What's in an Icon? Promises and Pitfalls of Data Protection Iconography

Authors:
Arianna Rossi
SnT, University of Luxembourg*
arianna.rossi@uni.lu

Monica Palmirani
CIRSFID, Università di Bologna
monica.palmirani@unibo.it

Abstract
Under the General Data Protection Regulation (GDPR), transparency of information becomes an obligation aimed at creating an ecosystem where data subjects understand and control what happens to their personal data. The definition of transparency stresses its user-centric nature, while design considerations to comply with this obligation assume central importance. This article focuses on the icons established by the GDPR Art. 12.7 to offer "a meaningful overview of the intended processing". Existing attempts to represent data protection through icons have not met widespread adoption and reasons about the strengths and weaknesses of their creation and evaluation are here discussed. Building on this analysis, we present an empirical research proposing a new icon set that responds to GDPR requirements. The article also discusses the challenges of creating and evaluating such icon set and provides some future directions of research for effective an effective implementation and standardization.

1. Introduction

Information duties are a cornerstone of European data protection law[1] and are commonly realized through the regulatory tool of mandated disclosures: privacy terms inform the data subjects about how data controllers will use and protect their personal information and about their rights. The underlying rationale postulates that the establishment of full transparency facilitates individuals with the decision about the permissible use of their personal data.[2]

Notwithstanding the historical, philosophical, legal, and economic reasons supporting mandated disclosure, research[3] and anecdotal evidence show that privacy policies are ineffective at informing

* The author performed this work while at CIRSFID, University of Bologna and ICR, University of Luxembourg.

[1] For an historical evolution of the information paradigm and the reasons behind its origins in the 1960s, *see generally* Gloria González Fulster, "How uninformed is the average data subject? A quest for benchmarks in EU personal data protection," *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política 19* (2014): 92-104; Alessandro Mantelero, "The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics," *Computer Law & Security Review 30*, no. 6 (2014): 643-660. For an historical background on the regulatory tool of consent and its critical analysis, *see generally* Eoin Carolan, "The continuing problems with online consent under the EU's emerging data protection principles," *Computer Law & Security Review 32*, no. 3 (2016): 462-473.

[2] The provision of information is considered the bedrock for the data subject to make the choice either to engage or disengage with a service *see* Helen Nissenbaum, "A contextual approach to privacy online," *Daedalus 140, no. 4* (2011): 34.

[3] *See generally* George R. Milne and Mary J. Culnan, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," Journal of interactive marketing 18, no. 3 (2004): 15-29; Wainer Lusoli et al., "Pan-European survey of practices, attitudes and policy preferences as regards personal identity data management," (2012); 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," *Information, Communication & Society* (2018): 1-20.

individuals.[4] "Most individuals simply do not read the [privacy] terms, and even if they did, most individuals have difficulty fully comprehending what they actually agreed to and the risk they inherited by that consent".[5] It is frequently assumed that individuals do not care about their privacy[6] and they take the conscious decision of ignoring the legal terms at their own risk.[7] Yet, self-reported data indicate the opposite: they wish to be informed, but concrete obstacles hamper them.[8] Moreover, individuals are not able to base their decisions on full information disclosures, and this effect grows stronger the less the information is understandable and the less the individuals are experienced in the domain.[9]

There are reasons of two orders behind non-readership: some generally concern the characteristics of human reasoning and decision-making,[10] while others are external and pertain to the quality of privacy policies. In this article, only the latter are addressed, by adopting an interdisciplinary perspective that crosses legal information design, semiotics, usable privacy research, user research and legal informatics. The rest of the paper describes the motivation and the development of a research project that led to the creation of DaPIS, an ontology-based icon set representing core notions of data protection and aimed at enhancing the transparency of the information on data processing provided to individuals, as established by the General Data Protection Regulation.[11] The main research questions motivating the DaPIS project have been:
RQ1: What are the reasons why data subjects disregard the legally binding terms describing how their personal data will be processed?
RQ2: What are the requirements introduced by the GDPR's transparency obligations, especially for what concerns nonverbal communication?
RQ3: Which existing technologies can be used to create machine-readable visual structure and visualizations of legal documents?
RQ4: What idiosyncratic features have icons with respect to other kinds of graphical means and how do they impact ease of interpretation?
RQ5: What is the function and context of use of data protection icons?

---

[4] "While transparency has been emphasized as an important practice for decades, existing privacy notices often fail to help users make informed choices. They can be lengthy or overly complex, discouraging users from reading them" *see* Florian Schaub et al., "A design space for effective privacy notices," *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (2015): 1. *See also* Neil Robinson et al., "Review of the European data protection directive," Rand Europe (2009): 28-33.
[5] Woodrow Hartzog, "Website design as contract," *Am. UL Rev. 60* (2010): 1651-1652.
[6] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018), 47.
[7] For a through critical discussion on this assumption, *see* Robert H. Sloan and Richard Warner, "Beyond notice and choice: Privacy, norms, and consent," *J. High Tech. L. 14* (2014): 16-21. Not reading can also be the outcome of a rational decision, *see* note 18.
[8] *See* European Commission, *Special Eurobarometer 487a*, *The General Data Protection Regulation Report,* http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222 (Last accessed: June 21, 2019): 51-55; European Commission, *Flash Eurobarometer 443, e-Privacy Report*, https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy, 2016 (Last accessed July 2, 2018): 2-4; European Commission. *Special Eurobarometer 431, Data Protection Report*, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf, 2015 (Last accessed July 2, 2018): 18-19.
[9] Andreas Oehler and Stefan Wendt. "Good consumer information: The Information Paradigm at its (dead) end?" *Journal of Consumer Policy* 40, no. 2 (2017):182.
[10] Research from behavioral science has exposed many hurdles in privacy and security decision-making. *See generally* Alessandro Acquisti et al., "Nudges for privacy and security: understanding and assisting users' choices online," *ACM Computing Surveys (CSUR) 50*, no. 3 (2017): 44.
[11] European Parliament and Council of European Union, 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 (General Data Protection Regulation), O.J. L 119, 4.5.2016, p. 1—88, 2016. Hereafter: GDPR.

This article is organized as follows: section 2 provides a brief literature review about the documented problems that prevent privacy policies from being useful informative instruments for the data subject. Section 3 illustrates the novel requirements about the quality of information introduced by the GDPR, meant to implement transparency in a way that can respond to the above limitations. The thematic focus of this article lies on the machine-readable icons envisioned in Article 12.7 GDPR and, hence, the following sections tie together two strands of literature. Section 4 provides a short overview of the technologies and standards currently used for the management and (semi-)automated extraction of information from legal documents, whilst section 5 introduces iconographical considerations, with a focus on the legal domain, and describes past attempts to create icons for the data protection domain. Section 6 relies on both lines of research to present the rationale, the design process and the outcomes of an interdisciplinary project that culminated in the creation of DaPIS. Finally, section 7 details possible future directions of research, while section 8 takes stock of the lessons learned during the research described in the next pages.

2. Limitations of Privacy Policies: a Brief Literature Review

Privacy policies have long been criticized for a series of reasons[12] and have been defined as "that dense, unreadable, boilerplate text tucked away in some corner of practically every website and application on the Internet".[13] The communication about data practices is mainly drafted by lawyers for lawyers[14] and merely aims to fulfil the legal requirement of mandated disclosure.[15] This reality sharply contrasts with their stated objective, i.e. effectively inform data subjects about the collection and processing of their personal data and empower them to exercise their rights.[16] Studies show that privacy policies go beyond the understanding of the average internet user,[17] while their extreme length[18] causes information overload[19] and discourages reading.[20] Besides, privacy terms are

[12] *See* Arianna Rossi et al., "When Design Met Law: Design Patterns for Information Transparency." *Droit de la consommation* 122 (2019): 91-97.
[13] Hartzog, *Privacy's Blueprint*, 64.
[14] ``Privacy policies are written by lawyers, for lawyers, and appear to serve little useful purpose for the data subject due to their length, complexity and extensive use of legal terminology" Robinson, et al, *Review European DPD,* 29*;* Helena Haapio et al., "Legal Design Patterns for Privacy," In Erich Schweighofer et al. (Eds.), *Data Protection / LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS 2018* (Editions Weblaw, Bern 2018): 446 (ISBN 978-3-906940-21-2).
[15] Most privacy policies have the unique goal to discharge from liability the service provider. *See* Hartzog, *Website Design,* 1640-1641.
[16] In general, legal communication tends to focus on the essence and precision of the rules, but it is not aimed at responding to the needs of the people that are principally impacted by the text, i.e. mostly non-lawyers. *See* Haapio *et al*., *Legal Design Patterns,* 446. Within this view, privacy notices can be effective accountability mechanisms for companies and necessary auditing instruments for supervisory authorities and advocates, but "they are just not very good at notifying users." Hartzog, *Privacy's Blueprint*, 70. Robinson et al., *Review European DPD*, 29.
[17] *See generally* Carlos Jensen and Colin Potts, "Privacy policies as decision-making tools: an evaluation of online privacy notices," *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (ACM, 2004); Robert W. Proctor, M. Athar Ali, and Kim-Phuong L. Vu, "Examining usability of web privacy policies," *Intl. Journal of Human–Computer Interaction* 24, no. 3 (2008): 307-328; Benjamin Fabian, Tatiana Ermakova, and Tino Lentz, "Large-scale readability analysis of privacy policies," In *Proceedings of the International Conference on Web Intelligence* (ACM, 2017): 18-25; Obar and Oeldorf-Hirsch, *The biggest lie*.
[18] Estimations of privacy policies' reading time are provided in Obar and Oeldorf-Hirsch, *Biggest Lie,* 12; Fabian, Ermakova, and Lentz, *Large-scale Readability,* 21-22; Aleecia M. McDonald and Lorrie Faith Cranor, "The cost of reading privacy policies," *ISJLP* 4 (2008): 543.
[19] Too much information overwhelms users, which in turn do not react reasonably, but "skim, freeze or pick out information arbitrarily" Ryan Calo, "Against notice skepticism in privacy (and elsewhere)," *Notre Dame L. Rev.* 87 (2011): 15. This evidence suggests that the information duties' basic assumption, i.e. providing more information rebalances information asymmetries, is flawed. Oehler, *Good Consumer Information,* 179.
[20] Obar and Oeldorf-Hirsch, *Biggest Lie,* 18. Individuals carry out a cost-benefit analysis that considers time and effort required for reading and understanding. Frederik Zuiderveen Borgesius, "Consent to Behavioural Targeting in European

frequently expressed in vague language,[21] leaving individuals puzzled about their intended meaning.[22]

Whereas attempts to simplify unnecessary language complexity are gaining acceptance and support,[23] whether legal information is displayed intelligibly is too often disregarded:[24] privacy notices are often presented as a visually undifferentiated "wall of text"[25] that is "impenetrable"[26] to the human eye. The absence of any information structure[27] in the text hinders comprehension and weakens intellectual performance.[28] Indeed, people do not read privacy policies word by word, but rather skim their text to find relevant information in order to answer their doubts or to compare two services' practices.[29] Therefore, the presence of structural elements can guide readers towards the most relevant parts of the document (i.e. attention hierarchy).

