The Layered Privacy Language Art. 12 - 14 GDPR Extension – Privacy Enhancing User Interfaces

Armin Gerl[1], Bianca Meier[2]

Abstract: On 25th May 2018, the EU-wide General Data Protection Regulation (GDPR) came into force in order to strengthen the rights of Data Subjects. Although the GDPR specifies the required information, which has to be presented to a Data Subject, it can still be argued for a lack of transparency due to unfavorable presentation of the privacy policy. Furthermore, no systematic approach for the enforcement of privacy policies in technical systems is deployed. These issues are tackled by the both human- and machine-readable Layered Privacy Language (LPL), which models legal privacy policies. This work introduces an extension for LPL to comply with Art. 12 - 14 GDPR. Additionally, user interface prototypes will be introduced to allow the creation of LPL privacy policies by the Data Protection Officer as well as a structured presentation of the LPL privacy policy for web-applications.

Keywords:

GDPR; Informed Consent; Layered Privacy Language; Privacy Policy; Privacy Management

1 Introduction

Where personal data is collected or processed users (Data Subjects) have to be informed about it by the privacy policy. Although this document is essential and contains all legally required information, users often do not read the privacy policies [Bi15] [St16]. This behaviour has various reasons, for example complexity, legal language or the length of the privacy policy [An11a]. Thus, the presentation of the privacy policy has to be reconsidered. McDonald and Cranor analyzed the cost of reading privacy policies in their study. The result was the following: If every American internet user reads all privacy policies, which are displayed to him, the whole nation needs for reading 54 billion hours per year. Breaking down this sum, every American citizen would require 40 minutes every day reading privacy polices [MC08]. As a result of this great expenditure of time, many users agree/consent to privacy policies without any understanding. The GDPR, which intends to strengthen the rights of Data Subjects, e.g. by requiring free and informed consent [GD16, Art. 7], seems not to have any noticeable effect on this behaviour. To avoid unknown processing of personal data, the Data Subject has to understand the contents of the privacy policy, which is non-trivial. Due to the complexity of the GDPR and its definition of information that has to be provided to the Data Subject [GD16, Art. 12 - 14], also the creation of GDPR

[1] University of Passau, Chair of Distributed Information Systems, Passau, Germany armin.gerl@uni-passau.de
[2] University of Passau, Chair of Distributed Information Systems, Passau, Germany bianca.meier@uni-passau.de

doi:10.18420/inf2019_51

compliant privacy policies is challenging for the Controller, which can be supported by the Data Protection Officer (DPO). Because, no uniform approach of creating and handling is available, the management of privacy policies is a tedious and time-consuming task which may be individual for each DPO and Controller. Furthermore, this results in various structures, wordings and presentations of privacy policies hindering the understanding for the Data Subjects.

To tackle this challenge, we propose a systematic computer science approach to create and present privacy policies in a unified way utilizing the Layered Privacy Language (LPL). Based on LPL an overarching framework enables the privacy-preserving processing of personal data directly based on the decisions of the users. Therefore, users negotiate and agree/consent to a LPL privacy policy, which represents the individuals' privacy settings. This personalized privacy policy is considered for each processing, i.e. processing of personal data is restricted to specific purposes. Thus, the users' decisions on its privacy are directly influencing if and how its personal data is processed [Ge18b]. Furthermore, the human- and machine-readable LPL enables a systematic creation of privacy policies, which can be verified for completeness, and the structured presentation of privacy policies. To comply with the requirements for the contents of a privacy policy, LPL is extended according to Art. 12 - 14 GDPR [GP18a]. We detail how this LPL extension complies to the GDPR, such that legal privacy policies can be modelled.

The main contribution of this work consists of the introduction of the *LPL Policy Creator*, which intends to support the Controller with the creation and management of privacy policies. And the extension of the *LPL Policy Viewer*, presenting users the required information, based upon previous work [GP18b] [Ge18a] to comply with the GDPR requirements for privacy policies. As a result users can perceive standardized policies including all necessary information in a layered approach [Gr18]. The remaining of the paper is structured as follows. Section 2 reviews related work regarding other privacy languages and the visualizations of privacy policies. The extension of LPL to the Art. 12 - 14 of the GDPR is detailed in section 3. The *LPL Policy Creator* is introduced in section 4. Section 5 presents the updated *LPL Policy Viewer* for the presentation of the privacy policy to the user. Lastly, section 6 concludes this work and gives an outlook.

