, for instance, with the threat of losing their account.[48]

IV. Visualisation Through Privacy Icons as a Solution Approach

In literature, there is a broad discussion on how regulation should deal with those deficiencies. This section provides a short overview on solution approaches that have been proposed, and then, it elaborates on the advantages of visualisation through privacy icons as a solution approach that preserves the role of individual consent.

1. Solution Approaches Alternative to Visualisation

In light of the manifold deficiencies as described above, some scholars are sceptical about viability of consent in general,[49] and others considered giving up on consent altogether,[50] or, based on the argument of consent overuse,[51] suggested limiting[52] its scope or making it subsidiary vis-à-vis other grounds of processing.[53] Accordingly, instead of performing a balancing of interests on an individual level, the legality of data processing would be determined by third parties, either ex post through the judicial system or ex ante through competent authorities.[54] However, such a substitution of consent with decisions of higher authorities would not sufficiently observe the underlying principle of autonomy as described above.[55]

Alternatively, other proposals aim to improve the process of granting consent by mostly focusing on making users better informed. One early example for a technical approach is the Platform for Privacy Preferences Project (P3P).[56] By using a machine-readable syntax for privacy policies, it enabled the user's browser to interpret the privacy statements, and could, for example, warn of unwanted elements in accordance with the user's preferences.[57] While the P3P could not reach a critical mass in terms of broad usage, there are similar recent projects that try to utilise the newest research results in the fields of machine-learning[58] and artificial intelligence in order to assist consent decisions.

Especially so-called Personal Information Management Systems (PIMS)[59] should be mentioned. One of the key elements of PIMS is an algorithm that learns about the user's privacy behaviour and preferences, and then helps him or her in implementing those preferences through a (partly) autonomous choice architecture. Those opportunities facilitated by machine-readable privacy policies have not gone unnoticed by the European legislature; unfortunately, machine-readability is only briefly mentioned

[48] Forbrukerrådet, 'DECEIVED BY DESIGN: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy' (Norwegian Consumer Council 2018) 22-25 <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

[49] *see eg,* Bart W Schermer et al, 'The Crisis of Consent: How Stronger Legal Protection may Lead to Weaker Consent in Data Protection' (2014) 16(2) Ethics and Information Technology 171 (speaking of 'consent desensitisation').

[50] *cf* Philip Radlanski, *Das Konzept der Einwilligung in der datenschutzrechtlichen Realität* (Mohr Siebeck 2016) 97.

[51] Alexander Roßnagel et al, *Datenschutzrecht 2016, „Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts* (Kassel University Press 2016) 97-98; Benedikt Buchner, *Informationelle Selbstbestimmung im Privatrecht* (Mohr Siebeck 2006) 254.

[52] ibid 130-131.

[53] Radlanski (n 50) 204-206, 232-233; *see also,* Article 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context' 5062/01/EN/Final (13 September 2001) 23 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf>.

[54] *cf* Buchner (n 51) 276-278 (proposing data trustees ('Datentreuhänder') in addition to consent).

[55] Such a practice could particularly conflict with German Constitutional Law, *see* Patricia M Rogosch, *Die Einwilligung im Datenschutzrecht* (Nomos 2013) 97-99.

[56] W3C, 'Platform for Privacy Preferences (P3P) Project' <https://www.w3.org/P3P/>.

[57] ibid.

[58] 'The Usable Privacy Project', <https://www.usableprivacy.org/>, working on the automated translation of privacy policies into machine-readable text through natural language processing.

[59] European Data Protection Supervisor (EDPS), 'Opinion on Personal Information Management Systems (Opinion 9/2016): Towards more user empowerment in managing and processing personal data' (2016) 5 <https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf>. *See also*, Stiftung Datenschutz, 'Policy Paper: New ways of providing consent in data protection – technical, legal and economic challenges' (Stiftung Datenschutz 2017) <https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_PolicyPaper_New_ways_of_providing_consent_in_data_protection_EN_final.pdf>.

within the GDPR.[60] Efforts in this field are ongoing and the direction of research is promising, but it is too early to assess the future impact of such technical solutions as of yet. In the remainder of this Section IV, we elaborate on visualisation via privacy icons as a promising solution approach.

2. Definition of Privacy Icons

Our study focuses rather on a measure that could be implemented more quickly: Privacy icons. With the term 'privacy icons' we refer to a set of standardised,[61] easily (even intuitively) comprehensible and self-implementable[62] pictograms that display aspects of specific data processing practices (evaluated on the basis of their risks).[63] Thus, users may gain a better understanding of possible privacy consequences, which would reduce uncertainty and facilitate better informed decisions. By investigating questions of design and content of such privacy icons in the past several years, various projects have established the foundation for further research in the field.[64]

3. Chances and Challenges of Privacy Icons

Privacy icons have a significant potential to counteract many of the previously mentioned factors that hamper the decision process.