Another critical dimension for disclosures to be used as decision-making tools is timing. Many legislations, as the GDPR, require data controllers to disclose information at the moment of collection of data (Art. 13). However, if users are engaged in a different activity, the notice is experienced as a nuisance[30] rather than as a useful privacy tool, thus causing individuals to deliberately ignore it.[31]

3. The end or a new era for mandated disclosures?

Given that privacy policies are rarely read and poorly understood, while consent is rarely genuinely informed, the tool of mandated disclosure has attracted fierce criticism. Some scholars have reached the conclusion that information paradigm as regulatory tool has failed[32] and must therefore be abandoned. Solutions that enhance transparency are criticized because language simplification or similar interventions alone cannot solve the non-reading problem.[33]

Law-What are the Policy Implications of Insights from Behavioural Economics?," *Amsterdam Law School Legal Studies Research Paper; No. 2013-43* (Amsterdam: University of Amsterdam, IViR. 2013): 31-34. DOI: 10.2139/ssrn.2300969.

[21] E.g. "We *may* collect information about you"; "we disclose *certain* personal data with third parties." *See generally* Irene Pollach, "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent," *Journal of Business Ethics* 62, no. 3 (2005); Joel R. Reidenberg et al., "Ambiguity in privacy policies and the impact of regulation," *The Journal of Legal Studies* 45, no. S2 (2016): S163-S190.

[22] Jaspreet Bhatia et al., "A theory of vagueness and privacy risk perception," In *Requirements Engineering Conference (RE), 2016 IEEE 24th International*, IEEE (2016): 26.

[23] *See generally* Michele M. Asprey, *Plain language for lawyers* (Federation Press, 2003); Peter Butt, "Legalese versus plain language," *Amicus Curiae* 2001, no. 35 (2012): 28-32.

[24] In late 2017, only a minority of the most trafficked sites on the web displayed visual structure. Haapio et al., *Legal Design Patterns Privacy*, 449.

[25] Stefania Passera, "Beyond the wall of text: How information design can make contracts user-friendly," *International Conference of Design, User Experience, and Usability* (Springer Cham, 2015): 342.

[26] European Data Protection Supervisor, *Opinion 4/2015 Towards a New Digital Ethics*, (2015): 4.

[27] I.e. information hierarchy and meaningful visual organization, e.g. divide the document in digestible paragraphs, organize the content in the relevant sections, provide informative headings and differentiate font bolds. *See* Arianna Rossi et al., "Legal Design Patterns: Towards a New Language for Legal Information Design," *Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019* (Bern Weblaw, 2019): 517-526; Arianna Rossi et al., *When Design Met Law*: 93.

[28] Passera, *Beyond Wall of Text*, 343.

[29] *See generally* McDonald and Faith Cranor, *Cost of Reading*; Robert W. Reeder et al., "A user study of the expandable grid applied to P3P privacy policy visualization," *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, (ACM, 2008): 45-54.

[30] "[N]othing more than an unwanted impediment to the real purposes of going online" *see* Obar and Oeldorf-Hirsch, *Biggest Lie,* 22.

[31] The cookie consent is the most striking example of this nuisance.

[32] "[T]here is considerable agreement that transparency-and-choice has failed" Nissenbaum, *Contextual Approach*, 34.

[33] *See generally* Omri Ben-Shahar and Carl E. Schneider. *More than you wanted to know: The Failure of Mandated Disclosure* (Princeton University Press, 2014).

Nevertheless, two main arguments can be proposed against the abandon of privacy disclosures. Firstly, still two thirds of all legislation are based on the information paradigm.[34] The GDPR is no exception. Secondly, the quality of disclosures shows extensive room for improvement. Encouraging results from a growing body of literature on good legal information design[35] and research on usable privacy[36] both from Europe and US[37] suggest that it is worth attempting to change the *status quo* for the better.

Opportunely, under the GDPR, a revolutionary shift has occurred: the quality, accessibility, and comprehensibility of the information describing data practices [38] assume an unprecedented importance to demonstrate compliance.[39] Although plain and clear language has been advocated for years,[40] it is only with the GDPR that this requirement becomes prominent.[41] The specificity of the intended audience and the characteristics of human cognition shall be taken into account to provide effective disclosures: "[t]he concept of transparency in the GDPR is user-centric rather than legalistic"[42] specifies the Article 29 Data Protection Working Party.[43] Communications cannot be addressed to abstract data subjects, but should rather be tailored to specific users in specific contexts.[44]

The unprecedented acknowledgement in the law of the potential of visualizations[45] to achieve transparency of information must be understood within this novel attention to user-centered

---

[34] Oehler, *Good Consumer Information,* 181.

[35] *See generally* Haapio and Passera, *Contracts as Interfaces*; Stefania Passera, *Beyond the Wall of Contract Text. Visualizing Contracts to foster Understanding and Collaboration within and across organizations* (Aalto University, 2017)*;* Passera, *Beyond Wall of Text*; Stefania Passera and Helena Haapio. "Transforming contracts from legal rules to user-centered communication tools: A human-information interaction challenge." *Communication Design Quarterly Review* 1, no. 3 (2013): 38-45; Robert Waller et al., "Cooperation through clarity: Designing simplified contracts," *Journal of Strategic Contracting and Negotiation* 2, no. 1-2 (2016): 48-68.

[36] *See generally* Joshua Gluck et al., "How short is too short? Implications of length and framing on the effectiveness of privacy notices," *12th Symposium on Usable Privacy and Security (SOUPS)*, (2016): 321-340; Norman Sadeh et al., *The usable privacy policy project*, Technical Report, CMU-ISR-13-119 (Carnegie Mellon University, 2013); Schaub, et al. *Design Space.*

[37] Despite obvious discrepancies, both in the American and European contexts mandated disclosures are recognized as central policy tool. The importance of the understandability of information provided to users is underlined in both legislations (for the US see e.g. the California Consumer Privacy Act), while even the critiques to privacy notices and the proposed solutions are similarly expressed on both sides of the Atlantic. This is why analogies between the two models can be drawn: best practices for good legal information design can be universally applied since they resonate with the capacity of processing information of all human beings, rather than being tied to a specific legal framework.

[38] Article 12 overtly specifies that the information to data subjects must be disclosed in a "concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child." European Parliament and Council, *GDPR*.

[39] *See generally* Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679, 17/EN WP260 rev. 01* (2018). *http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2010/0609/COM_COM(2010)0609_EN.pdf (*Last accessed October 1, 2018): 5.

[40] Article 29 Data Protection Working Party, *Opinion 10/2004 on More Harmonised Information Provision*, 2004, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en.pdf (Last accessed October 1, 2018): 6.

[41] "Compared to the DPD, the GDPR now includes rules on how the information must be presented to data subjects and not only which information should be presented" Christopher F. Mondschein, "Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12 (1) and (7) GDPR." *Eur. Data Prot. L. Rev.* 2 (2016): 509.

[42] WP29, *Guidelines Transparency,* 5.

[43] Hereafter: WP29.

[44] For instance, a teenager uploading pictures on Instagram supposedly has different cognitive needs and past experiences than an adult opening a bank account.

[45] "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used" European Parliament and Council, *GDPR*, Recital 58. "Importantly, the principle of transparency

communication. In order to reduce excessive amounts of written information,[46] Article 12.7 of the GDPR provides for the presentation of information in combination with machine-readable, standardised icons to give "in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing". Namely, the icons should be easily noticeable (i.e. visible), comprehensible (i.e. intelligible), and composed by recognizable elements (i.e. legible). Yet, it is harder to exactly define what "a meaningful overview" might mean and translate it into concrete design requirements, while also the standardization process raises open questions. This paper attempts to provide some preliminary answers to such doubts. Although eventually it will be the role of the European Commission to give directions on the creation of the icons, the need of expert advice is emphasized both in the GDPR[47] and by the WP29 which encouraged an "evidence-based approach" and "extensive research"[48] to inform the development and application of the icons and determine their efficacy.[49]

The research described in the following intends to contribute to establishing the foundations for further research in the domain. The GDPR's incentive to machine-readable icons identifies two parallel and intertwined lines of research: the first direction is related to the technologies for the management and (semi-)automated extraction of legal information (see section 4), whilst the second is linked to legal visualizations and the user-centric design of legal information (see section 5). Whereas the latter eases humans' understanding, the former ameliorates machines' accessibility to legal information.[50] The final aim is the transformation of legal documents into both human- and machine-understandable formats.[51]

4. Machine-interpretable legal information

Although machine-readable does not figure among the definitions in the GDPR, it can be explained as "a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure".[52] It is from this definition and the extensive research area on semantic web technologies for the legal domain that the project presented in these pages has originated- Legal documents, indeed, can be enriched with

in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate" WP29, *Guidelines Transparency,* 25. The use of visual elements to enhance the comprehensibility of the law is gaining acceptance, since adequate knowledge visualization can support learning, reasoning and memorization, and fight information overload. S*ee generally e.g.* M. Hagan, *Law by Design,* http://www.lawbydesign.co; Gerlinde Berger-Walliser, Thomas D. Barton, and Helena Haapio, "From visualization to legal design: A collaborative and creative process." *American Business Law Journal* 54, no. 2 (2017): 347-392; Volker Boehme-Neßler, *Pictorial law: modern law and the power of pictures* (Springer Science & Business Media, 2010); C. R. Brunschwig, *Visualisierung von Rechtsnormen—Legal Design [Visualization of Legal Norms],* PhD diss., Doctoral Thesis (Zürcher Studien zur Rechtsgeschichte, 2001); Haapio and Passera, *Contracts as Interfaces*.

[46] WP29, *Guidelines Transparency*, 25.

[47] "In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. 2.In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. 3.It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level." European Parliament and Council, *GDPR*, Recital 166.

[48] WP29, *Guidelines Transparency*, 26.

[49] In general, empirical research ("user testing" WP29, *Guidelines Transparency,* 14) must demonstrate the intelligibility and effectiveness of a specific privacy notice.

[50] Helena Haapio, Daniela Plewe, and Robert deRooy. "Contract Continuum: From Text to Images, Comics, and Code," *Trend and Communities of Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium IRIS 2017* (2017): 4.

[51] *See generally* Thomas D. Barton et al., "Successful Contracts: Integrating Design and Technology," in *Legal tech, Smart contracts and Blockchain*, Edited by Corrales M., Fenwick M., Haapio H. (Eds) (Springer, 2019).

