Knowledge of the Law in the Big Data Age
G. Peruginelli and S. Faro (Eds.)

doi:10.3233/FAIA190020

DaPIS: An Ontology-Based Data Protection Icon Set

Arianna ROSSI [a,b,1] and Monica PALMIRANI [b]
[a] *SnT, University of Luxembourg*
[b] *CIRSFID, Università degli Studi di Bologna (Italy)*

Abstract. Privacy policies are known to be impenetrable and lengthy texts that are hardly read and poorly understood. This is why the General Data Protection Regulation (GDPR) introduces provisions to enhance information transparency including icons as visual means to clarify data practices. However, the research on the creation and evaluation of graphical symbols for the communication of legal concepts, which are generally abstract and unfamiliar to laypeople, is still in its infancy. Moreover, detailed visual representations can support users' comprehension of the underlying concepts, but at the expense of simplicity and usability. This Chapter describes a methodology for the creation and evaluation of DaPIS, a machine-readable Data Protection Icon Set that was designed following human-centered methods drawn from the emerging discipline of Legal Design. Participatory design methods have ensured that the perspectives of legal experts, designers and other relevant stakeholders are combined in a fruitful dialogue, while user studies have empirically determined strengths and weaknesses of the icon set as communicative means for the legal sphere. Inputs from other disciplines were also fundamental: canonical principles drawn from aesthetics, ergonomics and semiotics were included in the methodology. Moreover, DaPIS is modelled on PrOnto, an ontology of the GDPR, thus offering a comprehensive solution for the Semantic Web. In combination with the description of a privacy policy in the legal standard XML Akoma Ntoso, such an approach makes the icons machine-readable and automatically retrievable. Icons can thus serve as information markers in lengthy privacy statements and support an efficient navigation of the document. In this way, different representations of legal information can be mapped and connected to enhance its comprehensibility: the lawyer-readable, the machine-readable, and the human-readable layers.

Keywords. data protection, icons, semantic technologies, ontology, transparency, legal design

1. Introduction

Traditionally, the protection of data subjects in the EU has employed the fundamental tool of mandated disclosure about the collection, use and sharing of their personal data. By be informed about the existence of such data practices, individuals would be in control of their personal information and would be able to make an informed choice either to use or not a certain service (i.e. informed consent) [1]. However, research (e.g., [1]; [2]; [3];

[1]This research was carried out while Arianna Rossi was a fellow at the ICR, University of Luxembourg and was supported by the LAST-JD PhD program (http://www.last-jd.eu/) financed by the EACEA.

[4]; [5]) and empirical evidence have revealed the poor implementation of the principle of transparency of information: often privacy policies serve the mere function of legal compliance, rather than fulfilling their supposed informative function. As much other legal communication [6], "[p]rivacy 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" ([7], p. 29). As a consequence, privacy policies are hardly read and insufficiently understood by data subjects.

Although some scholars support the complete abandon of mandated disclosures [8], the General Data Protection Regulation (GDPR)[2] has challenged this assumption: it has imposed transparency of information as a legal obligation on the data controller and has provided very specific indications about how to translate such abstract requirement into practical and implementable solutions. The quality of the information assumes an unprecedented importance to demonstrate compliance: plain language must be employed in any communication addressed to data subjects (Article 12.1) to overcome the use of overly complex language in lengthy texts that discourage individuals from reading (see e.g. [9]). Moreover, Article 12.7 introduces the possibility to accompany the information provided to data subjects with standardized icons to present "in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing". Such icons must be machine-readable if employed in electronic format.

Although eventually it will be the role of the European Commission to adopt delegated acts to guide the creation of these icons, the need of expert advice is emphasized in Recital 166 GDPR and in the dedicated Guidelines on Transparency by the Article 29 Working Party[3], which encourages an 'evidence-based approach' and 'extensive research' ([10], p. 26) to inform the development and application of the icons, and to determine their efficacy. The investigation presented in this Chapter intends to provide a contribution to the (still) scarce academic research about such topic and to provide the foundations for further investigation.

2. Research Scenario

The GDPR's call for machine-readable graphical elements to express data practices identifies two relevant intertwined lines of research. On the one hand, there are the technologies for the management and (semi-)automated extraction of information from legal documents that provide information interpretable by machines (explored in Section 3). On the other hand, there are interventions that aim to facilitate humans' accessibility to legal information to tackle the problems outlined above: namely, a specific area of Legal Design, i.e. the human-centered design of legal information (illustrated in Section 4). Without an interface, machine-readable information is confined to the exclusive world of computers and technical experts, whereas user-friendly and visualized documents are not meaningful for machines [11]. DaPIS, the Data Protection Icon Set modeled on a computational ontology of the GDPR, is an attempt to reconcile these two directions of research. This Chapter details a methodology to create a 'visual layer' from marked-up privacy

[2]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), OJ L 119/1, 4.5.2016.

[3]Now the European Data Protection Board.

policies that complement the well-established levels of legal information representation [12], with the aim of communicating data practices in an user-friendly manner.