Pictures, as opposed to texts, have an advantage in terms of faster recognition as well as less effortful memory recall, an effect known as 'picture superiority'[65]. The effect of pictorial representations on privacy-protective behaviours has been observed in some studies. Raja et al showed that users were able to better comprehend warning information and had a better risk perception when they were confronted with firewall warnings that depicted metaphors, such as a locked door and a bandit, compared to the usual text warnings.[66]

Generally, it should be kept in mind that data protection is usually not a priority for users, as they are mostly focused on achieving their primary goal, for instance, acquiring a commodity or obtaining access to an online service. In order to draw their attention away from their primary goal towards data processing aspects, highly salient, external stimuli are needed.[67] This could be achieved through risk-based icons.

Icons have additional advantages: they can communicate meanings independently of textual literacy and linguistic barriers in a standardised manner. It is important, however, to consider cultural differences in terms of the meaning of symbols and colours.[68] Further, standardised privacy icons would enable comparability of options across entities, which ultimately could lead to users' awareness of truly having a choice, especially in e-commerce: In 2011, Tsai et al discovered that when privacy information of websites is made more accessible and noticeable in a way that enables users to easily detect differences in retailers' privacy management, they prefer retailers that are more privacy-protective, even if this means paying more for a product, compared to cheaper offers from retailers less protective of users' privacy.[69] The resulting privacy-sensitive re-

[60] art 12(7), recital 60 GDPR and art 20(1), recital 68 GDPR.

[61] On the importance of standardisation *see* Art. 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' 17/EN WP 260 rev. 01 (11 April 2018) 25-26 <https://bit.ly/2t2anbv>.

[62] Self-implementable means that data processors, based on general implementation guidelines, retain a certain latitude regarding the selection of icons presented according to individual data processing specifities.

[63] s V. below.

[64] To mention just a few projects we looked into so far: Louisa Specht and Linda Bienemann, 'Informationsvermittlung durch standardisierte Bildsymbole - Ein Weg aus dem Privacy Paradox?' in Louisa Specht, Nikola Werry and Susanne Werry (eds) *Handbuch Datenrecht in der Digitalisierung* (forthcoming); Arianna Rossi and Monica Palmirani, 'GDPR by Legal Design' <http://gdprbydesign.cirsfid.unibo.it/>; 'The Mozilla Privacy Icons Project' <https://wiki.mozilla.org/Privacy_Icons>; 'Terms of Service Didn't Read' <https://tosdr.org/>; 'CommonTerms', <http://www.commonterms.net/>, ([discontinued) archived version available under <https://t1p.de/ct2018>; 'The Privacy Nutrition Labels' <https://cups.cs.cmu.edu/privacyLabel/>; Mary C Rundle, 'International Data Protection and Digital Identity Management Tools', 13 September 2006 (Position Paper Submitted for the W3C Workshop on Language for Privacy Policy Negotiation and Semantics-Driven Enforcement in Ispra/Italy, 17 and 18 September 2006).

[65] Allan Paivio, *Imagery and Verbal Processes* (Holt, Rinehart & Winston 1971); Allan Paivio, 'Imagery in Recall and Recognition' in John Brown (ed.), *Recall and Recognition* (Wiley-Blackwell 1976) 103.

[66] Fahimeh Raja et al, 'A Brick Wall, a Locked Door, and a Bandit' (2011) 11 Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS 1.

[67] For further information about attentional processes, *see* Fumi Katsuki and Christos Constantinidis, 'Bottom-Up and Top-Down Attention: Different Processes and Overlapping Neural Systems' (2013) 20(5) The Neuroscientist 509.

[68] Jakob Nielsen, 'International User Interface' in Jakob Nielsen (ed.), *Usability engineering* (Morgan Kaufmann 1994) 239.

[69] Janice Y Tsai et al, 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study' (2011) 22 Information Systems Research 254.

consideration of the data processing induced by icons could even be utilised as a competitive advantage.[70]

Icons, of course, are not a silver bullet. Broad and frequent display carries the danger of users habituating to them. Empirical studies on security warning habituation report a decrease in users' visual attention due to the repeated exposure to standardised warning messages.[71] However, there are some mechanisms that can be taken into consideration while working against habituation effects, such as polymorphic variations of the design, for example, variations in colour, highlights, signal words, contrasts or borders.[72]

The icons set cannot be exhaustive, however. The presentation of too many icons would most likely lead to an information overload,[73] which would affect not only attentional processes but would also be problematic with regard to the limited capacity of the working memory.[74]

Therefore, a set of icons can neither replace legal transparency obligations under the GDPR, nor can it visualise all risky aspects of data processing. Its mission is rather to reduce uncertainty and cognitive effort by increasing the transparency and tangibility of possible privacy consequences. Furthermore, icons should increase users' attention, motivation and awareness in dealing with typical data processing aspects and their inherent risks prior to consent. Hence, the icons set will merely supplement the privacy policy while functioning as an attention-getting entry point. The challenge is to develop icons that are salient and meaningful and, at the same time, indicate their limitations of being non-exhaustive in order to not mislead users.[75]