2 Related Work

Next to LPL other privacy languages have been proposed to enhance the privacy experience, which we will shortly describe and compare to, to show the strengths of LPL.

The *Privacy Preferences Project*, short P3P, is standardized by the the World Wide Web Consortium (W3C) [CAG02]. P3P intended to provide privacy policies in a standardized format and therefore enable automatic processing of them. Naturally, P3P does not consider GDPR, because it has been proposed before GDPR. P3P models privacy policies in XML, which then is provided by the website to the user via the browser. To model privacy policies a pre-defined vocabulary is used, which only allows for a restricted extent the modelling of real privacy policies, e.g. the vocabulary for purpose is fixed. In contrast LPL does not use a pre-defined vocabulary for its elements. To support the user with the decision if the provided P3P privacy policy complies with its personal privacy preferences the *A P3P Preference Exchange Language (APPEL)* is introduced [CAG02]. Processing both the personal privacy preferences of the user and the P3P privacy policy provided by the website, the browser plugin *Privacy Bird* [CGA06] visualizes the fulfillment of the users privacy preferences via an icon. Three different icons exist: A green bird, which tells the user, that his personal privacy settings are consistent with the privacy policy. A red bird indicates that they are not consistent. Lastly, a yellow bird indicates that the tool is unable to retrieve a privacy policy from the website. Thus, only a few indications are given to user, but no further information, interaction, or possibility for consent management are given.

The privacy language PrimeLife (PPL) [An11b] intends to handle access control and data usage at the same time. The newest guidelines of the GDPR will not be considered, because PPL was implemented before it. PPL comes with a user interface for the presentation and negotiation of privacy policies. To tackle the challenge that it is hard for the user to define its own privacy preferences, pre-configured levels of privacy are provided – 'Nearly Anonymous', 'Minimal Data' and 'Requested Data' – which can be chosen and changed by the user at any time [An11b]. To visualize the data processing, a dialog called *Send Data?* is proposed [An11b], which presents the user in a tabular visualization the collected data for each purpose. Additionally, data recipients are listed. The user interfaces enables the comparison to the users personal settings, but does not allow the negotiation of the content of the privacy policies. This is in contrast to LPL, which supports negotiation.

The *SPECIAL Project*, which was funded by European Union's Horizon 2020 research, proposes a GDPR compliant privacy dashboard [PRK17] based upon SPECIAL's Usage Policy Language [PB17]. The privacy dashboard provides a time-line consisting of each processing of data. Data items are divided in four groups: 'Data I provide', 'Data of me provided by others', 'Data of my behavior' and 'Inferred data about me'. This subdivision improves the transparency of data processing for the Data Subject. In addition to this time-line, the user interface informs about the privacy policy in a written way and third parties. It is important to notice, that the user can give/withdraw his consent to the processing for any purpose, which represents the negotiation of a privacy policy in LPL. Hereby, it is differentiated between required and non-required purposes. Required purposes have to be agreed upon by the user and are usually necessary for the service, thus they cannot be withdrawn from the privacy policy. On the other hand non-required purposes have to be consented to by the user.

3 LPL with Art. 12 - 14 Extension

LPL is intended to represent all privacy policy concerning processes including creation, negotiation, managing and enforcing of privacy policies [Ge18b]. Thus, LPL has to be presentable in a human-readable way that supports free and informed consent, while personalization of the privacy policy is encouraged. Furthermore, LPL enables the enforcement of the privacy policy due to policy-based access control and de-identification mechanisms. Therefore, data can only be processed by authenticated and authorized entities in a, if necessary, de-identified way. To achieve this personal anonymization, pseudonymization methods, and privacy models are integrated.

This work focuses on the creation and presentation of privacy policies in the context of Art. 12 - 14 GDPR, such that LPL policies can be used within the European legal framework. For the presentation of LPL privacy icon capabilities and human-readable headers and descriptions with internationalization support have been introduced [Ge18a] [GP18b]. Therefore, Art. 12 - 14 GDPR has been analyzed and requirements have been derived. Comparing the original version of LPL [Ge18b] against those requirements it was found that the basic policy structure is full-filled, but several informative requirements are missing for which an extension has been proposed [GP18a]. Furthermore, LPL has been extended by pseudonymization capabilities, which are necessary in health care scenarii [GB19]. Within this work we consider LPL with all mentioned extensions (see Fig. 1) to cover its full extent for creation and presentation. Therefore, we reconsider the requirements defined by Gerl and Pohl [GP18a] and compare them to the updated LPL in the following.