Moreover, the integration with technology also has the goal to reproduce at scale and efficiently those good practices of Legal Design that have proved useful and valuable in specific contexts. Many human-centered solutions applied to legal content are unique and crafted *ad hoc* for specific users in specific contexts (e.g. in contract design, see e.g. [13]; [14]). Instead, information for data subjects and for consumers is mainly addressed to unspecified audiences and the drafters do not usually now the demographics of their potential readers, thus it becomes difficult to design good user-oriented communications. Although there does not always exist a one-fits-all solution, this challenge motivates the investigation and establishment of best practices that can be generalized, or even standardized. Legal Design patterns (i.e. repeatable, systematized and extensible solutions to recurring problems in the legal domain) [15]; [16]; [17]; [18] can represent a viable manner to support the concrete implementation of abstract legal principles [19], like the principle of transparency, as opposed to a jungle of bespoke solutions. The ontology-based companion icons presented in the next paragraphs correspond to one of those patterns [20].

The next Sections illustrate the methodology that was designed to create DaPIS and integrate it with existing semantic technologies for the legal domain (see also [21]). Section 3.1 exemplifies the multi-layered structure that characterizes the machine-interpretable representation of legal documents and adds an additional visual layer. Section 3.2 describes the design of PrOnto, i.e. an ontology of the GDPR, and its constitutive modules, that provided DaPIS' objects of representation. Then, Section 4.1 briefly introduces Legal Design, while in the following Section 4.2 the iterative cycle of icon design is illustrated, alongside the importance of multi-disciplinarity to solve such challenging task (Section 4.3) and the features of modularity and compositionality that constitute the icon set are exposed (Section 4.4). Lastly in Section 4.5, the iterative evaluation phases are shortly illustrated. The final Section 5 provides indications about possible future directions of research.

3. Integrating Machine-Readable and Visual Representations for the Legal Domain

3.1. A Multi-layered Architecture: Adding a Visual Layer

The adoption of semantic technologies in the legal domain envisages a multi-layered architecture for the formal representation and the management, maintenance and communication of the information contained in legal documents. Indeed, different information is expressed through strictly separate layers: text; structure; legal metadata; legal ontology; legal rules [12].

The first three levels can be implemented through the Akoma Ntoso XML schema which is nowadays a well-established international standard adopted by many institutions around the world. Akoma Ntoso enables the addition of descriptive structure (i.e., the structural and semantic mark-up) to the content of such documents [12]. The metadata level (i.e. the third layer) adds descriptions about the content of the legal document [22]: the tags of the inline semantic mark-up can be linked to a reference in the metadata section that, in turn, points to an external resource that defines the meaning of such tags [12], namely an ontology (i.e. the fourth layer). Lastly, the fifth layer provides the legal

meaning of the text and transforms the norms into rules to allow, for example, automated reasoning through machine-interpretable languages like LegalRuleML.

Figure 1 illustrates the application of such multi-layered architecture structure to privacy policies. When the text of a privacy policy is marked up with tags linked to instances of a specific ontology, its semantic content can be described in a univocal and machine-interpretable fashion. The concepts of the ontology can be associated to their corresponding icon and, hence, be semi-automatically summoned by the semantic tags[4]. The underlying assumption, derived from [13]; [16], hypothesizes that icons can accompany the text to clearly indicate where a specific information item appears in long privacy policies, thereby supporting the activity of information finding of the reader in a quicker and more effective manner (i.e. 'companion icons').

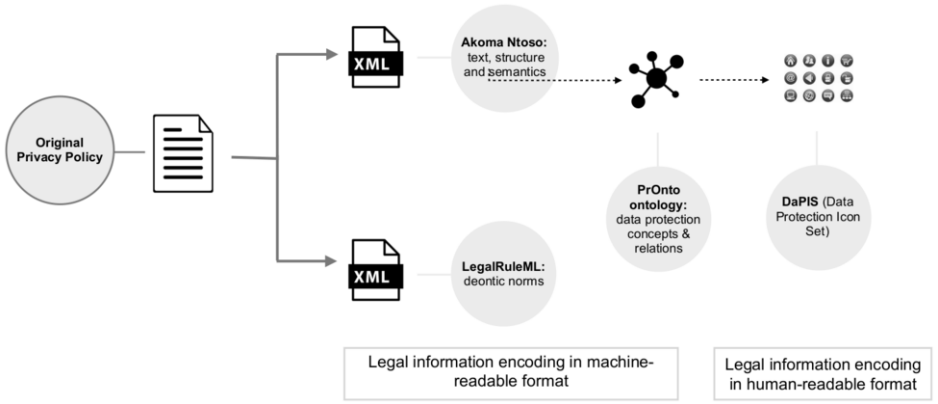


Figure 1. The multi-layered architecture of a privacy policy [12] combined with an additional visual dimension

The description of legal information in a machine-interpretable format also allows automated reasoning on legal texts, for example to draw inferences and match expressions in natural language to the corresponding ontological instance (e.g. the expressions 'you' and 'user' can both refer to the concept of data subject). Moreover, an ontology is independent from language, which counts as an additional strength: the same icon can be provided for text spans expressed in different languages, which yet refer to the same ontological concepts, whilst correspondent labels in different languages can be provided for the same icon.

For such reasons and following the Regulation's call for 'machine-readable' icons on electronical devices, DaPIS (see Section 4) has been fashioned on the conceptual modules of the computational ontology PrOnto. Figure 2 illustrates the network among the document, its mark-up in Akoma Ntoso, the metadata references pointing at the external ontology and the human-oriented representation characterized by information architecture and companion icons.

[4]Provided the development of such a tool, which was not the goal of the project described in these pages, though.

