Extending Layered Privacy Language to Support Privacy Icons for a Personal Privacy Policy User Interface

Armin Gerl
DIMIS, University of Passau
Passau, Germany
armin.gerl@uni-passau.de

The LPL Personal Privacy Policy User Interface (LPL PPP UI) is designed to allow for informed and free consent. An extension for the Layered Privacy Language and the Privacy Icons Overview is introduced here. The capabilities of the LPL PPP UI consist of informing the Data Subject about the contents of a privacy policy in a structured way, personal privacy interactions, and giving the Data Subject an overview utilising privacy icons are presented. The impact of the Privacy Icons Overview is further evaluated, taking into consideration both speed and accuracy. Furthermore, additional challenges for the creation of a privacy policy user interface as well as privacy icons are presented.

GDPR, Personal Privacy, Privacy Icons, Privacy Language, Usable Privacy

1. MOTIVATION

The Layered Privacy Language (LPL) expresses and enforces privacy properties such as personal privacy, user consent, data provenance, and retention management [1]. It is intended to allow Data Subjects to accept and consent to privacy policies and enforce privacy-preserving processing based upon a personalised privacy policy. To allow a user to consent to a privacy policy, we propose a user interface supporting privacy icons based on LPL. The General Data Protection Regulation (GDPR), entered into force on 25th May 2018. It is designed to standardise data privacy laws across Europe to protect and empower all EU citizens' data privacy and to rework the way organisations approach data privacy. The GDPR specifies that consent has to be given freely, specific, informed and unambiguous [2, Art. 4 No. 11]. Additionally, the concept of Personal Privacy [3] is considered. It states that the user can influence the privacy properties of the processing. Furthermore, the GDPR states that the contents of the privacy policies can be represented by standardised icons [2, Art. 12 No. 7]. Accordingly, we propose an extension of LPL considering those properties. Current state-of-the-art privacy policies are usually purely text-based and only allow two options – consent or dissent. It is debatable whether such privacy policies really inform the users about the processing of their data. Therefore, we introduce a user interface, based on LPL. On the one hand it allows the display of privacy icons and on the other hand it allows the personalisation of the privacy policy allowing consent and dissent to purposes. In the first user interface prototyping with LPL, we discovered that LPL lacks proper multi-lingual support, as well as human-readable descriptions for all of its elements. Additionally, the legal requirement, that icons should be included in a machine-readable format, is not fulfilled.

The main contributions of this paper are the UI Extension for LPL, the LPL Personal Privacy Policy Interface, LPL Privacy Icons and the Privacy Icon Overview evaluation. The paper is structured as follows: In section 2, the LPL User Interface Extension is introduced. Section 3 introduces LPL Privacy Icons, which will be utilised in section 4 describing the LPL Personal Privacy Policy User Interface (LPL PPP UI). Section 5 describes the Privacy Icon Overview. The paper is concluded in section 6, which also provides an outlook for future works.

2. LPL UI EXTENSION

LPL, considering both legal and computer science view on privacy, represents privacy policies, which can be structured as a set of purposes, each describing the processed data and how the data has to be anonymised. Its intended use is to be

Proceedings of British HCI 2018. Belfast, UK.

presented to and accepted by the Data Subject to enable a privacy-preserving processing of the personal data. The structure of LPL is detailed by Gerl et al. [1]. An overview is given in the following to show its limitations.

The root element is the *LayeredPrivacyPolicy* containing the *'lang'* attribute defining the displayed language, introducing redundant policy definitions for each privacy policy. It contains a set of *Purpose* elements, each defining the processing of data. The *Purpose* contains the *'required', 'optOut'* and *'description'* attributes. The *'required'* attribute defines if the purpose can be dissented to. The *'optOut'* attribute defines if the purpose has to be actively dissented (opt-out) or consented to (opt-in). The 'description' attribute is used for a human-readable description of the purpose in the language defined by the previously-described *'lang'* attribute. For each *Purpose* a set of *Data* elements is defined. Each *Data* element has the attributes *'required'* and *'description'*, with the same intended functionality.