[52] Recital 21 of Directive 2013/37/EU17

machine-readable specifications that enable semantic reasoners to extract meaning from the text and apply inference rules:[53] XML[54] mark-up is used to embed meta-textual information into the legal document, complemented by languages (like OWL)[55] that define conceptual structures pertaining to a certain domain knowledge. Hence, the concepts of a specific domain (for example EU data protection law) can be formally codified in an ontology,[56] which can assign machine-readable semantic meaning to the legal terms of a certain document.

With such architecture, it is therefore possible to operate concept mining on large quantities of privacy policies and to embed the machine-readable specifications into the legal terms during or after the drafting. The XML encoding allows for a structured, semantically-enriched layout: ideally, each section of a privacy policy provides details about a certain topic (e.g. purposes of data processing, place of storage of data, etc.). Such information can be leveraged to improve the document architecture, i.e. structure it through elements that convey hierarchy of information and thereby ameliorate the ease of reading. Besides, the machine-readable specifications can be leveraged to adapt the display of information to the reader on multiple layers and thereby accommodate the informative needs of different audiences. For instance, whereas supervisory authorities need access to the entire notice, data subjects might find more meaningful to only be shown the first layer of a layered notice.[57]

The project illustrated in the following sections is based on the idea that the concepts that are formally represented in the ontology can be linked to their linguistic realization in the privacy notice and to their corresponding icons, thus creating a network of machine-readable and visual representations[58] (see Figure 1). This does only have the function of fulfilling the GDPR requirement of machine-readable icons, but also allows for the semi-automatic retrieval and display of the visualizations encoded in the ontology, once that the semantic expressions in natural language of the text have been associated to their corresponding ontological representations through the XML mark-up. Thus, semantically-enriched privacy policies can be leveraged to generate a user-friendly visual layer composed of structured layout and iconographical elements that can ease the navigation, comprehension and comparability of these documents.[59]

---

[53] Such heterogeneous information contained in legal documents can be formally represented through a multi-layered architecture: (1) the textual layer provides the representation of the document's original content; (2) the structural layer provides a hierarchical organization of the text; (3) the metadata layer connects document's information with external ontological resources; (4) the ontological layer is the formal model of the concepts mentioned in the document; (5) the logical layer provides the legal interpretation and modelling of the legal meaning of the text, and the transformation of the norms into legal rules to allow legal reasoning. *See* Monica Palmirani and Fabio Vitali, "Akoma-Ntoso for legal documents," *Legislative XML for the semantic Web* (Springer, Dordrecht, 2011): 78-79.

[54] Akoma Ntoso (http://www.akomantoso.org) has been adopted by OASIS (https://www.oasis-open.org) as legal open XML standard for legislative, judiciary and legal documents.

[55] The W3C Web Ontology Language (OWL) is a computational logic-based language that can represent rich and complex knowledge in documents that are known as ontologies. OWL is part of the W3C's Semantic Web technology stack (https://www.w3.org/OWL/).

[56] A classical definition in artificial intelligence research characterizes ontologies as an explicit, formal specification of a shared conceptualization. Thomas R. Gruber, "A translation approach to portable ontology specifications," *Knowledge acquisition* 5, no. 2 (1993): 199-220. In the Semantic Web, ontologies are massively adopted in the Semantic Web to support the uniform description, retrieval and sharing of legal knowledge through the definition of legal concepts and their linguistic realization.

[57] The first layer should ``include the details of the purposes of processing, the identity of controller and a description of the data subject's rights [... It] should also contain information on the processing which has the most impact on the data subject and processing which could surprise them." *See* WP29, *Guidelines Transparency,* 18. The display of the first layer might be helpful especially in those occasions when the user is carrying out a task (e.g. a ticket purchase) and the reading of the privacy terms would be regarded as a nuisance.

[58] The idea is further explored in Arianna Rossi and Monica Palmirani, "DaPIS: an Ontology-Based Data Protection Icon Set," In G. Peruginelli and S. Faro (Eds.), *Knowledge of the Law in the Big Data Age. Frontiers in Artificial Intelligence and Applications* no. 317 (IOS Press, 2019).

[59] *See* section 2.

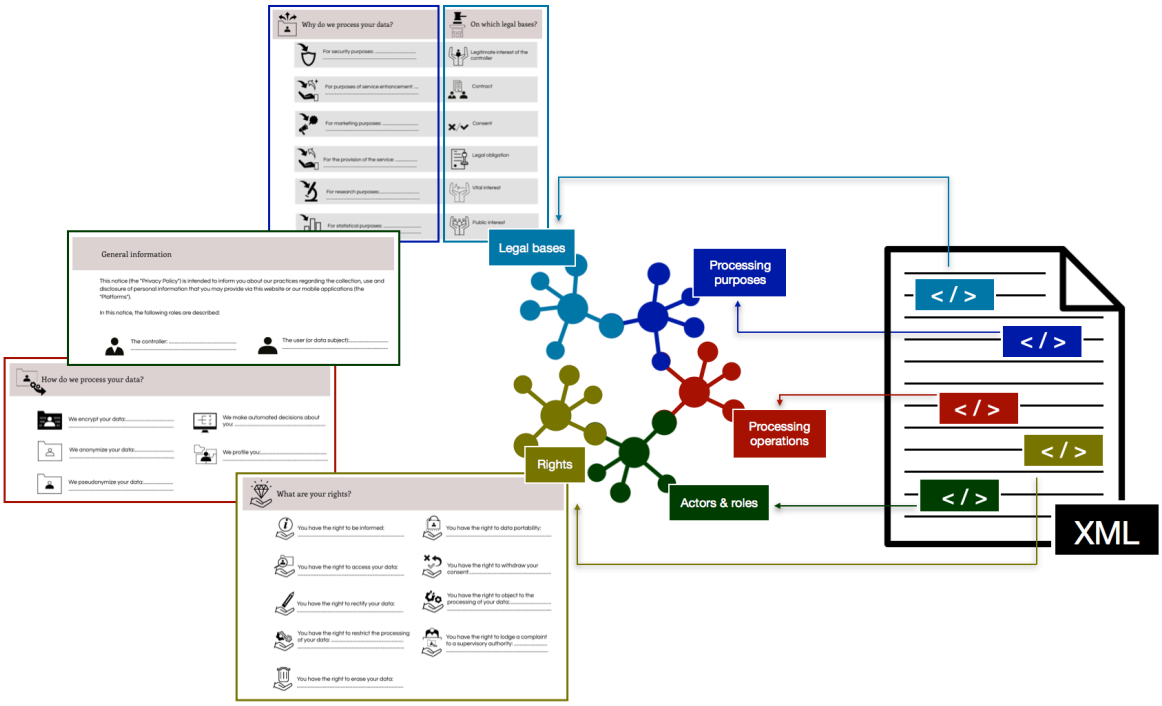


Figure 1: From the right, the XML tags linked to the different conceptual modules of the ontology and the corresponding sections of a visualized privacy policy

The data protection icon set that will be described in the next section was modelled on a selection of conceptual modules formalized in PrOnto[60] (Privacy Ontology). The icon set visualizes fundamental aspects of data processing regulated by the GDPR (especially those information items mandated by Articles 13-14): data (e.g. personal data, sensitive data) and documents (e.g. consent, privacy policy), agents and roles (e.g. data subject, data controller, supervisory authority), data processing workflow (e.g. anonymize, encrypt, transfer), processing purposes (e.g. scientific purposes, marketing purposes), legal bases (e.g. legal obligation, consent, legitimate interest), and data subjects' rights (e.g. right to access, right to erasure).[61]

5. On the Nature of (Data Protection) Icons

Once that a set of concepts was identified through the analysis of the legal requirements and the formal conceptualization described in the previous sections, principles drawn from ergonomics, semiotics and Legal Design[62] provided the methodological framework for the creation and evaluation of DaPIS (Data Protection Icon Set). The following paragraphs will introduce a few necessary

[60] For a thorough description of the ontology, its goals and the methodology to build it, *see generally* Monica Palmirani et al., "PrOnto: Privacy Ontology for Legal Reasoning," *International Conference on Electronic Government and the Information Systems Perspective* (Springer, Cham, 2018): 139-152; Monica Palmirani et al. "Legal Ontology for Modelling GDPR Concepts and Norms." *Legal Knowledge and Information Systems: JURIX 2018: The Thirty-first Annual Conference*. Vol. 313. IOS Press, 2018.

[61] *See* Rossi and Palmirani, *DaPIS*.

[62] Legal Design is an interdisciplinary research defined as "the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying" *see* M. Hagan, *Law by Design,* http://www.lawbydesign.co, Chapter 1. On the application of design methods to the legal domain, *see generally* Berger-Walliser et al, *From visualization*; Brunschwig, *Visualisierung*. A "Legal Design Manifesto" describing approaches, goals and methods of legal design has been recently published (https://www.legaldesignalliance.org/). *See also generally* Amanda Perry-Kessaris, "Legal Design for Practice, Activism, Policy and Research," *46:2 Journal of Law and Society* (Forthcoming). Available at SSRN: https://ssrn.com/abstract=3295671 or http://dx.doi.org/10.2139/ssrn.3295671 .

considerations on iconography, illustrate previous attempts to build an iconic language for the data protection domain and propose a function for the icons envisioned in Article 12.7. Such observations have been instrumental for the creation of DaPIS.

5.1. Semiotics and Iconography

Icons are attractive nonverbal means of communication because they can be easily recognized, processed and memorized and can serve as cognitive support for the classification of content.[63] Although it is commonly assumed that icons communicate in quickly, concisely, and across linguistic and cultural differences,[64] in fact their interpretability depends on a variety of factors. Familiarity is a crucial dimension for ease of recognition and it comprises both previous experience with the graphical symbol and knowledge of the symbol's underlying concept.[65] Semantic transparency is also a critical factor:[66] icons depicting objects (i.e. resemblance icons) are more easily interpreted than arbitrary icons,[67] whose meaning must be learned rather than deduced.[68] Moreover, the function assigned to a graphical symbol by its designer can be different from the meaning attributed to it in practice, i.e. there can be misalignments between the designers' intentions and the sense-making activity of the user. Complexity, i.e. the amount of icon's details, influences search activity.[69] Finally, when creating a set of icons, attention should be devoted both to the degree of discriminability of one icon from the others of the set and to the coherence across the elements of the set.[70]

5.2. The specificity of icons for legal and data protection matters

Since familiarity is a critical dimension to determine ease of interpretation, it is good practice in icon design to rely on established visual conventions[71]. However, only a few symbols exist for legal matters[72] (most notably the scale and the gavel), while in data protection only a few cybersecurity symbols are well-known (i.e. the shield and the padlock).[73] On the other hand, the widespread use of graphical user interfaces has favoured the creation of common mental references between a number of icons and their function (e.g. a pencil for the edit function, a bin for the cancel function, a user silhouette for the profile page on social medias, etc.).