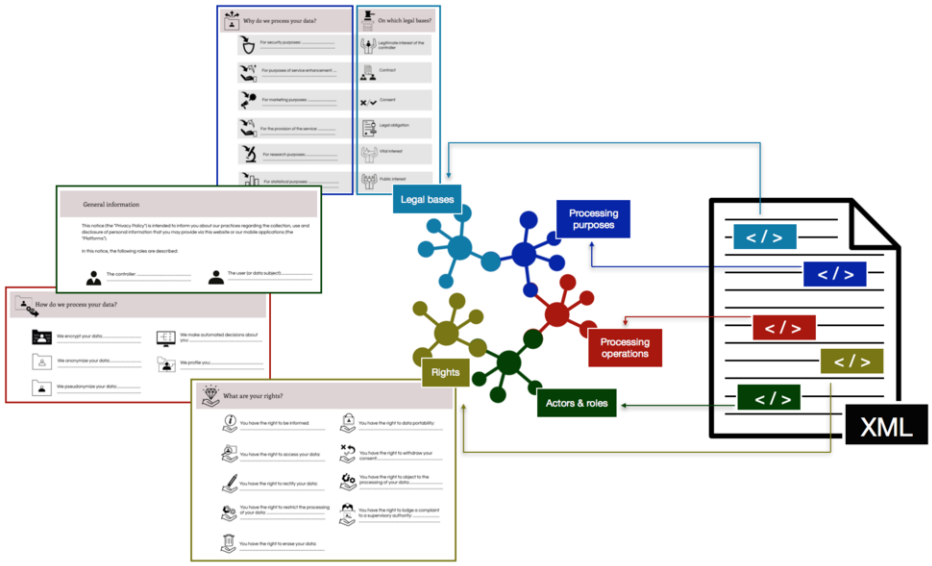


Figure 2. The semantic network among the Akoma Ntoso mark-up of a privacy policy (on the right-hand side), the corresponding concepts arranged in classes of the PrOnto ontology (in the middle) and a visual layer characterized by information architecture and companion icons (on the left-hand side)

3.2. PrOnto

This Section briefly introduces PrOnto[5], the computational ontology that formally models the concepts and norms contained in the GDPR and that has described in detail elsewhere [23]; [24]; [25]. The GDPR provides a European legal framework that defines concepts of data protection, relations among them, and a common vocabulary to describe them. PrOnto is mainly aimed at helping companies and organizations to comply with the many obligations set forth by the GDPR. Combined with other Semantic Web technologies and legal reasoners, goal of this ontology is to facilitate the data controllers' fulfillment of their duties, such as the undertaking of the Data Protection Impact Assessment and the detection of those violations (e.g. a data breach) that envisage countermeasures. Yet, the GDPR constitutes only the initial, central core of norms that have been modeled in Pronto, which is meant to be expanded to other legal frameworks and jurisdictions.

3.2.1. The Design of PrOnto

PrOnto has been designed by following MeLOn [23], an interdisciplinary methodology for the creation of legal ontologies, which is composed of a series of recursive steps. In the first place, the research questions that the ontology aims to address and practical use-cases for its eventual application have been defined: namely, modeling the legal norms defined in the GDPR to allow legal reasoning and compliance checking. Thus, PrOnto has put an emphasis on the modeling of the processing operations, and of the obligations

[5]Developed within the FNR/CORE DAPRECO (DAta Protection REgulation COmpliance https://www.fnr.lu/projects/data-protection-regulation-compliance/) project, at the University of Luxembourg and University of Bologna.

and rights belonging to the different roles (e.g., data subject, controller, etc.) defined by the Regulation.

Then, the GDPR was analyzed by a team of legal knowledge engineers to extract relevant concepts and relations among them, e.g. the different stakeholders affected by this Regulation and their respective rights and duties. This knowledge was then integrated with expert feedback and additional information taken from other authoritative sources, such as Opinions and Guidelines from the Article 29 Working Party (e.g. [26]) and guidance from the UK's Information Commissioner's Office[6], as well as international standards[7]. Moreover, best practices for ontological knowledge modeling have been followed: PrOnto is framed in foundational and core ontologies such as ALLOT [27], FRBR [28], LKIF-core [29], and PWO [30]. In addition, ontology design patterns that express values in time and context [31] have been reused.

MeLOn also provides for the evaluation of the ontology in application to concrete use-cases in terms of coherence, completeness, efficiency, effectiveness, agreement, and usability. Lastly, a testing phase that makes use of the OntoClean method [32] and of SPARQL queries establishes if the research goals defined at the beginning of the ontology design have been reached. PrOnto is currently being employed in projects where its capacity to indicate legal compliance in a variety of scenarios is being assessed [25]. Publication and feedback collection is the last step that contribute to reach a shared agreement within the community of legal experts.