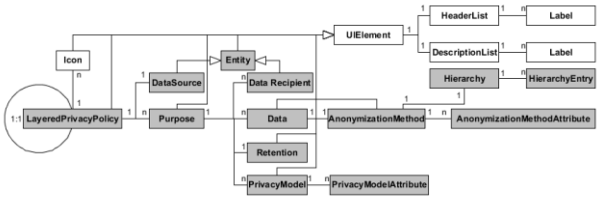


Figure 1: Extension of the Layered Privacy Language. White elements are part of the User Interface Extension of LPL, grey elements already existed in LPL. Some attributes are omitted for better readability.

No representation of icons in a machine-readable format or a proper multi-lingual support has been given by LPL as of its described state.

Therefore, we extended LPL (see Figure 1) and added a list of *'Icon' elements* for the *'LayeredPrivacyPolicy'* element, defining privacy icons, identified by a unique *'name'.* To support multi-lingual support, we removed all existing *'description'* fields and replaced them with *'DescriptionList' and 'HeaderList' each* containing a set of *'Label'* elements. For example, the

descriptionList =

{('en', 'Hello'),('de', 'Hallo'),('fr', 'Bonjour')}

defines 'Hello' in English, German and French. Both the *'HeaderList'* and *'DescriptionList'* have been added to the *'LayeredPrivacyPolicy'*, *'Purpose'*, *'Entity'*, *'Data'*, *'AnonymizationMethod'*, *'Retention'*, *'PrivacyModel'* and the new *'Icon'* element by inheritance of the *'UIElement'*. This allows the creation of detailed multi-lingual natural language descriptions of the privacy policy and therefore avoids redundant definitions of the same privacy policy for different languages.

3. LPL PRIVACY ICONS

Next to a proposed set of privacy icons specifically for the GDPR [4] several additional sets can be found [5] [6]. None of the privacy icon sets is established as a widely-adapted standard.

Our approach on designing a privacy icon set is based on the analysis of privacy policies and method descriptions that are used by the public sector, more specifically research projects. We identified most commonly-used topics and purposes. This resulted in a comprehensive privacy icon set (see Figure 2) that can be used by LPL. It contains icons representing data sharing, retention, anonymisation, and common purposes such as marketing. The privacy icon set for LPL can be exchanged to facilitate the eventually officially agreed on privacy icons for the GDPR. We are aware that the icons have to be evaluated, which is outside the scope of this paper.

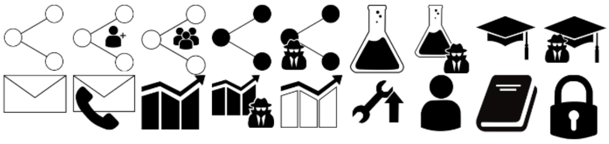


Figure 2: Overview of LPL Privacy Icons.

4. LPL PERSONAL PRIVACY POLICY USER INTERFACE (LPL PPP UI)

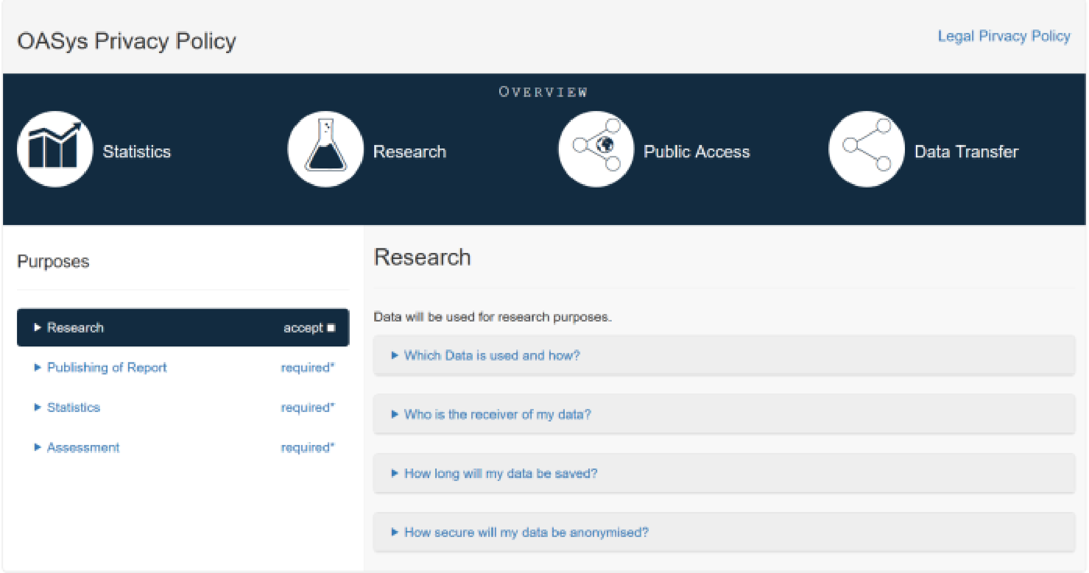
In the following, we describe related works for user interfaces of privacy languages and the design process that leads to the creation of the LPL PPP UI and its structure.