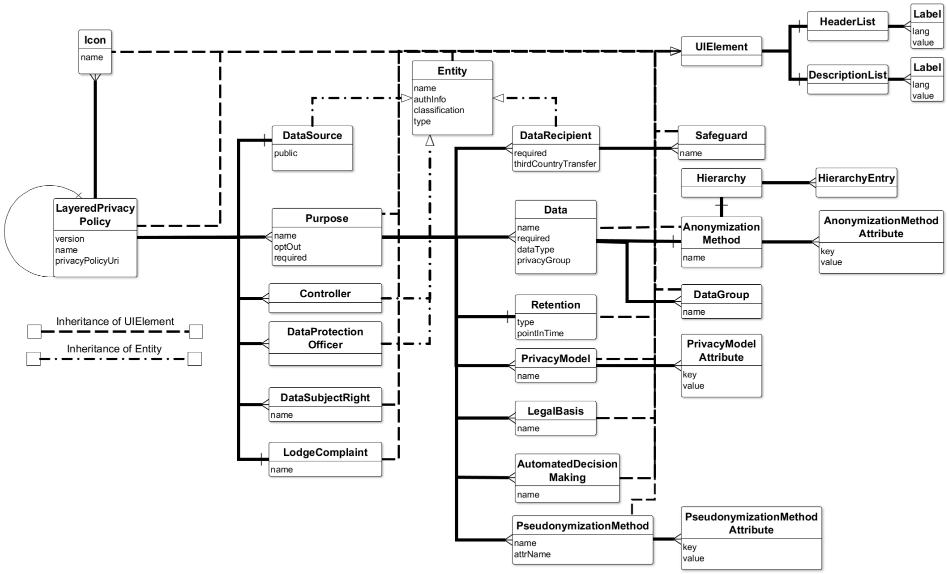


Fig. 1: The structure of the Layered Privacy Language [Ge18b] with the *User Interface Extension* [Ge18a], *Pseudonymization Extension* [GB19], and *Art. 12 - 14 GDPR Extension* [GP18a].

3.1 Comparison of LPL to Art. 12 - 14 GDPR Requirements

The main articles of the GDPR dealing with the requirements for privacy policies are Art. 12 - 14, which will be compared to the capabilities of LPL in the following (see Tab. 1).

In Art. 12 GDPR general provisions for the communication to the Data Subject, especially regarding transparency, are stated [GD16, Art. 12]. First of all it states that a privacy policy has to be provided in a clear and plain language [GD16, Art.12 (1) Sentence 1], which is enabled through the UIElement providing all key elements with human-readable headers and descriptions, which has been introduced in the *User Interface Extension* [Ge18a]. Furthermore, the privacy policy can be provided in a written or electronic form [GD16, Art.12 (1) Sentence 2], under which LPL falls as an electronic format. What cannot be covered by the LPL model itself is the realization of the Data Subject Rights [GD16, Art. 12 (2)], their response time [GD16, Art. 12 (3)], or the protection of the Controller from excessive Data Subject Rights requests [GD16, Art. 12 (5)], because this is concerning an overarching privacy framework using LPL. Realization of the semi-automatization of Data Subject Rights is hereby subject to future work. The last requirement derived of Art. 12 allows the usage of standardized icons [GD16, Art. 12 (7)], which are covered by LPL through the introduction of the Icon-element for privacy icons [Ge18a].