3.2.2. PrOnto's Modules

In the following PrOnto's conceptual modules that constituted the object of DaPIS's design (see Section 4) are described:

1. *Data and documents*: personal data (as opposed to non-personal data and anonymized data), sensitive data, and the documents (e.g. privacy policies, DPIAs, contracts, etc.) that describe and regulate the relationships among different actors involved in the processing;
2. *Agents and roles*: agents can play multiple roles depending on the context and the processing operation (e.g. the same person can be a data subject in one context and a data controller in another one) which also determine their rights and duties;
3. *Processing operations*: these are modelled through a workflow [30], i.e. a sequence of steps with a specific input and a specific output. The essential actions in data processing that were rendered graphically are: anonymize (subclass of delete), pseudonymize (subclass of derive), automated decision-making (individual of infer, specified with a boolean data property), profiling, direct marketing, encrypt, copy, and transfer of personal data to third countries (individual of the class transmit, specified with a place axiom);
4. *Deontic Operators*: the legal norms are modeled in terms of deontic operators (i.e. rights, obligations, permissions, and prohibitions), in order to be integrated with LegalRuleML to support compliance checking with the GDPR. In the perspective of transparency, the rights of the data subject (Articles 12-22) assume paramount importance;

[6]ICO (2014). *Deleting Personal Data*. Technical report.
[7]ISO (2018). *ISO 31000:2018 – Risk management*.

5. (a) *Processing purposes*: the principle of lawfulness (Article 6) establishes that personal data processing must be motivated by specific purposes, that were extracted from articles and recitals of the normative text; (b) *Legal bases*: every purpose must be supported by one of the possible legal bases laid down in Article 6: consent, contract, legal obligation, public interest, vital interest, legitimate interest. Note that the consent and the contract are subclasses of the document class.

Table 1 lists DaPIS' icons in correspondance of the classes and subclasses composing PrOnto.

Table 1. Classes and subclasses of PrOnto that have been visualized in DaPIS

Superclass	Class
(1) Data	Personal Data
(2) Agents' roles	Data subject Data controller Supervisory authority
(3) Processing operations	Copying Pseudonymization Anonymization Direct marketing Automated decision-making Profiling Encryption Transfer of personal data to third countries Storage of personal data in the EU Data sharing with third parties
(4) Data subject's rights	Right to be informed Right of access Right to rectification Right to erasure Right to withdraw consent Right to data portability Right to restriction of processing Right to object to processing Right to lodge a complaint
(5a) Processing purposes	Research purposes Statistical purposes Purpose of information security Purpose of provision of the service Purpose of service enhancement Marketing purposes Profiling purposes
(5b) Legal bases for processing	Consent Legal obligation Vital interest Public interest Legitimate interest Contract

In conclusion, unlike other data protection icon sets focusing on data types and a handful of processing operations (e.g. [33]; [34]), DaPIS provides a systematic formalization and classification of data protection concepts and relations among them. It addition-

ally covers legal bases for processing, rights of the data subject and a more extended set of processing purposes. These information items ought to be presented to data subjects when processing takes place according to Articles 13 and 14 GDPR. Although some of the other icon sets partially overlap with the one described in these pages and can thus be successfully integrated, DaPIS also provides graphical representations for concepts that have never been visualized, like the rights of the data subject.

4. DaPIS: The Data Protection Icon Set

The project described in these pages has used the structured and formalized representation of the data protection domain explained above to define and circumscribe the items meant to be visualized. Legal Design methods were then employed for the creation of the icon set.

4.1. Legal Design and Users of the Law

Legal Design is an interdisciplinary approach for "the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying" ([35], Chap. 1). Human-centered design focuses on the development of solutions that consider the target audience's needs: in this view, 'users of the law' are not only lawyers, judges and regulators, but also citizens, businesses and laypeople in general. For this reason, Legal Design favors interdisciplinarity and participatory design approaches [36], with the aim to recompose the fracture between the theoretical assumptions of the law and actual individual's need and abilities.

In the case of the discrepancy briefly analyzed in Section 1, the law provides for instruments (i.e. mandated disclosures) that should guide the data-related choices of data subjects in an autonomous and informed manner. Yet, the implementation of the principle of transparency is generally so poor and problematic that individuals do not view privacy policies as an empowering instrument to understand their rights and how legal rules apply to them, but rather as a nuisance that is ignored or rapidly clicked away. As they are traditionally fashioned, privacy terms serve the needs of lawyers and regulators, but not those of data subjects. Indeed, a wall of text without any affordance for the human eye discourage individuals from engaging with the reader. On the contrary, visual cues can demonstrably attract reader's attention, reinforce memorization and support effective information finding.

4.2. An Iterative Architecture for the Design of DaPIS

Legal Design includes participatory design methods in its toolkit in order to consider and involve all the users of the law. This is why, DaPIS was created through a series of multi-stakeholders' workshops that followed the design cycle phases: 1. discover; 2. synthesize; 3. build; 4. test; 5. evolve [35]. Three working versions of DaPIS were created and evaluated in an iterative manner: the icons of each version were evaluated in a user study (see Section 4.5) and, if needed, consequently refined in the following workshop(s). Figure 3 exemplifies the DaPIS design cycle.