4.1. Related Works

Existing user interfaces for other privacy languages have been surveyed in the process of our development and evaluation. For P3P the '*AT&T Privacy Bird*' browser plugin [7], privacy policy visualisations [8] [9], as well as a '*Nutrition Label*' [10] [11] have been proposed. For PPL the '*Send Data?*' browser extension has been developed [12]. Also representatives of the legal view postulate that new ways to inform the Data Subject have to be found [13]. Accordingly, we focus on representing privacy policies created by LPL to inform the user about its content utilising privacy icons with the LPL Personal Privacy Policy User Interface as described in the following.

4.2. Design Process

Although different user groups can be identified [14], each Data Subject has to be informed on the contents of the privacy policy. Therefore, a more general design concept, namely the *Visual Information Seeking Mantra* [15], has been used. The intention is to use an *Overview* with privacy



OASys Privacy Policy

Legal Pirvacy Policy

OVERVIEW

Purposes

▸ Research	accept ■
▸ Publishing of Report	required*
▸ Statistics	required*
▸ Assessment	required*

Research

Data will be used for research purposes.

▸ Which Data is used and how?

▸ Who is the receiver of my data?

▸ How long will my data be saved?

▸ How secure will my data be anonymised?

Figure 3: LPL Personal Privacy Policy User Interface example.

icons to inform the Data Subject ‘at first glance’. This includes the possibility to *Filter* further *Details on Demand* according to their personal needs.

The remaining design principles have been excluded for the scope of this prototype but possible implementation is discussed in the following. *View Relationships* could visualise how data fields are used within automatic decision-making [2, Art. 13 No. 2]. A *History* of accepted privacy policies could be made available for the Data Subject to reflect its decisions, which would also require the Data Subject to *Extract* the privacy policy contents.

4.3. User Interface Structure

In the following, we will present the structure of the *LPL Personal Privacy Policy User Interface (LPL PPP UI)* based on a real privacy policy of a research project (see Figure 3).

The header contains the title of the privacy policy as well as a link to a regular privacy policy representation. *Overview* is given in two sections of the user interface. On the one hand the top bar, utilising privacy icons, gives an overview over the processing of the personal data. On the other hand the left column represents the purpose overview. The purpose overview lists all purposes, showing *opt-in* and *opt-out* purposes, as well as purposes which are *required* to be consented to. An interested Data Subject may look into further details of each purpose utilising the purpose details, by selecting (filtering) the shown details. The purpose details show a purpose description and allow the inspection of the data elements, recipients, retention, and privacy model.

For the data elements, each is listed in the data overview that can be accessed by a click on the corresponding header. Its details will be displayed in the data details. Accordingly, each recipient is shown in the recipient overview and its description is shown in recipient detail. The retention is related to all the data of the corresponding purpose and is textually displayed.

The privacy model defines the properties that have to be fulfilled for the set of data described in the corresponding purpose. Rather than describing a privacy model by an abstract definition that should not be understood by any non-experts, the privacy model will be described by the risk of de-anonymisation. For example, *k-Anonym*ity with *k=3* has a risk of 33% for de-identification in case of a *Record Linkage* attack scenario [16].

With LPL PPP UI the Data Subject is allowed to accept or decline purposes. In the *Purpose Overview* we distinguish between required and non-mandatory purposes. Required purposes cannot be declined. Non-mandatory purposes are displayed with an additional checkbox that the user can interact with, in order to consent or dissent. This is only checked for *opt-in* purposes.