Lack of familiarity with the icon's underlying legal concept (e.g. encryption) must also be taken into consideration to determine the efficacy of graphical symbols: only less arbitrary icons can be explanatory and reveal unknown meanings. An additional difficulty is posed by the fact that legal concepts are usually abstract in nature, thus difficultly depictable. Such characteristics also challenge

---

[63] Connie Malamed, *Visual language for designers: principles for creating graphics that people understand* (Rockport Publishers, 2009): 119.

[64] Sarah J. Ishwerwood, Siné JP McDougall, and Martin B. Curry, "Icon identification in context: The changing role of icon characteristics with user experience," *Human Factors* 49, no. 3 (2007): 465. For a critical examination of the supposed universality of icons, *see generally* Robert Dewar, "Design and evaluation of public information symbols." *Visual information for everyday use: Design and research perspectives* (1999): 285-303.

[65] Isherwood, *Icon Identification,* 467.

[66] Isherwood, *Icon Identification,* 467.

[67] Malamed, *Visual Language*, 118. For new exposures, ease of identification also depends on the icon's concreteness, which is the extent to which real objects, materials, or people are depicted (*see* Isherwood, *Icon Identification,* 466*)*. This effect diminishes as users gain experience over the icons, though.

[68] Jon Hicks, *The icon handbook* (Five Simple Steps, 2011): 22.

[69] Isherwood, *Icon Identification,* 466.

[70] Dewar, *Design Evaluation,* 49-50.

[71] Hicks, *Icon Handbook*, 95.

[72] The highway code represents the most successful example of an internationally established legal visual language. Yet, the supposed universality of traffic signs derives from constant use, international standardization of the norms, and explicit education of the drivers.

[73] However, these symbols express great variety across applications (e.g. browser types) and no standard exists. *See* Tara Whalen and Kori M. Inkpen, "Gathering evidence: use of visual security cues in web browsers," *Proceedings of Graphics Interface 2005* (Canadian Human-Computer Communications Society, 2005): 143-144.

standard icon evaluation methods,[74] which are mainly suited to determine the comprehensibility of graphical symbols whose referent is known to the interpreter. Differences of comprehension rates among icons also depend on the person that interprets them, i.e. her culture, age, expertise, etc. Finally, researchers underline the importance of the provision of contextual cues that mirror the actual usage situation of the icons (i.e. ecological validity) to support the sense-making process of individuals.[75] From such observations follows that it is far from straightforward to establish universally comprehensible icons.

5.3. Lessons drawn from existing data protection icon sets

Some attempts to design and evaluate icons for privacy and data protection have been made[76] and vary deeply[77] e.g. as whether they represent a legal assessment of a certain data processing practice, or as whether they have undergone any comprehensibility evaluation. The PrimeLife project[78] is notably the most structured attempt to design and evaluate icons for data protection in the European context.

However, most of the icons created during such project were discarded based on the results of two user studies[79] and on founded fears of information overload derived by a too high number of icons. The evaluation importantly highlighted how visual vocabulary depends on culture, therefore calling for intercultural user audiences, while it also suggested that simplification of the elements and uniformity of the design styles are critical. Nevertheless, it is not entirely clear to which extent the context of use of the icons was shown to the participants in order to support their interpretation. Furthermore, it could have been acknowledged that those icons that were less easily recognized (e.g. anonymization, user tracking, etc.) depict less familiar and concrete concepts than the ones that were considered "intuitive and easy to understand"[80] (e.g. medical data, deletion, etc.). Since familiarity

---

[74] *See ISO 9186-1:2014. Graphical symbols - Test methods - Part 1: Method for testing comprehensibility*.

[75] Wolff suggests that without such precautions, low recognition scores would falsely indicate that more design and test work is necessary, *see* Wolff, Jennifer Snow, and Michael S. Wogalter. "Comprehension of pictorial symbols: Effects of context and test method." *Human Factors* 40, no. 2 (1998): 173-186.

[76] *See* (in order of publication) Mary C. Rundle "International personal data protection and digital identity management tools." *The Berkman Center for Internet & Society Research Publication Series* (2006); M. Mehldau, *Iconset for Data-Privacy Declarations v 0.1* (https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf); Joshua Gomez, Travis Pinnick and Ashkan Soltani, *Privacy Coding Methodology (*http://knowprivacy.org/policies_methodology.html) (2009)*;* Renato Iannella, Adam Finden, and Stacked Creations. "Privacy awareness: Icons and expression for social networks." In *Proceedings of the 8th Virtual Goods Workshop and the 6th ODRL Workshop*, 2010: 1-15; Ben Moskowitz and Aza Raskin, Privacy Icons, https://wiki.mozilla.org/Privacy_Icons (2011); Cornelia Graf et al., "Final HCI research report." *Primelife Project Deliverable D* 4 (2011); European Parliament. Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [COM(2012)0011 - C7-0025/2012 - 2012/0011 (COD)]* (2013); TRUSTe, "*TRUSTe and Disconnect Introduce Visual Icons to Help Consumers Understand Privacy Policies*"(http://www.truste.com/blog/2014/06/23/truste-disconnect-introduce-visual-icons-to-help-consumers-understand\-privacy-policies/) (2014); PrivacyTech *"Privacy Icons" https://www.privacytech.fr/privacy-icons/ (*2017); L. Specht und 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).

[77] For a literature review of existing data protection icon sets, *see generally* Arianna Rossi and Monica Palmirani, "A Visualization Approach for Adaptive Consent in the European Data Protection Framework," *Conference for E-Democracy and Open Government (CeDEM)* (IEEE, 2017): 159-170.

[78] *See generally* Graf, *Final HCI.*

[79] *See* Simone Fischer Hübner and Harald Zwingelberg. "UI prototypes: Policy administration and presentation-version 2." (2010): 19-28; Graf, *Final HCI,* 50-60; Leif-Erik Holtz, Katharina Nocun, and Marit Hansen. "Towards displaying privacy information with icons," *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, (Springer, Berlin, Heidelberg, 2010): 338-348.

[80] Leif-Erik Holtz, Harald Zwingelberg, and Marit Hansen, "Privacy policy icons," *Privacy and Identity Management for Life* (Springer, Berlin, Heidelberg, 2011): 283.

with icon and its referent is key, as argued earlier, it cannot be expected that all symbols can be interpreted with the same ease, regardless of these dimensions.

One of the unique attempts to consider, during their conception and design, the context where the icons would appear is represented by the table included in the 2013's Draft report of the LIBE Committee on the Regulation proposal.[81] Such table contains six icons *vis-à-vis* of their verbal explanation. In this case, however, it is the prescriptive character of the specific context (i.e. the table) that limits their possible use (e.g. on small screens), thus constituting a drawback rather than a support for successful implementation. A user study[82] highlighted how the convoluted combination of symbols in the various table columns hindered the comprehension of the icons' meaning. Even such study, however, shows limited ecological validity, because it investigated the icons' meaning in isolation, even though they were explicitly designed to appear next to their textual explanations.

5.4. Context of use and function of the data protection icon set

To orient the design of the icon set, a reflection on the envisaged context of use and the ensuing function of the icons appears therefore crucial. They are meant to appear in combination with text and provide a meaningful overview of the intended processing – but neither the GDPR nor the WP29 have further specified the goal and the context of implementation of the icons. Thus, many questions remain open, starting from defining "meaningful" and translate the definition into functional requirements, especially considering that what is meaningful for a certain user might not be meaningful for another. Besides, it is unclear what function should the icons assume and whether it should be the same in different layers of privacy policies, consent requests, privacy dashboards, etc. – i.e. in all those cases when information about the processing must be presented to the data subject.

Similarly to the Primelife project's final recommendations,[83] we also share the belief that, to reach global acceptance, icons should have a headline function, rather than make a statement about the fairness or riskiness of processing. It can be argued that it would be more meaningful to provide individuals (data subjects and supervisory authorities alike) with an obvious visual summary of the risky or unlawful practices conducted on personal data, in order to support their decision-making, e.g. whether to use a certain service or head elsewhere.[84] However, it can be challenging to determine *a priori* criteria to take a decision about the lawfulness or the riskiness of certain practices outside a specific context.[85] Moreover, the adoption of icons that clearly illustrate whether the data practices of an organization are lawful or not might be opposed by many data controllers, since the GDPR does not impose an obligation upon them. Such solution would appear more realistic if the role of assigning such the icons to the data processing practices of a certain organization was played by a third party, like auditors or consumer associations.

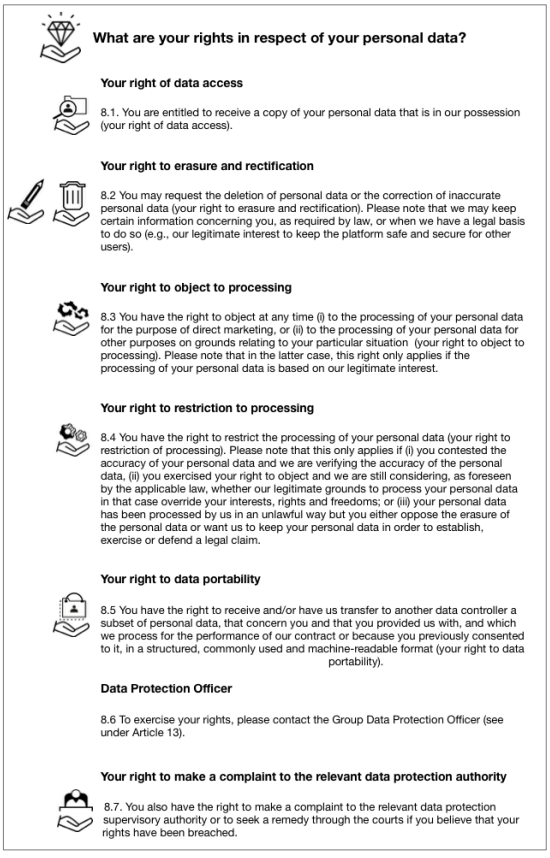
Although such solutions might be promising and investigable in future studies, in the present research graphical symbols do not provide a judgement on the lawfulness or the riskiness of processing practices and leave to the individuals the freedom to evaluate for themselves whether a certain

---

[81] *See* European Parliament, *Draft Report,* Annex 1. The display of such icons would have constituted a legal obligation for websites, were the amendments approved. Trace of this proposition can be found in the GDPR's call for icons.
[82] *See generally* John Sören Pettersson, "A Brief Evaluation of Icons in the First Reading of the European Parliament on COM (2012) 0011," *IFIP International Summer School on Privacy and Identity Management* (Springer, Cham, 2014): pp. 125-135.
[83] Graf, *Final HCI,* 54-55.
[84] This is the approach proposed in Zohar Efroni et al., "Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing" (draft with the author, forthcoming 2019) and by the participatory research lab of Berlin University of the Arts and the Berlin Technical University (*see* https://www.privacy-icons.info/).
[85] But s*ee* Hamza Harkous et al., "Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning," *arXiv preprint arXiv:1802.02561* (2018). In this respect, one viable solution for the EU context would concern the exploration of the levels of risk entailed in DPIAs.

organization's data practices satisfy their privacy expectations. Besides, depicting single concepts, instead of statements about concepts, is the most suitable integration with an ontological formalization of legal knowledge.