4. The Legal Framework

Such a solution is also encouraged by the GDPR, which, for the first time in EU data protection legislative history, indicates the importance of visualisation in the field of data protection and even included a suggestion for a set of icons in an earlier draft.[76] Alongside possibilities such as certificates, seals and marks (Articles 42 and 43 GDPR), it allows for displaying standardised icons in Article 12(7), 12(8) GDPR.[77] Icons that are already encouraged to be used voluntarily under Article 12(7) can also be made obligatory:[78] According to Article 12(8), the Commission can determine the information *to be displayed* by icons and the procedures for *providing* such icons. When executing its power, the Commission can expect support from the European Data Protection Board (EDPB) (Article 70(1)(r)) and should undertake appropriate consultations – especially at expert lev-

[70] Lorenz Franck, 'Art. 12 DSGVO' in Peter Gola (ed.), *Datenschutz-Grundverordnung* (2nd ed, CH Beck 2018) Rn 46 (on icons as a competitive advantage).

[71] Soyun Kim and Michael S Wogalter, 'Habituation, Dishabituation, and Recovery Effects in Visual Warnings' (2009) 53(20) Proceedings of the Human Factors and Ergonomics Society Annual Meeting 1612; Bonnie B Anderson et al, 'Users Aren't (Necessarily) Lazy: Using neuroIS to explain Habituation to Security Warnings' (2014) Thirty Fifth International Conference on Information Systems 1.

[72] Bonnie B Anderson et al, 'Your Memory Is Working Against You: How Eye Tracking and Memory Explain Habituation to Security Warnings' (2016) 92 Decision Support Systems 3; Bonnie B Anderson et al, 'From Warning to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It' (2016) 33(3) Journal of Management Information Systems 713; MS Wogalter and CB Mayhorn, 'The Future of Risk Communication: Technology-based Warning Systems' in Michael S Wogalter (ed.), Handbook of Warnings (CRC Press 2006) 783-793.

[73] *cf* Martin Eppler and Jeanne Mengis, 'The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines' (2004) 20(5) Information Society 325; Peter G Roetzel, 'Information Overload in the Information Age: a Review of the Literature from Business Administration, Business Psychology, and Related Disciplines With a Bibliometric Approach and Framework Development' (2018) Business Research 1.

[74] The visual working memory plays a decisive role in decision-making and is defined as the 'active maintenance of visual information to serve the needs of ongoing tasks.' *See* Steven J Luck and Edward K Vogel, 'Visual Working Memory Capacity: From Psychophysics and Neurobiology to Individual Differences' (2013) 17(8) Trends in Cognitive Science 391.

[75] *cf* David Spiegelhalter, Mike Pearson and Ian Short, 'Visualizing Uncertainty About the Future' (2011) 333(6048) Science 1393.

[76] European Parliament, 'Position of the European Parliament [on the GDPR, Annex]' (2012) PE526.549, EP-PE_TC1-COD(2012)0011 (Annex); for an interesting study on the limited intelligibility of the proposed icons, *see* John Pettersson, 'A Brief Evaluation of Icons in the First Reading of the European Parliament on COM (2012) 0011' in Jan Camenisch, Simone Fischer-Hübner and Marit Hansen (eds), *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (Springer 2017) 125. The academic and general discussion on privacy and visualisation preceded its inclusion in the GDPR legislation drafts.

[77] *see also,* the corresponding art 8(3), 8(4) in the Commission's draft for the ePrivacy Regulation, Commission, 'Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', COM(2017) 10 final, 2017/0003(COD).

[78] Instead of many, *see* Matthias Bäcker, 'Art. 12 DS-GVO' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG: Kommentar* (2nd edn, CH Beck 2018) 24. For an opposing view, *see* Holger Greve, 'DS-GVO Art. 12' in Gernot Sydow (ed.), *Europäische Datenschutzgrundverordnung* (2nd edn, Nomos 2018) 32 (with further references).

el[79] (Recital 16) – which stresses the relevance of a science-driven process.

Concerning the contents of such obligatory icons, Article 12 GDPR draws no exact guidelines. Article 12(7) indeed refers to Articles 13, 14 and states that the icons may *complement* the information duties laid out in those articles. However, Article 12 neither determines that icons should represent all the obligatory information mentioned in Articles 13, 14, nor does it provide that the contents are limited to this kind of information. Instead, the reference to Articles 13, 14 only addresses the scope of Article 12(7) and 12(8). The provisions concerning icons should (primarily) apply when Articles 13, 14 require a provision of information – in contrast to information presented based on Article 15, for example.[80] However, when it comes to possible contents of the icons, Article 12(7), 12(8) should be interpreted broadly[81], as it is the GDPR's aim to inform the user comprehensively. Correspondingly, Recital 60 states that 'any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context' should be delivered to the data subject and may be provided through icons. Consequently, when choosing the contents of the icons, Articles 13, 14 do not limit the Commission's power under Article 12(8).