5. PRIVACY ICON OVERVIEW EVALUATION

We evaluated whether the LPL PPP UI with *Privacy Icon Overview* is advantageous over an LPL PPP UI without *Privacy Icon Overview*. The goal was to observe the benefit of presenting to a user the privacy icons. As the basis for the privacy policies, we used the previously-mentioned privacy policy of a research project.

5.1. Experiment Design

The participants received tasks that simulate an interested Data Subject inspecting the privacy policies to receive an overview. For the evaluation of the Privacy Icon Overview, we created two similar tasks. We present a distinct privacy policy to each participant with the task to inform them about the purposes of the processing of the user's data, before using a questionnaire to answer which purposes are given. Each correctly answered question scored a point.

In the experiment 10 random volunteers participated, separated into two groups (A and B). Group A had three female and two male participants. Group B had two female and three male participants. Each group had to fulfil two tasks. The participants use the internet regularly, but have not been educated or provided information about the LPL PPP UI or the LPL Privacy Icons. Nor have they been involved in the development. The tasks are presented by alternating an LPL PPP UI with Privacy Icon Overview and LPL PPP UI without Privacy Icon Overview. If group A has to do the task with the Privacy Icon Overview than group B has to do the task without the Privacy Icon Overview. Therefore, each group had to fulfil one task with a regular and LPL privacy policy.

5.2. Results

It was observed that the average time spent on the view with Privacy Icon Overview is higher compared to the view without Privacy Icon Overview in task 1, and vice-versa for task 2. Additionally, it can be observed that both for task 1 and 2 the average score improved by about 6% for the LPL PPP UI with Privacy Icon Overview compared to the LPL PPP UI without Privacy Icon Overview (see Table 1).

Table 1: *Mean quantitative results of the Privacy Icon Overview Evaluation are shown. Average time is measured in seconds (s) and the score is percentual to the maximum score. Tasks are differentiated according the usage of LPL PPP UI with Privacy Icon Overview or LPL PPP UI without Privacy Icon Overview.*

Task	**With Overview**		**Without Overview**	
	Time (s)	*Score (%)*	*Time (s)*	*Score (%)*
1 (A/B)	19.59	37	16.83	31
2 (B/A)	15.14	67	21.00	60

5.3. Interpretation

Based on the results, it cannot be shown that the usage of LPL PPP UI does have clear and inherent advantages concerning the time required for informing oneself. Although it is not evident, the results of task 2 may indicate time advantages of the Privacy Icon Overview over the LPL PPP UI without it.

Considering the average score measurements, the LPL PPP UI with Privacy Icon Overview shows an advantage consistently. However, it must be acknowledged that the scores for task 1 are in general quite low (i.e. 31% and 37%). This could be caused by the task design (e.g. unclear instructions, which may have been better understood by the participant during task 2, resulting in a general better score). Overall, we interpret the results as positive and promising for further research.

6. CONCLUSION AND FUTURE WORKS

This paper presented an extension for the Layered Privacy Language (LPL) to support multi-lingual human-readable descriptions and privacy icons. Furthermore, the LPL Privacy Icons are introduced based on existing privacy policies and method descriptions. The Privacy Icon Overview has been introduced as a part of the LPL Personal Privacy Policy User Interface (LPL PPP UI) to give Data Subjects an overview on the processing of their data. Lastly, the Privacy Icon Overview has been evaluated according to the speed and accuracy of informing a Data Subject. The results are promising, but not reliable due to the extent of the experiments and should be checked launching a more extensive experiment. The results indicate that precision can be improved. But they do not show a clear advantage considering the speed of informing a user. We estimate that experiments with more tasks as well as more participants would create more reliable and significant results.

LPL, its framework, the LPL Privacy Icons and the LPL Personal Privacy Policy User Interface (LPL PPP UI) are elements in ongoing work. Further research has to be conducted, for which an outlook is provided. Privacy icons have to be developed and evaluated to be standardised for the GDPR. In terms of LPL PPP UI, further developments of the user interface are anticipated to enhance the usability of the user interface. For example the identification, presentation and interaction with elements for adjusting personal privacy elements have to be researched. To this end, we estimate especially the presentation of complex concepts, like anonymisation methods or privacy models, as challenging for the Data Subject. From this arise additional challenges considering special user groups, e.g. children, which have to be informed. Each of the mentioned developments must be evaluated considering higher participant counts as well as with more elaborate tasks to achieve significant, indicative, and decisive results.