For such reasons, DaPIS envisions graphical symbols as "companion icons", i.e. icons that represent the meaning or the function of the text section they accompany.[86] In this view, they act as information markers in documents to support text navigation, information finding and memorization (see Figure 2). The motivations supporting this functional choice lies in the fact that legal icons have limited self-explanatory nature. When they convey abstract meanings, such as data practices, they might not be universally understood if they are not accompanied by some sort of textual explanation.[87] Moreover, this type of visual elements cannot convey subtle and nuanced meanings:[88] they can rather give salience to certain elements that would be otherwise lost in lengthy and undifferentiated texts. This is why, it is wrong to expect that these tiny graphical elements can and will substitute the legal text completely, as it is sometimes feared.[89] But they can accompany the text to enhance the effectiveness of communication by combining verbal and nonverbal elements. In this context, icons help readers to skim, search the document and identify information quickly and efficiently, and even compare it across separate documents. As the icons' use spread in a coherent way across more organizations, they become more and more easily recognizable by individuals.



What are your rights in respect of your personal data?

Your right of data access

8.1. You are entitled to receive a copy of your personal data that is in our possession (your right of data access).

Your right to erasure and rectification

8.2 You may request the deletion of personal data or the correction of inaccurate personal data (your right to erasure and rectification). Please note that we may keep certain information concerning you, as required by law, or when we have a legal basis to do so (e.g., our legitimate interest to keep the platform safe and secure for other users).

Your right to object to processing

8.3 You have the right to object at any time (i) to the processing of your personal data for the purpose of direct marketing, or (ii) to the processing of your personal data for other purposes on grounds relating to your particular situation (your right to object to processing). Please note that in the latter case, this right only applies if the processing of your personal data is based on our legitimate interest.

Your right to restriction to processing

8.4 You have the right to restrict the processing of your personal data (your right to restriction of processing). Please note that this only applies if (i) you contested the accuracy of your personal data and we are verifying the accuracy of the personal data, (ii) you exercised your right to object and we are still considering, as foreseen by the applicable law, whether our legitimate grounds to process your personal data in that case override your interests, rights and freedoms; or (iii) your personal data has been processed by us in an unlawful way but you either oppose the erasure of the personal data or want us to keep your personal data in order to establish, exercise or defend a legal claim.

Your right to data portability

8.5 You have the right to receive and/or have us transfer to another data controller a subset of personal data, that concern you and that you provided us with, and which we process for the performance of our contract or because you previously consented to it, in a structured, commonly used and machine-readable format (your right to data portability).

Data Protection Officer

8.6 To exercise your rights, please contact the Group Data Protection Officer (see under Article 13).

Your right to make a complaint to the relevant data protection authority

8.7. You also have the right to make a complaint to the relevant data protection supervisory authority or to seek a remedy through the courts if you believe that your rights have been breached.

---

[86] *See* the "companion icons" pattern in Haapio and Passera, *Contracts as interfaces*; Rossi et al., *Towards New Language*.
[87] *See generally* Susan Wiedenbeck, "The use of icons and labels in an end user application program: an empirical study of learning and retention," *Behaviour & Information Technology* 18, no. 2 (1999): 68-82.
[88] In the interpretation of the WP29 (*Guidelines Transparency*, 25), the icons are meant to enhance transparency by reducing the extreme amount of information and, upon standardization, to be used across the continent as universal shorthand for that information. However, reducing the complexity and the potentially infinite combinations of linguistic terms into a limited set of icons is impossible and non-functional.
[89] *See* Samson Esayas, Tobias Mahler, and Kevin McGillivray, "Is a Picture Worth a Thousand Terms? Visualising Contract Terms and Data Protection Requirements for Cloud Computing Users," *International Conference on Web Engineering* (Springer, Cham, 2016): 42; Berger-Walliser et al, *From visualization,* 5.

Figure 2: A possible "visual layer" for the Blablacar privacy policy's section about data subjects' rights, with visual structure and companion icons accompanying the different sections. The original text was not changed.

Although the icons are not meant to appear in isolation, it is fundamental to evaluate their ability to convey the correct meaning. This matter has great relevance if individuals take legally-binding decisions based on the visualizations, such as entering into a contract with a service provider or giving consent to certain data practices. Misunderstanding of the icons or oversimplification of privacy terms might cause liability issues.[90] Usability tests on existing data protection icons[91] show that "critical confusions,"[92] namely interpretations opposite to the intended meaning, are possible due to multiple reasons: misalignment between designers' intentions and users' expectations on the icon meaning and differences in individuals' level of education, age, and cultural background. This is why user-centric methods drawn from design principles can be necessarily applied.

5.5. Legal Design

Following its human-centered nature, Legal Design assumes that the "users of the law"[93] are not only legal experts, but also laypeople. Therefore, when useful for its goals, it favours participatory design methods:[94] the design process starts from an analysis of the needs and abilities of the intended users of an artefact (i.e. the icons and the privacy policies) that are involved at every stage of the design, from the conceptual phase till the evaluation. One of legal design research areas focuses on graphic communication tools,[95] but does not aspire to become a prescriptive theory that generates "a single `right' […] image or layout".[96] Rather, it can be conceived as a creative and iterative process that provides indications about the chances of suitable use of a certain element, e.g. a visualization, given information type and goal of the design. Multi-stakeholders' collaborations are encouraged since they leverage on the multiple skills and knowledge of the different stakeholders involved, and this reciprocal understanding reduces the chances of personal bias.[97]

---

[90] *See* Marit Hanse, "Putting Privacy Pictograms into Practice-a European Perspective," *GI Jahrestagung* 154 (2009).
[91] *see generally* Holtz, Nocum and Hansen, *Towards Displaying*; Pettersson, *Brief Evaluation;* Iannella and Finden, *Privacy Awareness.*
[92] Michael S. Wogalter, "Factors influencing the effectiveness of warnings," In *Visual Information for Everyday Use*, (CRC Press, 2014): 102.
[93] See also Section 2.
[94] On participatory design, *see generally* Douglas Schuler and Aki Namioka, *Participatory design: Principles and practices* (CRC Press, 1993). Research has established that people tend to project their own beliefs and assumptions on others. User research, as a collaborative exploration between designer and user, provides a definition of the problem and of the potential areas of intervention, and steers the generation of ideas and solutions. Berger-Walliser et al., *From Visualization,* 13-14.
[95] Berger-Walliser et al., *From Visualization,* 6.
[96] Berger-Walliser et al., *From Visualization,* 22.
[97] *See* Berger-Walliser et al., *From Visualization,* 14. Indeed, previous research has found that it is arduous for experts to think like non-experts and, thus, symbols created by the target audience are more likely to be correctly interpreted by other members of the target audience, since they share similar mental models and cognitive profiles. *See* Patrice Caire et al., "Visual notation design 2.0: Towards user comprehensible requirements engineering notations," *Requirements Engineering Conference (RE), 2013 21st IEEE International* (IEEE, 2013): 115.

6. Design and evaluation of DaPIS

6.1. Methodology for the design of DaPIS

For the creation of DaPIS, a series of design workshops was held in July 2017, March 2018, and July 2018[98] and followed the (legal) design cycle.[99] The risk of misalignments between designers' intentions and the sense-making activity of individuals oriented the research towards participatory design methods for the creation of the icon set. Interdisciplinarity was a critical element: academics and professionals with legal and technical background interpreted, explained, and exemplified the data protection concepts to the other participants; graphic designers and other professionals coming from visual disciplines contributed with techniques and tools to produce functional visualizations for the intended audience and the intended medium; and, lastly, laypeople added non-expert views and knowledge to the design process, for instance about the visual conventions they were familiar with.

The systematic formalization of knowledge described in section 4 provided the conceptual framework for the creation of the visualizations. The existing visual vocabulary for technical, legal and data protection matters (see section 5.2) was re-adapted to a certain extent, but revealed insufficient: for many concepts, new symbols had to be created. The design followed iterative cycles: during each workshop, initial icon prototypes were proposed, discussed and refined in subsequent phases, so that feedback from other participants, but also from externals, was collected at every stage of the design. In this way, the shortcomings and strengths of the proposed ideas were identified before the actual creation of high fidelity icons and chances of failure at later stages (e.g. during the evaluation phase) were minimized.

Not only each workshop followed an iterative cycle, but iterative was also the design cycle overall: whereas the first design workshop explored the best suited visual means to render complex data protection notions, the following workshops focused on more specific aspects related to usability of the graphical symbols, harmonization of the design style of the set, and digital rendering of the prototypes. Furthermore, three user studies,[100] each one following one of these phases, were conducted to determine the comprehensibility and legibility of the icons. Based on the results after each user study, icons were vetted and refined in the following workshop, and further evaluated if necessary.

Given the previous research on graphical symbols, it was not surprising that concepts with a higher degree of concreteness (e.g. "contract"), for which an exemplification could be easily provided (e.g. "research purposes"), or that could rely on established visual convention (e.g. the bin to signify erasure in the "right to erasure" icon) were more quickly and effortlessly visualized by the participants. Conversely, abstract or general concepts such as "rights", "processing purposes", "service enhancement" and "service provision" were object of thoughtful consideration and, even, intense debate. Decisions that appeared arbitrary to some group members had eventually to be taken.

One of the major challenge that repeatedly emerged during the workshops was represented by the tentative of striking a balance among the priorities of the different stakeholders. On the one hand, legal experts warned of the existing risks of oversimplification in the visualization of data protection

[98] The first workshop was organized at the Legal Design Lab, Stanford University (US) in July 2017 and developed the first prototypes of the icon set. Three further workshops were held at CIRSFID, Università di Bologna (IT) in March 2018 with the Accademia di Belle Arti di Bologna. One last workshop was organized at CIRSFID in July 2018 with the Accademia di Belle Arti di Bologna. Further details can be found in Rossi & Palmirani, *DaPIS* and in Arianna Rossi, "Legal Design for the General Data Protection Regulation. A Methodology for the Visualization and Communication of Legal Concepts" PhD thesis, Alma Mater Studiorum Università di Bologna, PhD in Law, Science and Technology 31 Ciclo, Forthcoming.

[99] Hagan, *Law by Design,* "Design Process for Lawyers".

[100] See next section.

concepts. On the other hand, icons containing few details had to be preferred to achieve ease of recognition and allow icons' usability in multiple contexts (i.e. small screens).