The development of DaPIS can be described as follows:

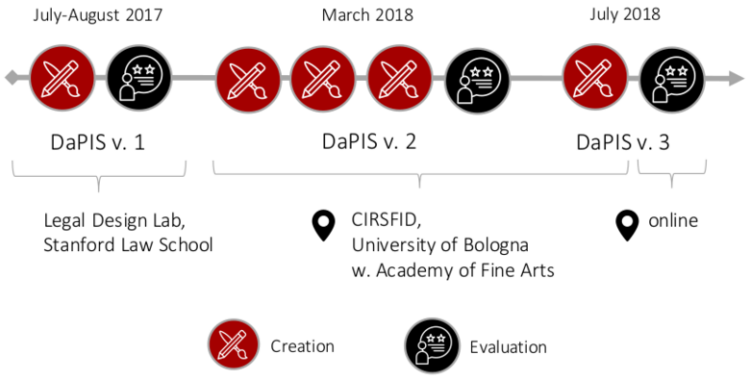


Figure 3. The iterative cycle of DaPIS design

1. DaPIS version 1, in July-August 2017, at the Legal Design Lab of Stanford Law School (US): one exploratory workshop to design the first prototypes of the icon set;
2. DaPIS version 2, in March 2018, at the CIRSFID, University of Bologna, Italy, in collaboration with the Academy of Arts of Bologna and Società Italiana Informatica Giuridica: three multi-stakeholders' workshops focused on further icon design and redesign of DaPIS version 1;
3. DaPIS version 3, in July 2018, at the CIRSFID in collaboration with the Academy of Arts of Bologna: one last workshop to refine DaPIS version 2.

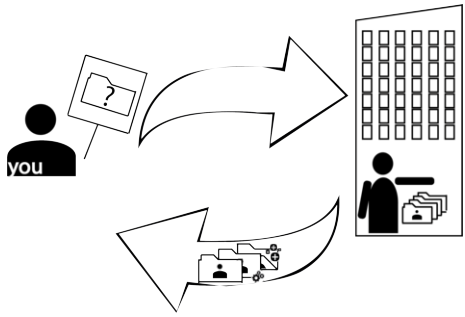
The first workshop was exploratory: it mainly served to indicate best practices for icon design of data protection concepts (i.e. mostly abstract and unfamiliar legal-technical concepts) and to rule out the less viable hypotheses that had been initially postulated. For instance, the modularity of composition of icons (see Section 4.4) was one of the proposed strategies that later informed the further development of the icon set. On the contrary, after the first icons' evaluation study and during the following workshops, the methodological choice to design literal and detailed representation of complex notions (e.g. the right to access) for alleged ease of interpretation was abandoned in favor of visual metaphors that could summarize the same concept in a reduced number of pixels and could be more easily used in responsive design (Figure 4).

During the following workshops, the missing visualizations for the ontological classes described above were systematically prototyped and vetted in a coherent manner with respect to the other existing icons; those icons that had shown major flaws during the user studies were re-elaborated; and, finally, for some concepts alternative solutions were conceived[8]. DaPIS has thus been designed in an iterative manner, through a continuous discussion, vetting and refinement of alternative ideas and prototypes during multiple cycles of evaluation and thanks to participants with composite backgrounds.

4.3. Addressing the Challenge from a Multi-Disciplinary Perspective

Diverse mental models and visual vocabularies derived from different backgrounds and experiences have been explicitly taken into consideration for the design of DaPIS. A pre-

[8]In [20], Chapter 5, thorough and extensive details about DaPIS design and evaluation are provided. See also: http://gdprbydesign.cirsfid.unibo.it/.



(a) Literal representation

(b) Visual metaphor

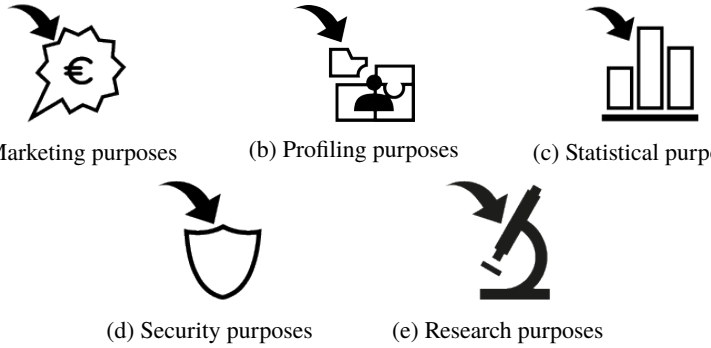
Figure 4. Two subsequent versions of the right to access. On the left-hand side, the first prototype that attempts to literally reproduce the definition of the concept. On the right-hand side, the re-elaboration of the prototype into a less literal, but more contained representation

cise methodological choice was represented by the involvement of different stakeholders in the phase of creation of DaPIS in order to leverage their multiple skills and assets. Participatory design enables mutual learning among individuals with different mindsets and levels of expertise, make implicit, expertise-specific assumptions evident and debunk common domain-dependent misconceptions. Concretely, in this case, it meant that experts with a technical background clarified specialized notions such as encryption or pseudonymization to the other members of the group to facilitate the process of visualization; lawyers and legal scholars interpreted GDPR's definitions, provided appropriate examples and repeatedly voiced their concerns about misinterpretation and oversimplification, ultimately influencing icons' design; graphic designers and other professionals from visual disciplines provided the guidelines, the techniques and the tools to create appropriate visualizations for the intended audience and the intended medium; representatives of the businesses-world expressed the challenges for widespread adoption and effective implementation of the icon set; and finally laypeople added non-expert, but at the same time non-trivial, views and knowledge to the design process, for instance about the visual conventions they were familiar with [37]; [38]. Treating such a composite group of individuals as co-designers allowed for the creation of an icon set that epitomizes a synthesis of the different views, needs and concerns of the people that might be, in various manners, impacted by it.