As obligatory icons would touch upon the data processor's rights and protected commercial interests, their content, design and implementation would have to be proportionate and compatible with superior legal frameworks. For instance, the processor's freedom to conduct a business according to Article 16 of the Charter of Fundamental Rights of the European Union (CFR)[82] would need to be balanced against the data subject's fundamental rights according to Articles 7, 8 CFR. In order not to violate the GDPR itself, the presentation of the icons would also have to unambiguously demonstrate that they only represent some key facts and should in no way obstruct access to the underlying privacy policy.

V. A Risk-Based Approach to Privacy Icons

We have seen that privacy icons can contribute to making consumers better informed before giving consent by alleviating some of the structural deficiencies mentioned above. In order to achieve the best possible results, the concept and the development of the icons must necessarily be based on scientific findings.

1. A Methodology for Icons Development

In the following, we outline our preliminary project plan. The development of the final icons set is divided into five phases.[83] The final goal is to create icons that visualise data processing aspects selected on the basis of their inherent risks and also to indirectly communicate those risks to the users.

Due to the complexity of possible negative privacy consequences, users will always encounter difficulties of identifying and estimating risks and will therefore be confronted with privacy uncertainty online. However, privacy uncertainty can be reduced and users decisions can be improved through a risk assessment[84] of data processing aspects (to be conducted within the first two phases explained below). We will identify risks, categorise them and develop decision criteria for the evaluation of their impact and severity using a multi-method approach.

Phase 1: The aim in phase one is to gather a broader understanding of the concept of risk which underlies the GDPR (see below V.2) and on that basis generate a comprehensive catalogue of data processing aspects and possible inherent risks. For this purpose, legal experts will conduct a qualitative content analysis[85] to systematically examine the GDPR. Thereafter, the tentative list will be enriched by further insights from expert interviews. In this context, we define 'ex-

[79] Correspondingly, Expert Group 3537 (Multistakeholder expert group to support the application of Regulation (EU) 2016/679)) was established in order to make use of the Commission's delegated power.

[80] *cf* Lorenz Franck (n 70) Rn 50 (even extending the scope of art 12(7) GDPR to other situations).

[81] *See also,* s V.1. below.

[82] Charter of Fundamental Rights of the European Union (2012) OJ C 326, 391-393.

[83] The authors also organised an expert workshop on the potential of icons with regard to informed consent at the Weizenbaum Institute in February 2019. A short summary of the workshop is available here: <https://weizenbaum-institut.de/media/Permalinks/PIP_Workshop-Short_Report_Engl_7May_FINAL.pdf>.

[84] For further information about risk analysis, *see* Charles Yoe, *Primer on Risk Analysis: Decision Making Under Uncertainty* (2nd ed, CRC Press 2019).

[85] Philipp Mayring, 'Qualitative Content Analysis' (2000) 1(20) Forum: Qualitative Social Research Art. 20.

perts' as persons who are active in data protection research or practice, such as IT security experts, information scientist, lawyers, et cetera.

Phase 2: In this phase, we will narrow down the selection to the most relevant and important data processing aspects that should be ultimately visualised. To do so, we will ask experts to rank data processing aspects according to their inherent risk based on predefined criteria such as the impact and severity of adverse privacy events, counterbalance aspects such as the use of state-of-the-art technologies, et cetera. Furthermore, we will ask a representative user sample to rank the same data processing aspects as well. This allows us to compare the expert and user sample ranking with each other and reveal any misconceptions about privacy risks in the public. A revelation of significant differences could highlight the importance of digital literacy and the need for change in the educational system, for instance, by introducing privacy and security courses. Moreover, this comparison would provide insights into the needs of users and to determine the presentation order of our final privacy icons set in order to further increase users' attention towards data protection. The last step within this phase will be the determination of different risk levels and their grading criteria of each data processing aspect, for example, which criteria lead to categorising encryption technologies as more safe or less safe.

Phase 3: This phase involves a collaboration with information designers to determine the final icons set in terms of the feasibility of visualising certain data processing aspects and their inherent risk levels.

Phase 4: Here, we will test the icons with regard to their intended purpose. We will evaluate and revise them at various stages of the development process using mixed methods. For example, a possible test could address the icons' comprehensibility, recognisability and information scent. We intend to research whether the icons increase users' motivation to engage with and their awareness of data protection issues. Moreover, it is of interest to find out whether the icons draw users' attention towards data protection in general.