Attention to balance among simplicity of representation, distinctiveness of some traits, but also coherency of elements across icons was also among the working guidelines for the participants.[101] For instance, an upward-facing hand was chosen to indicate the class of data subjects' rights. The metaphor underlying the hand represents the concept of being in control of the element located above it. This palm recurs in every data subject's right as common denominator among concepts belonging to the same class, but the meaning of the icon as a whole is specified by the element held by the hand: e.g. a bin for the right to erasure, a pencil for the right to rectification, etc. (see Figure 2).

6.2. Methodology for the evaluation of DaPIS

Evaluation of the icons is crucial, given that the goal is EU standardization. However, as illustrated in Section 5.3, only very few assessments have been carried out on data protection icon sets and even those show their limitations. That said, there is no good standard evaluation method that can be proposed for this specific context without any vetting, since legal icons have the peculiar characteristics explored in section 5.2. In this research, we have proposed an evaluation methodology that follows a two steps approach.[102] Firstly, icons are evaluated as stand-alone elements, i.e. according to classical dimensions such as comprehensibility and legibility. In the second place, a complementary evaluation concerns the extent to which the icons can indicate the desired function in context, i.e. whether they support the navigation through large amounts of information and increase speed and accuracy of comprehension. This article only covers the first phase of evaluation, while recommendations about the second phase will be provided in the last section.

The three user studies conducted on DaPIS were fundamental to confirm or reject the hypotheses formulated during the workshops. For instance, the first user study[103] confirmed that laypeople have low familiarity with many data protection concepts, apart from those that are more commonly known, such as anonymization, marketing, or transfer outside of the EU. On the other hand, this user test also disconfirmed an hypothesis championed by the legal experts: namely, that the more detailed the graphical representation, the easier the icon interpretation. The recognized excessive complexity guided the following icon (re)design towards simplicity and usability goals.

This observation also brought to the adoption of visual metaphors for some concepts. Indeed, the first exploratory workshop produced pictograms representing concepts in a literal manner (e.g. the right to data portability, see Figure 3). However, despite their concreteness and their arguable informational value, the prototypes are not suitable for small dimension screens and were judged too complex during the evaluation phase. On the contrary, a metaphor in which one idea is understood in terms of another is well suited to convey meaning through minimal elements. For these reasons, for instance, a folder in the shape of a suitcase was proposed to more compactly recall the right to data portability (see **Error! Reference source not found.**). Thus, many explanatory details of the first icon were lost but, if icons need to be usable and scalable elements, certain specifications must be left to the written privacy terms that they complement.

---

[101] See additional examples in Rossi & Palmirani, *DaPIS*.

[102] Such approach has been more thoroughly detailed in Rossi, *Legal Design for the GDPR*.

[103] 16 individuals participated in this study, held in Stanford in August 2017. The participants' age was very diverse, while their provenance was more uniform.

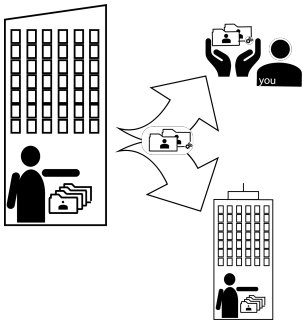


Figure 3a: The first icon prototype for the right to data portability, that literally depicts the concept's definition

Figure 3b: The redesign of the icon through a metaphor

Whereas this first user study was exploratory in nature, the second[104] study focused on classical measures to evaluate graphical symbols. Firstly, the icons' legibility was investigated, defined as the ease of recognition of the elements composing an icon. This dimension determines the ease of recognition of the icon as a whole and is important because, if some elements are not easily visible (e.g. due to their size) or recognizable (e.g. due to the way they are designed), they can hinder the comprehensibility of the icon's meaning. Moreover, low legibility rates can also determine hard distinguishability of an icon from another.

The second evaluation dimension was represented by ease of recognition, which is also considered "the most important single index of a symbol's effectiveness."[105] However, as recalled earlier, standardized evaluation methods[106] that employ quantitative measures such as hit rate (number of correct associations between icon and referent), are ineligible for this context because of the lack of familiarity with the icons' referents and the icons' abstractness. In the user studies described in this article, each icon was presented next to its definition: instead of measuring efficiency of association between concept and icon, the primary focus was placed on the explicit interpretation of the visuals. Users could provide a subjective rate (on a 1 to 5 Likert scale) to express their degree of agreement with the iconographical choice that had been made for a certain concept. The adoption of such a method had three main goals: firstly, find out through the uniformity of rates (or on the contrary through their variation) whether an icons was overall considered a good fit. Secondly, to clarify the difference between poor rates caused by icons' representation or design, and poor rates derived by lack of understanding of the underlying concept. And finally, avoid interpretation strategies based on the exclusion of previous associations, since such methods hide the level of subjective certainty about an association: in the first user study, the icons selected and associated to their meaning first were mostly those that the data subjects could more easily recognize (e.g. copying).

Lastly, it was attempted to establish the alignment between users' and designers' mental models: since the interpretation of a user might not correspond to the intended meaning embedded by a designer in a symbol, the participants were explicitly asked to explain whether they could grasp the rationale behind the iconographical choices made during the design phase. This was meant to find out whether, even if not immediately evident, the meaning of the icons can be divined upon reflection.

---

[104] 16 people participated in this in-person observations and interviews that took place in Bologna, in March 2018. The participants' age span ranged from 20 to 29 years old and the great majority were university students, indicating a high educational background. Three quarters (n=12) of the subjects described themselves as having intermediate digital skills, while half of the participants (n=8) claimed to have basic legal competences.

[105] Dewar, *Design Evaluation,* 292.

[106] *See generally* ISO 9186.2014:1.

To enhance the ecological validity of the testing scenario, during the study, the participants were provided a visualized privacy policy showing the icons' intended context of use and the entire set of icons. Not surprisingly, the icons that scored best (e.g. right to information, right to erasure, security purposes, scientific purposes, etc.) either represent concrete objects or familiar concepts, or are based on widespread representations.[107] Conversely, the concepts behind the icons that scored worst (e.g. purposes of provision of a service, purposes of enhancement of the service, public interest), are vague, general, unknown or abstract. In those cases where the association between icon and referent was deemed more appropriate, a general tendency shows that the users' interpretation more frequently coincided with the reason behind the design choice. These considerations and some pitfalls in legibility caused further vetting of the icons, that were lastly evaluated in a third[108] user study.

6.3. The final DaPIS

According to the results discussed in the previous pages and the subsequent redesign, an icon set composed of 37 elements was created and is illustrated in Annex 1.[109] It can be assumed that many of these elements can be adopted, although there still are few icons that need further research, since the user studies did not conduct to satisfactory results. The user studies described in the last section can be indicative but not conclusive, given the low number of participants and their socio-demographics, which were not representative of the EU population. Yet, the empirical approach described in this article has shed light on many design pitfalls, while participatory design has proved valuable to represent the many stakeholders that will be impacted by the use of the icon set. That said, creating data protection icons that should function as standard for the whole European Union might prove difficult and even impossible, considered that there is no "average user" to design for: European citizens have different levels of (technical and legal) knowledge, expectations and privacy concerns.

7. Future directions of research

Since the main obstacle to ease of recognition is lack of familiarity, it can be expected that the effect of training would increase recognition rates and determine easier recall of the icons. Thus, comprehension tests should be carried out as a longitudinal study spanning over a period of time, rather than as one-time only recognition test.[110] It would also be important to determine the icons' learning ease because it is reasonable to expect that individuals will learn to recognize the icons over time, as any new (visual or verbal) language. The function of DaPIS in context should also be tested,[111] namely in an online, interactive interface where the icons complement the privacy policy and act as navigation cues. In this context, an association task between symbol and referent to assess the icons' comprehensibility would be meaningful if carried out as an information finding task, thus

---

[107] This is also reflected in the users' explanations: such icons were described as "universal, immediate, instantly recognizable, clear, intuitive, unmistakable" because "grounded in our culture, codified and common on application software".

[108] 10 people took part in this last user study. Their age and educational level is comparable to the second study participants. Their origin was, however, more composite and the study was carried out online.

[109] The icon set is available at: http://gdprbydesign.cirsfid.unibo.it/dapis-2/.

[110] A helpful evaluation framework for graphical symbols whose referents are unknown is established by the international standard ISO 9186-3:2014 that introduces two consequent phases of testing: the first part aims to make users develop familiarity with the concepts (i.e. familiarity training), while the second part tests the comprehensibility of the corresponding graphical symbols (i.e. symbol referent association test). S*ee generally* ISO 9186-3:2014. *Graphical symbols - Test methods Part 3: Method for testing symbol referent association.* However, the fitness of this methodology for the present context must be carefully gauged: we have expressed our doubts and proposed alternatives in Rossi, *Legal Design for the GDPR*. Certain is that further research must be devoted to establish a valid evaluation framework for GDPR icons.

[111] I.e. the second phase of the evaluation, as anticipated in Section 5.2.

reproducing a realistic user task. Such a setting would provide higher ecological validity to the study and possibly determine higher icons' recognition rates.

Despite the necessity of increasing familiarity, research must be devoted to the cognitive overload that a numerous icon set might cause, especially at first exposures. In this respect, it would be meaningful to experiment whether the selection of a limited number of icons would be more meaningful than the entire icon language. In one possible scenario, only risky practices or practices that would have a significant impact on the individual would be displayed, e.g. the transfer of data outside of the EU and the existence of automated decision-making. Such selection of icons would thus compose the first layer of a layered approach, where a compact array of icons summarizes the most relevant data practices, provided that the selection is solidly grounded in methodology.

Another dimension that must still be scrutinized is the extent to which each icon is discernible from the others of the set, which is a crucial index for ease of recognition. The icons are part of a set and present common elements, therefore the less they overlap in terms of similarity, the more they will be memorisable. Yet, the more diverse, the more information overload they might cause on the individuals' cognitive capacities. In other words, their design should be sufficiently consistent to identify them as a family of icons, but also sufficiently distinctive to distinguish each element easily from the others. This could be carried out as a hit rate task with multiple answers where all the icons under the same conceptual category (e.g. rights) or having similar meanings (e.g. consent, right to withdraw consent, etc.) are displayed together.

8. Conclusions

The research described in this article is not finished because it has not yet reached conclusive results. Quite the contrary: it is intended to pave the way for further empirically-grounded and methodologically-motivated investigations into the domain of data protection iconography. What seems undoubtable concerns the impossibility to produce an icon set that will be considered perfectly representative of data protection concepts, i.e. perfectly semantically transparent, and will be effortlessly recognized by everybody. User research can give important insights as for what concerns legibility, while alternatives for those symbols that scored worst should be sought. Nevertheless, very high rates of ease of recognition will never be reached for unfamiliar concepts and unfamiliar icons, until their widespread adoption will increase their familiarity. One path to follow might be standardization open to versioning: after one icon set has been publicly discussed and adopted, empirical data on its use in real-world scenarios should be gathered and employed to further vet the set, considering also the needs of evolving societies and regulations. A fundamental step towards this goal is to initiate a multi-stakeholder discussion and collect multiple approaches and results from other researches.[112]

In conclusion, we advance a few general recommendations. Education of data subjects on data protection and privacy-conscious behaviours[113] is necessary to learn the concepts behind the symbols, while icons' standardization and consistent implementation by all relevant stakeholders would reduce the margins for free interpretation. Whereas researchers from many disciplines[114] can offer valuable insight for the further development and evaluation of data protection icons, it must be a goal of the

[112] A first step towards this goal has consisted in the establishment of the "Privacy Icons Forum": https://www.privacyiconsforum.eu/ (last accessed: June 20, 2019).