4.4. Modularity and Compositionality of the Icons

The use of the ontology as conceptual framework oriented the icon design towards a compositional visual vocabulary: each graphical element corresponds to one and only one ontological element. Such basic elements can be combined to create more complex notions. For instance, the purposes of processing are represented by an arrow, while the concept of right is visualized with an upward-facing hand. Thus, the subclasses of purposes (Figure 5) and the subclasses of rights (Figure 6) contain such elements to indicate that they belong to the same class, but are complemented with other elements that specify their meaning and distinguish them from the icons of the same class. Similarly, personal data is represented as a prototypical file folder with a users' figure atop of it, while the outcome of processing operations on such data are visualized as variations of the

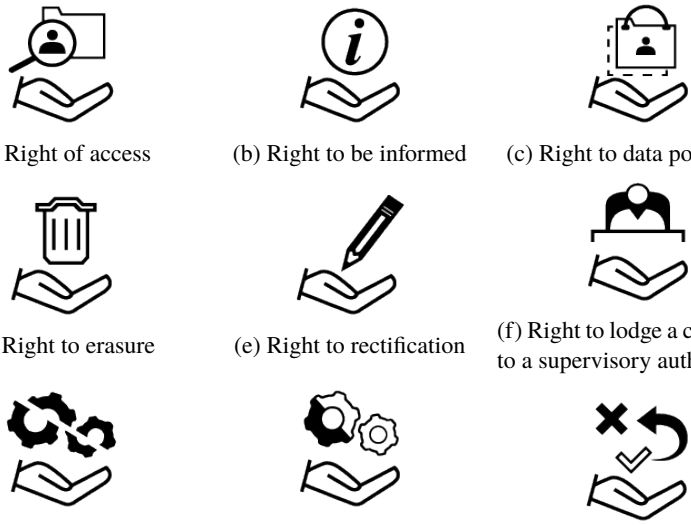
folder (Figure 7). The complete icon set, composed of 33 icons, is freely downloadable[9] and is more thoroughly illustrated in [20].



(a) Marketing purposes (b) Profiling purposes (c) Statistical purposes

(d) Security purposes (e) Research purposes

Figure 5. Icons representing the processing purposes: the recurrent arrow stands for 'purpose', while the complementary element specifies the type of purpose



(a) Right of access (b) Right to be informed (c) Right to data portability

(d) Right to erasure (e) Right to rectification (f) Right to lodge a complaint to a supervisory authority

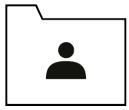
(g) Right to obejct to processing (h) Right to restriction to processing (i) Right to withdraw consent

Figure 6. Icons representing the rights of the data subject. The recurring element of the upward-facing hand symbolizes the 'right' and is meant to convey the concept of 'being in control' and 'having the power over' the element located above it, which specifies the meaning of the icon

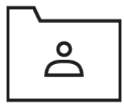
4.5. Evaluation of the Icon Set

As described above, an evaluation phase followed every phase of major (re)design of DaPIS, for a total of three:

[9] http://gdprbydesign.cirsfid.unibo.it/dapis-2/.

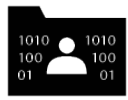


(a) Personal data



(b) Anonymized data

(c) Pseudonymized Data



(d) Encrypted Data

Figure 7. The variations of the icons representing personal data as outcomes of different processing operations

1. Evaluation of DaPIS 1: carried out at Stanford (US); 16 participants; origin: mostly American; age: between 19 and 76 years old; level of education: mostly with a high school diploma;
2. Evlauation of DaPIS 2: carried out in Bologna (IT); 16 participants; origin: Italian; age: between 20 and 29 years old; level of education: mostly with at least a Bachelor's degree;
3. Evaluation of DaPIS 3: carried out in an online environment, on the research website; 10 participants; origin: Italy, Armenia, Iran, Canada and Greece; level of education: mostly with a Master's degree.

Main aim of such assessments was the evaluation of the iconographical choices made during the design workshops. Key dimensions that were considered were legibility (i.e. the ease of recognizition of the different elements composing each icon) and ease of understanding (i.e. the correct matching between graphical symbol and its meaning) [39]. For the latter, however, standard evaluation frameworks are either meant for those symbols whose referent is known to users (e.g. the concept of airplane)[10]; or for those symbols whose referent is unknown (e.g. the concept of pseudonymization) but a previous phase of familiarity training has been carried out[11]. Since none of such evaluation methods were appropriate for a one-time only assessment, a subjective estimation of goodness of fit between definition of a concept and the proposed graphical representation [40] and explanations thereof were asked, to provide an indication for those solutions considered more or less promising. In order to do so, even the degree of agreement among the respondents' answers was taken into consideration because indicative in this respect: great variation in the answers implies disagreement about the icons' efficacy, while greater uniformity indicates consensus and, hence, pinpoints the more easily recognizable icons. For instance, positive ratings coincided for the icon representing the transfer to countries outside of the EU because it uses an easily recognizable prototypical representation (i.e. the stars in circle of the EU flag and the personal data folder), while diverse degrees of appreciation were gathered by, e.g., the icon representing public interest. This variety of ratings is also due to the fact that there are some graphical elements are more familiar to users than other, while concrete objects are also more easily visualizable,

[10]ISO (2014). *ISO 9186-1:2014. Graphical Symbols – Test Methods – Part 1: Method for Testing Comprehensibility*.

[11]ISO (2014). *ISO 9186-3:2014. Graphical Symbols – Test Methods – Part 3: Method for Testing Symbol Referent Association*.

and thus, apprehended. The motivations and explanations for the ratings provided by the participants constituted a valuable informative feedback that was crucial for further icon re-elaboration.