Phase 5: In the final step, we plan to create a manual with instructions for controllers on how to implement the icons set, for instance, in deciding which icons to use when certain data protection processes take place.[86]

2. The Concept of 'Risk' in the GDPR

The main objective of phase one of the project is to generate a comprehensive catalogue of data processing aspects and their inherent risks based on the GDPR. Therefore, we first need to understand the concept of 'risk' which underlies the GDPR.

a. Introduction

The central criterion underlying our project is the so-called 'risk-based approach'. This concept is neither new nor limited to the GDPR. It can already be found within the Data Protection Directive[87], for instance, in the context of the provisions on security in Article 17(1), or on prior checks of processing operations in Article 20(1).[88] The (former) Article 29 Working Party strongly supports this concept. In its respective statement, it explains that the level of risk involved in a specific data processing operation must be without any prejudice to the data subject's rights, while, however, the scale of the controller's obligations shall increase as the risk in the specific case increases.[89]

While the risk-based approach has been applied in particular to compliance requirements so far, our understanding is broader. The special Eurobarometer report on data protection from 2015 has shown that EU citizens are concerned about various risks in the context of personal data processing.[90] Communicating data processing aspects and their inherent risks in a way that is more accessible and transparent to users could address those concerns and promote informed decision-making. Against this backdrop, we intend to consider the particular level of risk associated with various aspects of personal data processing as a methodological criterion for deciding

[86] A more detailed description of each phase and the methods to be used will be provided in the respective articles that will build on and follow this article.

[87] Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).

[88] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' WP218 (30 May 2014) 2 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

[89] ibid 2-3.

[90] European Commission, 'Special Eurobarometer 431: Data Protection' [2015] <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf>.

which aspects of the processing should be visualised by privacy icons, how to design these icons, and how to implement them.

b. Legal Analysis

Our approach raises the basic question of how to understand the notion of 'risk' in accordance with the GDPR. While the GDPR does not provide for a legal definition of the term 'risk', numerous explicit and implicit references can be found within its provisions, such as in the context of the responsibility and liability of the controller (Article 24(1)), data protection impact assessments (DPIAs) (Article 35(1), (3), (4)), or profiling (Article 35(3)(a)).[91]

In principle, the GDPR distinguishes between situations where personal data processing is '*unlikely* to result in a risk to the rights and freedoms natural persons' (Recitals 80, 85, Articles 27(2)(a), 33(1)), where personal data processing is '*unlikely* to result in a high risk' (Recital 77), or, to the contrary, where the processing of personal data 'is *likely* to result in a risk' (Article 30(5)) or is even '*likely* to result in a high risk to the rights and freedoms of natural persons' (Recitals 84, 89, Article 34(1)).[92] Specifically, Recitals 75, 76 state that the risk 'may result from personal data processing which could lead to physical, material or non-material damage' while the risk's 'likelihood and severity [...] should be determined by reference to the nature, scope, context and purposes of the processing [...] on the basis of an objective assessment'. The GDPR does not define these key terms, yet the wording 'rights and freedoms' and 'physical, material or non-material damage' indicates the intention to provide a comprehensive protection to data subjects. It thereby calls for a broad understanding of the notion of 'risk'.

According to Article 1(2), it is the GDPR's explicit objective to protect 'the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'. In comparison, the notion of 'rights and freedoms' in the context of risk is broader and does not only refer to the fundamental rights provided for by the CFR – and its Article 8 on the protection of personal data in particular – or by the European Convention for the Protection of Human Rights and Fundamental Freedoms, but covers also ordinary law such as the GDPR itself.[93] Therefore, each personal data processing operation by default entails a certain risk to the right on the protection of personal data and to the rights secured for data subjects under the GDPR. Such risk materialises as a damage where the processing is not in accordance with the GDPR.[94] In addition, the wording 'physical, material and non-material damage' also is conceivably wide and can – according to the German data protection authorities[95] – be understood as any negative consequence of the intended processing itself, or even as any negative consequence of any deviation from the intended processing, for instance, unauthorised disclosure.

The GDPR provides specific examples of risks in several provisions. In particular, Recital 75 lists both risks and situations that are prone to jeopardise the rights and freedoms of natural persons, namely:

> [...] discrimination, identity theft or fraud, financial loss, damage to the reputation, [...] any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms, or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated [...] in order to create or use personal profiles; where personal data of vulnerable natural persons [...] are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Additional examples can be found in Recital 71 on profiling, Recital 85 on notifications of personal data breaches, or Recital 91 and Article 35(3) on situations where a DPIA is necessary.[96] It is also noteworthy that the GDPR does not clearly draw a distinction between data protection risks and typical IT securi-

[91] A comprehensive list of references provided by the authors is available at <https://weizenbaum-institut.de/media/Permalinks/Concept_of_Risk_in_the_GDPR_v.2_06.05.19.pdf>.

[92] Emphasis added.

[93] Datenschutzkonferenz, 'Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen' (26 April 2018) 1 <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf>.

[94] ibid 1, 3.

[95] ibid 2-3.