[113] As other researchers have already noted, see Graf et al., *Final HCI*, 60; Esayas, Mahler and McGillivray, *Is a Picture Worth*, 54.

[114] I.e. law, semiotics, human-computer interaction, design, computer science, cognitive psychology, philosophy, behavioural economics

regulators to find means and resources to carry out data protection education campaigns for European citizens[115] and standardization. Every segment of society[116] from each European country should be possibly included: despite its ambitiousness, it is a necessary step to produce icons that can be safely adopted at the EU level.

Throughout the phases of creation and evaluation of the icons, there was constant opposition between simplicity and preciseness of representation. Whereas the former is a fundamental feature to ensure usability and scalability of the visual elements to any dimension, the latter is important to convey the exact meaning of the corresponding concept. It is challenging to determine the extent to which a visual representation can be simplified and reduced to a few pixels without losing those traits that are necessary to convey its meaning. However, a trade-off must be struck, even if it is an arbitrary choice. Besides, although to a certain extent icons can convey unknown notions to data subjects, focus should be on other typologies of visual means that are more effective to reach this goal: pictograms, comics, infographics are obvious candidates, while animated gifs, videos and timelines can better convey movements and time sequences.[117]

Although they can contribute to implement transparency to a certain extent, it is unrealistic to expect that icons will be the universal language solving all the hurdles posed by traditional privacy policies. The language of these documents is typically vague and complex, while the amount of information provided is usually excessive for data subjects. Empirical research shows that the provision of detailed privacy information while the user is executing a different primary task is only experienced as a nuisance. Nevertheless, interdisciplinary studies can shed light on many overseen aspects of transparency with the aim of providing necessary and sufficient comprehensible information to empower data subjects to have more conscience and control over the flow of their personal data. Creative and original ways of communicating data practices are spreading, although they constitute only a minority,[118] but the GDPR's transparency obligation has provided a considerable incentive to innovation and empirically-based experimentation in this regard.

Acknowledgements

The research described in this paper was supported by the EACEA, financing the Joint International Doctoral Degree in Law, Science and Technology (LAST-JD), and by the Marie Sklodowska-Curie Mining and Reasoning with Legal Texts (MIREL) project. The authors would like to thank all those that have took part to this project in various degrees: Margaret Hagan, Legal Design Lab, Stanford University; Professor Danilo Danisi and his students, Accademia di Belle Arti di Bologna; and Chiara Cavazzuti, Accademia di Belle Arti di Firenze. All the participants to the "Law & Design for Privacy" workshops and to the user studies and the anonymous reviewers are also gratefully acknowledged.

Bibliography

Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon et al. "Nudges for privacy and security: Understanding and assisting users' choices online." *ACM Computing Surveys (CSUR)* 50, no. 3 (2017): 44.

Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679, 17/EN WP260 (2018)*

[115] Indeed, the protection of personal data and privacy is one of the fundamental digital skills of the European Digital Framework for Citizens (DigComp). See Joint Research Center, *DigComp into Action. Get inspired make it happen. A user guide to the European Digital Competence Framework* (2018): 7.

[116] The user studies described in this research had young highly educated participants. However, to produce generalizable results, they should be diverse in terms of age, gender, educational background, profession, technical proficiency, legal knowledge, and privacy awareness.

[117] *See generally* Rossi et al., *Towards New Language*; Rossi et al., *When Design Met Law.*

[118] *See generally* Haapio et al., *Legal Design Patterns.*

Article 29 Data Protection Working Party, *Opinion 10/2004 on More Harmonised Information Provision*, 2004, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en.pdf (Last accessed October 1, 2018)

Asprey, Michele M. *Plain language for lawyers*. Federation Press, 2003.

Barton, Thoma, Helena Haapio, Stefania Passera and James G. Hazard. "Successful Contracts: Integrating Design and Technology" In Legal tech, Smart contracts and Blockchain, Edited by Corrales M., Fenwick M., Haapio H. (Singapore, Springer, 2019).

Ben-Shahar, Omri, and Carl E. Schneider. *More than you wanted to know: The Failure of Mandated Disclosure*. Princeton University Press, 2014.

Berger-Walliser, Gerlinde, Thomas D. Barton, and Helena Haapio. "From visualization to legal design: A collaborative and creative process." *American Business Law Journal* 54, no. 2 (2017): 347-392.

Bhatia, Jaspreet, Travis D. Breaux, Joel R. Reidenberg, and Thomas B. Norton. "A theory of vagueness and privacy risk perception." In *2016 IEEE 24th International Requirements Engineering Conference (RE)*, pp. 26-35. IEEE, 2016.

Boehme-Neßler, Volker. *Pictorial law: modern law and the power of pictures*. Springer Science & Business Media, 2010.

Brunschwig, Colette. *Visualisierung von Rechtsnormen: legal design*. Schulthess, 2001.

Butt, Peter. "Legalese versus plain language." *Amicus Curiae* 2001, no. 35 (2012): 28-32.

Caire, Patrice, Nicolas Genon, Patrick Heymans, and Daniel L. Moody. "Visual notation design 2.0: Towards user comprehensible requirements engineering notations." In *2013 21st IEEE International Requirements Engineering Conference (RE)*, pp. 115-124. IEEE, 2013.

Calo, Ryan. "Against notice skepticism in privacy (and elsewhere)." *Notre Dame L. Rev.* 87 (2011): 1027.

Carolan, Eoin. "The continuing problems with online consent under the EU's emerging data protection principles." *Computer Law & Security Review* 32, no. 3 (2016): 462-473.

Dewar, Robert. "Design and evaluation of public information symbols." *Visual information for everyday use: Design and research perspectives* (1999): 285-303.

Efroni, Zohar et al., "Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing" (draft with the author, forthcoming 2019).

Esayas, Samson, Tobias Mahler, and Kevin McGillivray. "Is a picture worth a thousand terms? Visualising contract terms and data protection requirements for cloud computing users." In *International Conference on Web Engineering*, pp. 39-56. Springer, Cham, 2016.

European Commission, *Special Eurobarometer 487a*, *The General Data Protection Regulation Report,* http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222 (Last accessed: June 21, 2019).

European Commission, *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: a Comprehensive Approach on Personal Data Protection in the European Union. COM(2010) 609 final, 2010;* Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679, 17/EN WP260 rev. 01* (2018). http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2010/0609/COM_COM(2010)0609_EN.pdf (Last accessed October 1, 2018).

European Commission. *Flash Eurobarometer 443, e-Privacy Report*, https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy, 2016 (Accessed July 2, 2018).

European Commission. Special Eurobarometer 431, Data Protection Report, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf, 2015 (Accessed July 2, 2018).

European Data Protection Supervisor, *Opinion 4/2015 Towards a New Digital Ethics*, 2015.

European Parliament and Council of European Union, *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 (General Data Protection Regulation),* O.J. L 119, 4.5.2016, p. 1—88, 2016.

European Parliament. Committee on Civil Liberties, Justice and Home Affairs "*Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing*

of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [COM(2012)0011 - C7-0025/2012 - 2012/0011 (COD)] “, 2013.

European Parliament. Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [COM(2012)0011 - C7-0025/2012 - 2012/0011 (COD)]*, 2013.

Fabian, Benjamin, Tatiana Ermakova, and Tino Lentz. "Large-scale readability analysis of privacy policies." In *Proceedings of the International Conference on Web Intelligence*, pp. 18-25. ACM, 2017.

Fischer-Hübner, S., E. Wästlund, and H. Zwingelberg. "UI prototypes: Policy administration and presentation version 1. Deliverable D4. 3.1 of the EC FP7 project PrimeLife." (2009).

Fuster, Gloria González. "How uninformed is the average data subject? a quest for benchmarks in EU personal data protection." *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política* 19 (2014): 92-104.

Gluck, Joshua, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. "How short is too short? implications of length and framing on the effectiveness of privacy notices." In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pp. 321-340. 2016.

Gomez, Joshua, Travis Pinnick and Ashkan Soltani, *Privacy Coding Methodology (*http://knowprivacy.org/policies_methodology.html), 2009.

Graf, Cornelia, Christina Hochleitner, Peter Wolkerstorfer, Julio Angulo, Simone Fischer-Hübner, and Erik Wästlund. "Final HCI research report." *Primelife Project Deliverable D* 4, 2011.

Gruber, Thomas R. "A translation approach to portable ontology specifications." *Knowledge acquisition* 5, no. 2 (1993): 199-220.

Haapio, Helena, Daniela Plewe, and Robert deRooy. "Contract Continuum: From Text to Images, Comics, and Code." (2017).

Haapio, Helena, Margaret Hagan, Monica Palmirani, and Arianna Rossi. "Legal design patterns for privacy." In *Data Protection/LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS*, pp. 445-450. 2018.

Hagan, Margaret, *Law by Design*, http://www.lawbydesign.co (Last accessed March 19 2019)

Hansen, Marit. "Putting Privacy Pictograms into Practice-a European Perspective." *GI Jahrestagung* 154 (2009): 1-703.

Harkous, Hamza, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. "Polisis: Automated analysis and presentation of privacy policies using deep learning." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 531-548. 2018.

Hartzog, Woodrow. "Website design as contract." *Am. UL Rev.* 60 (2010): 1635.

Hartzog, Woodrow. *Privacy's blueprint: the battle to control the design of new technologies*. Harvard University Press, 2018.

Hicks, Jon. *The icon handbook*. Five Simple Steps, 2011.

Holtz, Leif-Erik, Harald Zwingelberg, and Marit Hansen. "Privacy policy icons." In *Privacy and Identity Management for Life*, pp. 279-285. Springer, Berlin, Heidelberg, 2011.

Holtz, Leif-Erik, Katharina Nocun, and Marit Hansen. "Towards displaying privacy information with icons." In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pp. 338-348. Springer, Berlin, Heidelberg, 2010.

Iannella, Rennato, Adam Finden, and Stacked Creations. "Privacy awareness: Icons and expression for social networks." In *Proceedings of the 8th Virtual Goods Workshop and the 6th ODRL Workshop*, 2010: 1-15.

Isherwood, Sarah J., Siné JP McDougall, and Martin B. Curry. "Icon identification in context: The changing role of icon characteristics with user experience." *Human Factors* 49, no. 3 (2007): 465-476.