5. Conclusions and Future Work

This Chapter has briefly presented the development and the main outcomes of a multidisciplinary project that combines machine-readable representations of legal information with corresponding (still underresearched, but increasingly investigated) human-oriented visual representations. The case study analyzed in these pages concerns the data protection domain and is meant to propose an implementation of the transparency principle set forth by the General Data Protection Regulation. In particular, an overview of PrOnto, an ontology of the GDPR's concepts (and norms), and DaPIS, a data protection icon set modeled on such concepts where provided. The explanation of the design and evaluation of such icon set has constituted the focus of this Chapter.

Future research should proceed in multiple directions. The PrOnto ontology is currently being developed, refined and expanded. Appropriate icons for additional classes can be created or mutuated from other icon sets that have been developed or are currently under development. However, it should be researched the number of icons that an individual can learn and retain without feeling overwhelmed. Furthermore, notwithstanding the user studies briefly described above, there are limitations that should be addressed in the future. Firstly, the participants to the studies were few, very diverse in terms of origin but uniform in terms of educational level (i.e. medium-high). Some of them had legal expertise or strong familiarity with technologies, while others did not. Secondly, since one of the main obstacles to ease of recognition is the lack of familiarity with the graphical symbol or with its referent, it should be expected that the effect of training increases recognition rates and determines easier recall. Thus, longitudinal studies that envisage consequent phases should be preferred [41] and should carried out involving individuals coming from all the Member States and of more varied demographics. Finally, as illustrated in [21], DaPIS should also be judged with respect to its function in context: namely, the capacity of its icons to act as information markers that effectively support the navigation through large amounts of legal information and increase speed and accuracy of comprehension.

DaPIS does not aim to be the ultimate, immutable data protection icon set to be standardized across the European member states. There even are some icons that would benefit from a re-design and better performing alternative solutions could be advanced. Other projects having similar aims exist [34], but might reach different outcomes. This research rather details a methodology for a design process that, on the one hand, values the multidisciplinarity that is necessary when dealing with complex contemporary topics like device-mediated data processing. On the other hand, it strives to an effective integration with semantic technologies for legal data that are mostly concerned with machine-interpretable meanings, but more rarely remember the human end-user. The goal of this research is to possibly inform the preparatory work and the decisions of the European Commission about the creation and implementation of the GDPR's icons and to stimulate an international, interdisciplinary debate.

References

[1] Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, 140*(4), 32-48.

[2] Monteleone, S. (2015). Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-aware Regulation. *Syracuse Journal of International Law and Commerce, 43*, 69.

[3] Schaub, F., Balebako, R., Durity, A. L. & Cranor, L. F. (2015). A Design Space for Effective Privacy Notices. In *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*, 1-17.

[4] Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*, 1880.

[5] Oehler, A. & Wendt, S. (2017). Good Consumer Information: The Information Paradigm at Its (Dead) End? *Journal of Consumer Policy, 40*(2), 179-191.

[6] Berger-Walliser, G., Bird, R. C. & Haapio, H. (2011). Promoting Business Success through Contract Visualization. *Journal of Law, Business & Ethics, 17*, 55.

[7] Robinson, N., Graux, H., Botterman, M. & L. Valeri (2009). *Review of the European Data Protection Directive (sponsored by the Information Commissioner's Officer)*. RAND Europe.

[8] Ben-Shahar, O. & Schneider, C. E. (2014). *More Than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton University Press.

[9] Fabian, B., Ermakova, T. & Lentz, T. (2017). Large-scale Readability Analysis of Privacy Policies. In *Proceedings of the International Conference on Web Intelligence*. ACM, 18-25.

[10] Article 29 Data Protection Working Party (2018). *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*, 17/EN WP251rev.01.

[11] Haapio, H., Plewe, D. & deRooy, R. (2017). Contract Continuum: From Text to Images, Comics, and Code. In Schweighofer, E., Kummer, F., Hötzendorfer, W. & Sorge, C. (Eds.). *Trends and Communities of Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium IRIS*. OCG Verlag, 411-418.

[12] Palmirani, M. & Vitali, F. (2011). Akoma-Ntoso for Legal Documents. In Sartor, G., Palmirani, M., Francesconi, E. & Biasiotti, M. A. (Eds.). *Legislative XML for the Semantic Web*. Springer, 75-100.

[13] Passera, S. (2015). Beyond the Wall of Text: How Information Design Can Make Contracts User-friendly. In *International Conference of Design, User Experience, and Usability*. Springer, 341-352.

[14] Waller, R., Waller, J., Haapio, H., Crag, G. & Morrisseau, S. (2016). Cooperation through Clarity: Designing Simplified Contracts. *Journal of Strategic Contracting and Negotiation, 2*(1-2), 48-68.

[15] Haapio, H. & Hagan, M. (2016). Design Patterns for Contracts. In Schweighofer, E., Kummer, F., Hötzendorfer, W. & Borges, G. (Eds.). *Networks. Proceedings of the 19th International Legal Informatics Symposium IRIS*. OCG Verlag, 381-388.

[16] Haapio, H. & Passera, S. (2019). Contracts As Interfaces: Exploring Visual Representation Patterns in Contract Design. In Katz, D., Bommarito, M. & Dolin, R. (Eds.). *Legal Informatics*. Cambridge University Press.