7. ACKNOWLEDGEMENTS

Thanks and credit to Florian Prey and Sophie Voitleitner for supporting the creation of the LPL PPP UI and LPL Privacy Icons.

8. REFERENCES

[1] Gerl A., Bennani N., Kosch H., Brunie L. (2018) LPL, Towards a GDPR-Compliant Privacy Language: Formal Definition and Usage. LNCS Transactions on Large-Scale Data- and Knowledge-Centered Systems, XXXVII, The final authenticated publication will be available online on SpringerLink, https://link.springer.com/.

[2] European Parliament, Council of the European Union. (2016) 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) (Text with EEA relevance). Official Journal of the European Union, European Union.

[3] Tao, Y., Xiaokui, X. (2008) Personalized Privacy Preservation. Aggarwal, Charu C. Privacy-Preserving Data Mining: Models and Algorithms. Springer US, Boston, MA.

[4] Pettersson, J. S. (2015) A Brief Evaluation of Icons in the First Reading of the European Parliament on COM (2012) 0011. Privacy and Identity Management for the Future Internet in the Age of Globalisation, Privacy and Identity 2014, 125-135.

[5] Moskowitz, B., Raskin, A. (2011) Privacy Icons. https://wiki.mozilla.org/Privacy_Icons (01.06.2018).

[6] Mehldau, M. (2018) Iconset for Data-Privacy Declarations v0.1. Let's simple declare what data is how used, stored, given away or deleted. https://cdn.netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf (01.06.2018).

[7] Crano, L. F., Arjula, M., Gudrun, P. (2002) Use of a P3P user agent by early adopters. Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society, Washington, DC, USA, November 21, pages 1-10. ACM, New York, NY, USA.

[8] W. Reeder, R. (2008) Expandable Grids: A user interface visualization technique and a policy semantics to support fast, accurate security and privacy policy authoring. School of Computer Science Carnegie Mellon University Pittsburgh, Pennsylvania, USA.

[9] W. Reeder, R., Bauer, L., Bauer, L. F., K. Reiter, M., Bacon, K., How, K., Strong, H. (2008) Expandable grids for visualizing and authoring computer security policies. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy, April 5-10, pages 1473–1482. ACM, New York, NY, USA.

[10] Kelley, P.G., Cesca, L., Bresee, J., Cranor, L.F. (2010) Standardizing privacy notices: an online study of the nutrition label approach. Proceedings of the 28th International Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA, April 10-15, pages 1573-1582. ACM, New York, NY, USA.

[11] Kelley, P.G., Bresee, J., Cranor, L.F., W. Reeder, R. (2009) A "nutrition label" for privacy. Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), Mountain View, California, USA, July 15-17, pages 4:1-4:12. ACM, New York, NY, USA.

[12] Angulo, J., Fischer-Hübner, S., Pulls, T., Wästlund, E. (2011) Towards Usable Privacy Policy Display & Management for PrimeLife. 5th International Symposium on Human Aspects of Information Security and Assurance (HAISA), London, UK, July 7-8, pages 108–118, University of Plymouth, London, UK.

[13] Stiftung Datenschutz. (2013) New ways of providing consent in data protection - technical, legal and economic challenges. https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_PolicyPaper_New_ways_of_providing_consent_in_data_protection_EN_final.pdf (01.06.2018).

[14] Deutschland sicher im Netz e.V. (2016) DsiN-Sicherheitsindex 2016. https://www.sicher-imnetz.de/downloads/dsin-sicherheitsindex-2016 (01.06.2018).

[15] Shneiderman, B. (1996) The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations. IEEE Symposium on Visual Languages, Boulder, CO, USA, September 03 - 06, pages 336-343. IEEE Computer Society, Washington, DC, USA.

[16] Sweeney, L. (2002) k-Anonymity: A Model for Protecting Privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10, pages 557–570.