[96] *see* n 91 (list of references to risks).

ty risks. Especially Recital 83 (and similarly Article 32(2)) states, that

> [i]n assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Also, provisions such as Articles 8, 9 and 10 GDPR that do not explicitly refer to risks indicate that certain aspects of data processing are prone to particular high risks by imposing special obligations on controllers.[97]

c. Risk Assessment

Although it seems difficult to measure certain risks mathematically, the GDPR stresses (Recital 76) the importance of an objective risk assessment.[98] Pursuant to this and based on the legal text of the GDPR, the Article 29 Working Party developed nine criteria of especially risky data processing. Those are 'Evaluation or scoring', 'Automated-decision making with legal or similar significant effect', 'Systematic monitoring', 'Sensitive data or data of a highly personal nature', 'Data processed on a large scale', 'Matching or combining datasets', 'Data concerning vulnerable data subjects', 'Innovative use or applying new technological or organizational solutions' and 'When the processing in itself prevents data subjects from exercising a right or using a service or a contract'.[99] It explains 'that the more criteria are met by the processing, the more likely it is to present a high risk [...] regardless of the measures which the controller envisages to adopt'.[100]

Pursuant to Article 35(4) GDPR, the national data protection authorities have developed so-called 'black lists' that provide an overview of personal data processing operations that typically cause high risks, and therefore, always require a DPIA. These non-exhaustive lists specify the stipulations of Article 35(1) GDPR, which, however, prevails in case of a possible conflict.[101] In order to ensure consistency throughout the EU, the EDPB has been publishing opinions on the respective lists.[102] The German data protection authorities, for instance, describe seventeen different aspects of personal data processing with inherent high risks, including, amongst others, 'Large-scale processing of personal data about the location of natural persons' such as 'Vehicle data processing – Car Sharing / Mobility Services' or 'Traffic flow analysis based on location data of the public mobile network'.[103] More generally and without limitation to DPIAs, the German data protection authorities also suggest a risk matrix that may help assessing specific risks by examining whether their likelihood and severity are minor, manageable, substantial or major.[104]

d. Individual v Societal Risks

Another question is whether only individual risks to the respective data subject may be taken into account, or whether societal risks[105] can be considered as well. The GDPR does not refer to societal risks explicitly, but it does not limit itself to specifically individual risks in general either.[106] It speaks of '[t]he risk to the rights and freedoms of natural persons' (Recital 75) in a relatively general way, and in the context of DPIAs even of 'the rights and legitimate interests of

[97] *cf* Article 29 Working Party (n 88) 2 regarding art 8 Data Protection Directive on the processing of special categories of data.

[98] Datenschutzkonferenz (n 93) 4.

[99] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' WP 248 rev.01 (4 October 2017) 9-11 <http://ec.europa.eu/newsroom/document.cfm?doc_id=47711>.

[100] ibid 11.

[101] EDPB, 'Opinion 5/2018 on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)' (25 September 2018) 5 <http://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-germany-sas-dpia-list_en>.

[102] EDPB, 'Opinions' <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en>; EDPB (n 101) 3.

[103] Datenschutzkonferenz, 'List of processing activities for which a DPIA is to be carried out' (17 October 2018) 1-2 <https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DPIA_list_1_1__Germany_EN.pdf>.

[104] Datenschutzkonferenz (n 93) 4-6. Similarly, but limited to the context of DPIAs, the French data protection authority also suggests four categories to assess the level of risk: CNIL, 'Analyse d'impact relative à la protection des données, Les bases des connaissances' (February 2018) 3-5 <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf>.

[105] On societal risks of privacy self-management, *see* Solove (n 3) 1892-1893; instructive on the relation of individual consent and social consequences, *see* Yoan Hermstrüwer, *Informationelle Selbstgefährdung* (Mohr Siebeck 2016) (exemplary 184-186).

[106] An exemption hereof is, for instance, recital 76 GDPR, which speaks of 'the risk to the rights and freedoms of the data subject' in the singular only.

data subjects and other persons concerned' (Article 35(7)(d)). Even more important, Recital 72 refers to the individual 'risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons' without limiting such discriminatory effects to the data subject in question. Moreover, the GDPR acknowledges in Recital 4 that '[t]he processing of personal data should be designed to serve mankind' and that [t]he right to the protection of personal data [...] must be considered in relation to its function in society'. Considering this and the fact that the GDPR aims at a high level of data subject protection, there are valid arguments to also take into account risks that go beyond merely individual ones.[107]

e. Risk-Based Approach and Privacy Icons in the Light of Article 12(7) GDPR

Finally, it should be examined, whether apllying such a risk-based approach as a methodological criterion for choosing data processing aspects for visualisation is consistent with Article 12(7) GDPR. Article 12(7) states that '[t]he information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons' without explicitly referring to risks or to any additional information. However, there seems to be no conflict between Article 12(7) and the application of a risk-based approach in the context of privacy icons or using icons to communicate data processing aspects that go beyond the content of Articles 13, 14 (Section IV.4).

Firstly, the intended visualisation primarily focuses on aspects of personal data processing as such, for instance, the category of the data being processed (eg, 'sensitive data'). This does not include visualisation of the underlying risks in the first place (eg, 'discrimination' or 'identity theft'). The level of risk inherent in the data processing works as a criterion for deciding which aspects of the processing should be visualised and how to design and implement the icons.