[17] Haapio, H., Hagan, M., Palmirani, M. & Rossi, A. (2018). Legal Design Patterns for Privacy. In Schweighofer, E., Kummer, F., Saarenpää, A. & Schafer, B. (Eds.). *Data Protection/LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS*. Editions Weblaw, 445-450.

[18] Rossi, A., Ducato, R., Haapio, H. & Passera, S. (2019). When Design Met Law: Design Patterns for Information Transparency. *Droit de la Consommation = Consumenterecht: DCCR*, 122-123, 79-121.

[19] Rossi, A., Ducato, R., Haapio, H., Passera, S. & Palmirani, M. (2019). Legal Design Patterns: Towards A New Language for Legal Information Design. In Schweighofer, E., Kummer, F. & Saarenpää, A. (Eds.). *Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS*. Editions Weblaw, 517-526.

[20] Rossi, A. (2019). *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 (forthcoming).

[21] Palmirani, M., Rossi, A., Martoni, M. & Hagan, M. (2018). A Methodological Framework to Design a Machine-readable Privacy Icon Set. In Schweighofer, E., Kummer, F., Saarenpää, A. & Schafer, B. (Eds.). *Data Protection/LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS*. Editions Weblaw, 451-454.

[22] Monica Palmirani, M., Sperberg, R., Vergottini, G. & Vitali, F. (2016). *Akoma Ntoso Version 1.0 Part 1: XML Vocabulary*. OASIS Committee Specification Draft 02 / Public Review Draft 02. Technical report.

[23] Palmirani, M., Martoni, M., Rossi, A., Bartolini, C. & Robaldo, L. (2018). PrOnto: Privacy Ontology for Legal Reasoning. In *eGovis 2018, the 7th International Conference on Electronic Government and the Information Systems Perspective*. Springer, 139-152.

[24] Palmirani, M., Martoni, M., Rossi, A., Bartolini, C. & Robaldo, L. (2018). PrOnto: Privacy Ontology for Legal Reasoning. In *Proceedings of the 18th European Conference on Digital Government*. Academic Conferences and Publishing International Limited, 142-151.

[25] Palmirani, M., Martoni, M., Rossi, A., Bartolini, C. & Robaldo, L. (2018). Legal Ontology for Modelling GDPR Concepts and Norms. In Palmirani, M. (Ed.). *Legal Knowledge and Information Systems. Proceedings of the 31st Jurix Conference*. IOS Press, 91-100.

[26] Article 29 Data Protection Working Party (2017). *Guidelines on Personal Data Breach Notification Under Regulation 2016/679*, 18/EN WP250rev.01.

[27] Barabucci, G., Di Iorio, A., Poggi, F. & Vitali, F. (2013). Integration of Legal Datasets: From Metamodel to Implementation. In *Proceedings of International Conference on Information Integration and Web-based Applications & Services*. ACM, 585.

[28] Functional Requirements for Bibliographic Records (2009). *International Federation of Library Associations and Institutions*. Technical report.

[29] Breuker, J. A. P. J., Hoekstra, R., van den Berg, K., Rubino, R., Sartor, G., Palmirani, M., Wyner, A. & Bench-Capon, T. (2007). *OWL Ontology of Basic Legal Concepts (LKIF-Core). Estrella: Deliverable*. UVA. Technical report.

[30] Gangemi, A., Peroni, S., Shotton, D. & Vitali, F. (2017). The Publishing Workflow Ontology (PWO). *Semantic Web, 8*(5), 703-718.

[31] Peroni, S., Palmirani, M. & Vitali, F. (2017). UNDO: The United Nations System Document Ontology. In *International Semantic Web Conference*. Springer, 175-183.

[32] Guarino, N. & Welty, C. (2002). Evaluating Ontological Decisions with OntoClean. *Communications of the ACM, 45*(2), 61-65.

[33] Graf, C., Hochleitner, C., Wolkerstorfer, P., Angulo, J., Fischer-Hübner, S. & Wästlund, E. (2011). *Final HCI Research Project*. PrimeLife Consortium. Technical report.

[34] Privacy Tech. *Privacy Icons*. https://www.privacytech.fr/privacy-icons/.

[35] Hagan, M. (2017). *Law by Design*, http://www.lawbydesign.co.

[36] Van Der Velden, M. & Moertberg, C. (2015). Participatory Design and Design for Values. In *Handbook of Ethics, Values and Technological Design*. Springer, 41-66.

[37] Rossi, A. & Palmirani, M. (2018). From Words to Images Through Legal Visualization. In *AI Approaches to the Complexity of Legal Systems*. Springer.

[38] Rossi, A. & Haapio, H. (2019). Proactive Legal Design: Embedding Values in the Design of Legal Artefacts. In Schweighofer, E., Kummer, F. & Saarenpää, A. (Eds.). *Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS*. Editions Weblaw, 537-544.

[39] Dewar, R. (1999). *Visual Information for Everyday Use: Design and Research Perspectives*, Chapter Design and Evaluation of Public Information Symbols. Taylor and Francis, 285-303.

[40] Wogalter, M. S., Silver, N. C., Leonard, S. D. & Zaikina, H. (2006). *Handbook of Warnings*, Chapter Warning symbols. Lawrence Erlbaum Associates Mahwah, 159-176.

[41] Flick, U. (2018). *An Introduction to Qualitative Research*. Sage Publications Limited.