ISO 9186-1:2014. *Graphical symbols - Test methods - Part 1: Method for testing comprehensibility*.

ISO 9186-3:2014. *Graphical symbols - Test methods Part 3: Method for testing symbol referent association*

Jensen, Carlos, and Colin Potts. "Privacy policies as decision-making tools: an evaluation of online privacy notices." In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pp. 471-478. ACM, 2004.

Joint Research Center, *DigComp into Action. Get inspired make it happen. A user guide to the European Digital Competence Framework* (2018), 7.

Lusoli, Wainer, Margherita Bacigalupo, Francisco Lupiáñez-Villanueva, Norberto Nuno Gomes de Andrade, Shara Monteleone, and Ioannis Maghiros. "Pan-European survey of practices, attitudes and policy preferences as regards personal identity data management." (2012).

Malamed, Connie. *Visual language for designers: principles for creating graphics that people understand*. Rockport Publishers, 2009.

Mantelero, Alessandro. "The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics." *Computer Law & Security Review* 30, no. 6 (2014): 643-660.

McDonald, Aleecia M., and Lorrie Faith Cranor. "The cost of reading privacy policies." *ISJLP* 4 (2008): 543.

Mehldau, Matthias. *Iconset for Data-Privacy Declarations v 0.1* (https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf).

Milne, George R., and Mary J. Culnan. "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices." *Journal of interactive marketing* 18, no. 3 (2004): 15-29.

Mondschein, Christopher F. "Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12 (1) and (7) GDPR." *Eur. Data Prot. L. Rev.* 2 (2016): 507.

Moskowitz, Ben and Aza Raskin, Privacy Icons, https://wiki.mozilla.org/Privacy_Icons, 2011.

Nissenbaum, Helen. "A contextual approach to privacy online." *Daedalus* 140, no. 4 (2011): 32-48.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services." *Information, Communication & Society* (2018): 1-20.

Oehler, Andreas, and Stefan Wendt. "Good consumer information: The Information Paradigm at its (dead) end?." *Journal of Consumer Policy* 40, no. 2 (2017): 179-191.

Palmirani, Monica, and Fabio Vitali. "Akoma-Ntoso for legal documents." In *Legislative XML for the semantic Web*, pp. 75-100. Springer, Dordrecht, 2011.

Palmirani, Monica, Michele Martoni, Arianna Rossi, Cesare Bartolini, and Livio Robaldo. "PrOnto: Privacy Ontology for Legal Reasoning." In *International Conference on Electronic Government and the Information Systems Perspective*, pp. 139-152. Springer, Cham, 2018.

Palmirani, Monica, Michele Martoni, Arianna Rossi, Cesare Bartolini, and Livio Robaldo. "Legal Ontology for Modelling GDPR Concepts and Norms." *Legal Knowledge and Information Systems: JURIX 2018: The Thirty-first Annual Conference*. Vol. 313. IOS Press, 2018.

Passera, Stefania, *Beyond the Wall of Contract Text. Visualizing Contracts to foster Understanding and Collaboration within and across organizations*. Aalto University, 2017.

Passera, Stefania. "Beyond the wall of text: How information design can make contracts user-friendly." In *International Conference of Design, User Experience, and Usability*, pp. 341-352. Springer, Cham, 2015.

Perry-Kessaris, Amanda. "Legal design for practice, activism, policy and research." *Journal of Law and Society* (2018).

Pettersson, John Sören. "A brief evaluation of icons in the first reading of the European Parliament on COM (2012) 0011." In *IFIP International Summer School on Privacy and Identity Management*, pp. 125-135. Springer, Cham, 2014.

Pollach, Irene. "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent." *Journal of Business Ethics* 62, no. 3 (2005): 221.

PrivacyTech *"Privacy Icons" https://www.privacytech.fr/privacy-icons/,* 2017 Rossi, Arianna, and Monica Palmirani. "A visualization approach for adaptive consent in the European data protection framework." In *2017 Conference for E-Democracy and Open Government (CeDEM)*, pp. 159-170. IEEE, 2017.

Proctor, Robert W., M. Athar Ali, and Kim-Phuong L. Vu. "Examining usability of web privacy policies." *Intl. Journal of Human–Computer Interaction* 24, no. 3 (2008): 307-328.

Reeder, Robert W., Patrick Gage Kelley, Aleecia M. McDonald, and Lorrie Faith Cranor. "A user study of the expandable grid applied to P3P privacy policy visualization." In *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, pp. 45-54. ACM, 2008.

Reidenberg, Joel R., Jaspreet Bhatia, Travis D. Breaux, and Thomas B. Norton. "Ambiguity in privacy policies and the impact of regulation." *The Journal of Legal Studies* 45, no. S2 (2016): S163-S190.

Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri. "Review of EU data protection directive: summary." *Information Commissioner's Office* (2009).

Rossi, Arianna. “Legal Design for the General Data Protection Regulation. A Methodology for the Visualization and Communication of Legal Concepts” PhD thesis, Alma Mater Studiorum Università di Bologna, PhD in Law, Science and Technology 31 Ciclo, Forthcoming.

Rossi, Arianna, Rossana Ducato, Helena Haapio, Stefania Passera, and Monica Palmirani. "Legal Design Patterns: Towards A New Language for Legal Information Design." In *Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS* (2019): 517-526.

Rossi, Arianna, Rossana Ducato, Helena Haapio, and Stefania Passera, “When Design Met Law: Design Patterns for Information Transparency.” *Droit de la consommation* 122 (2019): 79-121.

Rossi, Arianna and Monica Palmirani, “DaPIS: an Ontology-Based Data Protection Icon Set,” In G. Peruginelli and S. Faro (Eds.), *Knowledge of the Law in the Big Data Age. Frontiers in Artificial Intelligence and Applications* no. 317 (IOS Press, 2019).

Rundle, Mary C. "International personal data protection and digital identity management tools." *The Berkman Center for Internet & Society Research Publication Series*, 2006.

Sadeh, Norman, Alessandro Acquisti, Travis D. Breaux, Lorrie Faith Cranor, Aleecia M. McDonald, Joel R. Reidenberg, Noah A. Smith et al. "The usable privacy policy project." *Technical report, Technical Report, CMU-ISR-13-119* (2013).

Sartor, Giovanni, Monica Palmirani, Enrico Francesconi, and Maria Angela Biasiotti, eds. *Legislative XML for the semantic web: principles, models, standards for document management*. Vol. 4. Springer Science & Business Media, 2011.

Schaub, Florian, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. "A design space for effective privacy notices." In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pp. 1-17. 2015.

Schuler, Douglas, and Aki Namioka, eds. *Participatory design: Principles and practices*. CRC Press, 1993.

Sloan, Robert H., and Richard Warner. "Beyond notice and choice: Privacy, norms, and consent." *J. High Tech. L.* 14 (2014): 370.

Specht, Louise und 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).

TRUSTe, “*TRUSTe and Disconnect Introduce Visual Icons to Help Consumers Understand Privacy Policies*”(http://www.truste.com/blog/2014/06/23/truste-disconnect-introduce-visual-icons-to-help-consumers-understand\-privacy-policies/), 2014.

Waller, Robert, Jenny Waller, Helena Haapio, Gary Crag, and Sandi Morrisseau. "Cooperation through clarity: Designing simplified contracts." *Journal of Strategic Contracting and Negotiation* 2, no. 1-2 (2016): 48-68.

Whalen, Tara, and Kori M. Inkpen. "Gathering evidence: use of visual security cues in web browsers." In *Proceedings of Graphics Interface 2005*, pp. 137-144. Canadian Human-Computer Communications Society, 2005.

Wiedenbeck, Susan. "The use of icons and labels in an end user application program: an empirical study of learning and retention." *Behaviour & Information Technology* 18, no. 2 (1999): 68-82.

Wogalter, Michael S. "Factors influencing the effectiveness of warnings." In *Visual Information for Everyday Use*, pp. 127-144. CRC Press, 2014.

Wolff, Jennifer Snow, and Michael S. Wogalter. "Comprehension of pictorial symbols: Effects of context and test method." *Human Factors* 40, no. 2 (1998): 173-186.

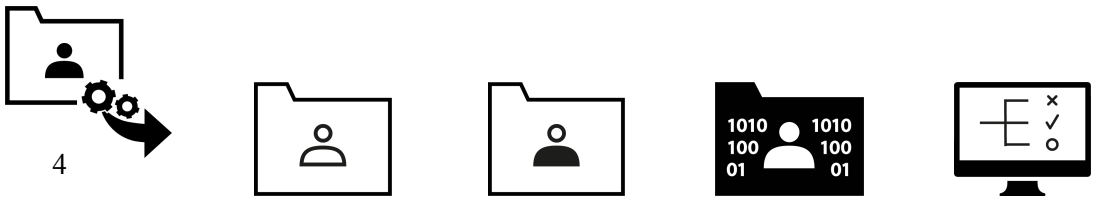
Zuiderveen Borgesius, Frederik. "Consent to Behavioural Targeting in European Law-What Are the Policy Implications of Insights from Behavioural Economics?." *Amsterdam Law School Research Paper* 2013-43 (2013).

Annex 1

Agents and roles: (1) Data subject; (2) Data controller; (3) Supervisory authority

1 2 3

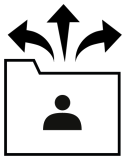
Processing operations: (4) Processing personal data; (5) Anonymization; (6) Pseudonymization; (7) Encryption*; (8) Automated decision-making; (9) Copying; (10) Data Sharing with third parties; (11) Transfer of data to third countries; (12) Storage of data inside the EU



4 5 6 7 8

9 10 11 12

Purposes of processing: (13) Processing purposes; (14) Research purposes; (15) Security purposes; (16) Statistical purposes; (17) Profiling purposes; (18) Marketing purposes; (19a) Purposes of provision of the service - alternative a*; (19b) Purposes of service enhancement - alt. a*; (20a) Purposes of provision of the service - alt. b*; (19b) Purposes of service enhancement - alt. b*

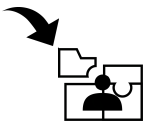


13

14

15

16



17

18

19a

19b

20a

20b

Legal bases: (21) Legal bases; (22) Contract; (23a) Legal obligation - alt. a; (23b) Legal obligation - alt. b; (24) Legitimate interest; (25) Vital interest; (26) Public interest; (27) Consent

21

22

23a

23b

24

25

26

27

Rights of the data subject: (28) Rights; (29) Right of access; (30) Right to be informed; (31) Right to rectification; (32) Right to erasure; (33) Right to restrict processing*; (34) Right to object to processing*; (35) Right to lodge a complaint to a supervisory authority; (36) Right to withdraw consent; (37) Right to data portability

28

29

30

31

32

33

34

35

36

37

* For the icons with this symbol, research about possible alternatives that can better convey the meaning should be carried out.