Secondly, a closer inspection reveals that some of the information mentioned in Articles 13, 14 actually concern aspects of data processing that are identified as especially risky elsewhere in the GDPR. Under certain circumstances, transfers to third countries or international organisations (Articles 13(1)(f), 14(1)(f)), for instance, require the explicit consent of the data subject 'after having been informed of the possible risks of such transfers [...]' (Article 49(1)(a)). Even more evident, automated decision-making and profiling (Articles 13(2)(f), 14(2)(g)) are clearly associated with particular risks in Recitals 71, 75, 91 and Article 35(3)(a). This interrelation between some of the information obligations pursuant to Articles 13, 14 and other references in the GDPR in the context of risk does not only mean that these aspects can be communicated in combination with privacy icons pursuant to Article 12(7), but may lead to the conclusion that there is a special need to inform the data subjects about aspects of personal data processing that entail particular risks.

Thirdly, the GDPR explicitly stresses the importance of communicating risks to data subjects several times in other places. According to Article 57(1)(b) and complemented by Recital 122, the supervisory authority should, amongst others, 'promote public awareness and understanding of the risks [...] in relation to the processing of personal data'. Even more important, Recital 39 states in respect of the principles of lawful processing that '[n]atural persons should be made aware of risks [...] in relation to the processing of personal data'. If privacy icons allow us to communicate risks even better, Article 12(7) should be teleologically interpreted as permitting us to visualise further aspects of data processing based on their respective level of risk in combination with privacy icons.

VI. Design and Enforcement Prospects

The icon development process as described in Section V.1 incorporates fundamental design and enforcement questions. In order to give an outlook on the future phases of the project, this section briefly discusses some of the most important aspects.

1. Design Considerations

Usability research differentiates between three basic types of icons: reference, arbitrary and resemblance

[107] The UK data protection authority also considers societal impacts as potential risk factors, however, without discussing the topic in detail; ICO, 'What is a DPIA?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/#what4>.

icons.[108] To increase memorability and recognisability, usability studies have shown the advantages of so-called resemblance icons, which reflect physical objects.[109] For instance, e-commerce portals often show the shopping cart icon so that people can easily and without the need of further cognitive resource derive the meaning.

Another consideration is whether the icons should be neutral in colour, content and design, or whether they should transport an evaluation, for instance, by signalling a warning through colour-grading. An icon might, for example, warn against the non-encrypted transmission of data by displaying an open red-coloured lock, while signalling safety by displaying a closed green-coloured lock where the transfer is encrypted. Using colours in this way carries a normative choice of the designer. An obligation to implement such icons might impinge more strongly upon the processor's rights and even be considered a form of paternalism (through nudging).[110]

Nevertheless, we believe that active warning signals are necessary and can be applied in a proportionate manner. The information level amongst users about the consequences of data processing is low. A risk-based approach aiming to indirectly communicate possible consequences (whilst visualising data processing aspects) can thereby reduce the information asymmetry, draw users' attention to such aspects and increase their motivation to deal with important data protection questions. Security and privacy research based on the protection motivation theory[111] show that making users aware of the severity of security threats (eg, by presenting possible risks) is one important factor that contributes to increased security protection on the levels of intentions and behaviours.[112]

In addition, including an (objective) assessment of the visualised data processing aspects would compensate for differing knowledge levels. The knowledge necessary to evaluate the risk-level induced by a data processing aspect can be highly influenced by media coverage. This can lead to systematic biases due to the occurrence of the availability heuristic[113]. In order to assess the significance of pseudonymisation, for example, users would need to know that there is also the possibility of anonymisation and have a basic understanding of the differences between anonymisation and pseudonymisation. Here, users' decisions could be facilitated by colour-grading. A red-coloured icon for regular data, an orange icon for pseudonymised data and a green icon for anonymised data would hopefully signal to the user that processing of fully anonymised data entails less risk than processing of pseudonymised data.[114]

Similarly, from a design perspective, coloured icons could improve comprehensibility. Colours would transport additional information and therefore help users to better understand the meaning. Keeping cultural differences and personal limitations in mind, we expect that a green closed lock, for example, will transport the intended meaning (encrypted transmission) more reliably than a black-and-white closed lock, which would have to be situated in relation to its counterpart (an open lock). In conclusion, the design of the icons does not necessarily have to be neutral but should transport additional evaluation information, where reasonable.

Another important design question concerns the number of icons to be displayed in each individual scenario. The number of icons displayed should be rather small in order to avoid any information overload. Therefore, icons that would have to be displayed in all cases are excluded in the selection process. For example, users' rights (such as the right to data portability) apply in a similar way to every data procession. Informing users of such rights should therefore

[108] Nielsen (n 68).

[109] ibid.

[110] Instructive on the interplay between nudging and paternalism regarding informed consent, *see* Sheng Yin Soh, 'Privacy Nudges: An Alternative Regulatory Mechanism to 'Informed Consent' for Online Data Protection Behaviour' (2019) 5(1) EDPL 65. Cass Sunstein and Lucia Reisch have recently emphasised that nudging, particularly through the government, should fulfil some legitimacy criteria that are somewhat comparable to being compatible with a "bill of rights". *See* Cass R Sunstein and Lucia A Reisch, 'A Bill of Rights for Nudging' (2019) EuCML 93.

[111] Ronald W Rogers, 'A protection motivation theory of fear appeals and attitude change' (1975) 91(1) Journal of Psychology 93.

[112] Scott R Boss et al, 'What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors' (2015) 39 (4) MIS Quarterly 837; Stanislav Mamonov and Raquel Benbunan-Fich, 'The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors' (2018) 83 Computers in Human Behavior 32.

[113] This heuristic describes how information that can be easily recalled from memory, for example through recent or more frequent media coverage, influences the judgement of the likelihood of an event. *See* Amos Tversky and Daniel Kahneman, 'Availability: A heuristic for judging frequency and probability' (1973) Cognitive Psychology 207.

[114] Concerning the interrelation of perceived hazards and colours, *see* Tonya L Smith-Jackson and Michael S Wogalter, 'Users' hazard perception of warning components: An examination of colors and symbols' (2000) 44 (6) Proceedings of the International Ergonomics Association & the Human Factors and Ergonomics Society Congress 55-557 (with further references).

be performed via channels of public education rather than *via* icons.

2. Enforcement Outlook

Once a set of icons has been designed, it is critical for the success of privacy icons that there is an enforcement strategy in place – a strategy that many of the projects so far seem to have lacked. Paradigmatically, the Mozilla Privacy Icons Project seems to have hoped that companies would see the icons as a 'competitive differentiator' and implement them voluntarily for strategic reasons.[115] Such a bottom-up implementation of privacy icons proved overly optimistic, as the usage of icons creates a level of transparency that is not necessarily in line with the data processing strategies of many companies.

Therefore, a more normative approach is required. As an amendment of the GDPR cannot be expected any time soon, the most direct[116] regulatory approach would be a delegated act by the Commission in accordance with Article 12(7) and (8) GDPR.[117] A finalised set of icons based on scientific findings could hopefully encourage the European Commission to favourably consider and promote this solution.

Alternatively, the EDPB and/or national supervisory authorities may encourage the use of icons by determining that the (non-)usage of a specific icons set could positively or negatively be considered when determining a fine. According to Article 83(2)(k) GDPR, the supervisory authority, '[w]hen deciding whether to impose an administrative fine and deciding on the amount of the administrative fine' shall give due regard to 'any other aggravating or mitigating factor applicable to the circumstances of the case'. This would allow supervisory authorities to take into account the (non-)usage of icons by the data controller when determining a fine. Such practice, in order to be proportionate and in accordance with higher-ranking law, would have to be determined and predictable ex ante.[118] This could be achieved in cooperation with the EDPB, which has the power to 'draw up guidelines for supervisory authorities concerning (...) the setting of administrative fines pursuant to Article 83' (Article 70(1)(k) GDPR). Alternatively, supervisory authorities could individually launch lighthouse projects, promoting a specific icons set and its consideration in the fine setting process, hopefully leading to a widespread use of the icons across Europe.

VII. Conclusion

The development of privacy icons for improving privacy decisions is premised on the importance of consent as a key instrument within data protection law that enables the exercise of self-determined choices. If personal autonomy as an underlying normative value is to be taken seriously also within the realm of data protection law, the institution of consent should be preserved and ameliorated. Reports on the 'death' of consent (or rather, of its hopeless systemic and operational failure) are greatly exaggerated.[119] Critics tend to overstate the deficiencies and overlook possible ways to improve the instrument of consent in data protection law.

Before we entirely surrender decisions about the use of personal data to regulators, administrative authorities and courts, it is advisable to invest more efforts in improving self-determined privacy choices. This article attempts to take one step in this direction by sketching a risk-based approach to the development and implementation of privacy icons as a partial answer to the practical challenges the institution of informed consent must face. The next steps of the project include, inter alia, the development of a comprehensive risk catalogue, conducting empirical research on the effect of visualisation on information asymmetry and on its capacity to elicit a behavioural change, and ultimately, developing an icons set for further testing and discussion.

[115] *See* Aza Raskin et al, 'Privacy Icons' <https://wiki.mozilla.org/Privacy_Icons>.

[116] As direct regulation is more transparent, this should be the favoured solution, *see* Lawrence Lessig, *Code: Version 2.0* (2nd edn, Basic Books 2006) 132-134.

[117] *See* s IV.4.

[118] For more discussion about the GDPR's sanction system, and especially, the determination of the fine's height, *see* Bergt, 'Art. 83 DS-GVO' in Kühling, Buchner (eds), *Datenschutz-Grundverordnung BDSG: Kommentar* (2nd edn, CH Beck 2018) 1-3, 50-52.

[119] *cf* Winfried Veil, 'The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law' (SSRN, 2018) 10/2018 Neue Zeitschrift für Verwaltungsrecht 686-696 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305056> (criticising 'the utopia of informational self-determination [and] the ineligibility of the legal instrument of consent.').