The following Art. 13 and Art. 14 have very similar content and will therefore be combined compared. Art. 13 describes the information that has to be provided where personal data are collected from the Data Subject [GD16, Art. 13] and Art. 14 describes the information that has to be provided before data is collected from the Data Subject [GD16, Art. 14]. Both articles demand that the identity of the Controller and its contact details are provided [GD16, Art. 13 (1)(a), Art. 14 (1)(a)], which is modelled in LPL as a set of Controller-elements to also consider Joint Controllers [GD16, Art. 26]. Furthermore, the contact details of the responsible DPO has to be provided [GD16, Art. 13 (1)(b), Art. 14 (1)(b)], which is covered by the DataProtectionOfficer-element of LPL. The purposes of the processing of personal data and their legal basis, including the legitimate interests [GD16, Art. 13 (1)(d), Art. 14 (2)(a)], have to be stated [GD16, Art. 13 (1)(c), Art. 14 (1)(c)], which LPL models a set of Purpose-elements each having a set of LegalBasis-elements. The Data Subject has to be informed about the collected data categories [GD16, Art. 14 (1)(d)] modelled by the DataGroup-element. The required personal data has to be communicated to the Data Subject [GD16, Art. 13(2)(e)], which is modelled by the Data-element having the required attribute. The data recipients for the personal data [GD16, Art. 13 (1)(e), Art. 14 (1)(e)], and if the data is transferred in a third country and the applied safeguards [GD16, Art. 13 (1)(f), Art. 14 (1)(f)] have to be provided, which is modelled by LPL as a set of DataRecipient-elements which have an attribute indicating a third country transfer and a set of Safeguard-elements if necessary. The storage period for the personal data has to be provided to the Data Subject [GD16, Art. 13(2)(a), Art. 14(2)(a)], which is modelled by the Retention-element of LPL. Furthermore, the Data Subject has to be informed about its Data Subject Rights [GD16, Art. 13(2)(b), Art. 14(2)(c)] and how to lodge a complaint [GD16, Art. 13(2)(d), Art. 14(2)(e)], which is implemented by the DataSubjectRights-element and LodgeComplaint-element globally for a policy. The Data Subject has to be informed if automated decision-making is performed based on the personal data [GD16, Art. 13(2)(f), Art. 14(2)(g)], which is modelled for each purpose by the AutomatedDecisionMaking-element. The Data Subject has further to be informed about the possibility to withdraw consent [GD16, Art. 13(2)(c). Art. 14(2)(d)], this is implicitly modelled in LPL by the required attribute for the Purpose-element that allows the user to (withdraw) consent to a purpose. This concept is further extended to the Data-element and DataRecipient-element allowing for several personalization options. Lastly, the Data Subject has to be informed about the source of personal data and if this source is publicly available [GD16, Art. 14(2)(f)], which is modelled b the DataSource-element with the public attribute denoting a public source.

Thus, LPL shows the capabilities to model all required information required by Art. 12 - 14 GDPR, whereas the implementation of the Data Subject Rights and their execution have to be considered by the overarching privacy framework utilizing LPL. It may be argued that the information stating that withdrawing consent is possible, may be modelled explicitly, but in LPL we consider personalization of the privacy policy as a feature that should cover this requirement and allow the user to influence its personal data ’from consent to processing’.

GDPR		**LPL**
Article	**Requirement**	**Implementation**
Art. 12(1) Sentence 1	Clear and Plain Language	UIElement
Art. 12(1) Sentence 2	Written or Electronic Information	LayeredPrivacyPolicy
Art. 12(2)	Data Subject Rights Realization	Framework
Art. 12(3)	Response Time	Framework
Art. 12(5)	Excessive Requests	Framework
Art. 12(7)	Standardized Icons	Icon
Art. 13(1)(a), Art. 14(1)(a)	Contact Details of Controller	Controller
Art. 13(1)(b), Art. 14(1)(b)	Contact Details of DPO	DataProtectionOfficer
Art. 13(1)(c), Art. 14(1)(c)	Purpose and Legal Basis	Purpose; LegalBasis
Art. 13(1)(d), Art. 14(2)(b)	Legitimate Interest	LegalBasis
Art. 14(1)(d)	Categories of Personal Data	DataGroup
Art. 13(1)(e), Art. 14(1)(e)	Recipients of Personal Data	DataRecipient
Art. 13(1)(f), Art. 14(1)(f)	Third Country Transfer	DataRecipient; Safeguard
Art. 13(2)(a), Art. 14(2)(a)	Storage Period	Retention
Art. 13(2)(b), Art. 14(2)(c)	Information: Data Subject Rights	DataSubjectRights
Art. 13(2)(c). Art. 14(2)(d)	Information: Withdraw Consent	Purpose
Art. 13(2)(d), Art. 14(2)(e)	Information: Lodge a Complaint	LodgeComplaint
Art. 13(2)(e)	Information: Required Data	Data.required
Art. 14(2)(f)	Source of Personal Data	DataSource
Art. 13(2)(f), Art. 14(2)(g)	Automated Decision-Making	AutomatedDecisionMaking

Tab. 1: Overview of the implementation of the legal requirements for privacy policies according to Art. 12 - 14 GDPR by the Layered Privacy Language.

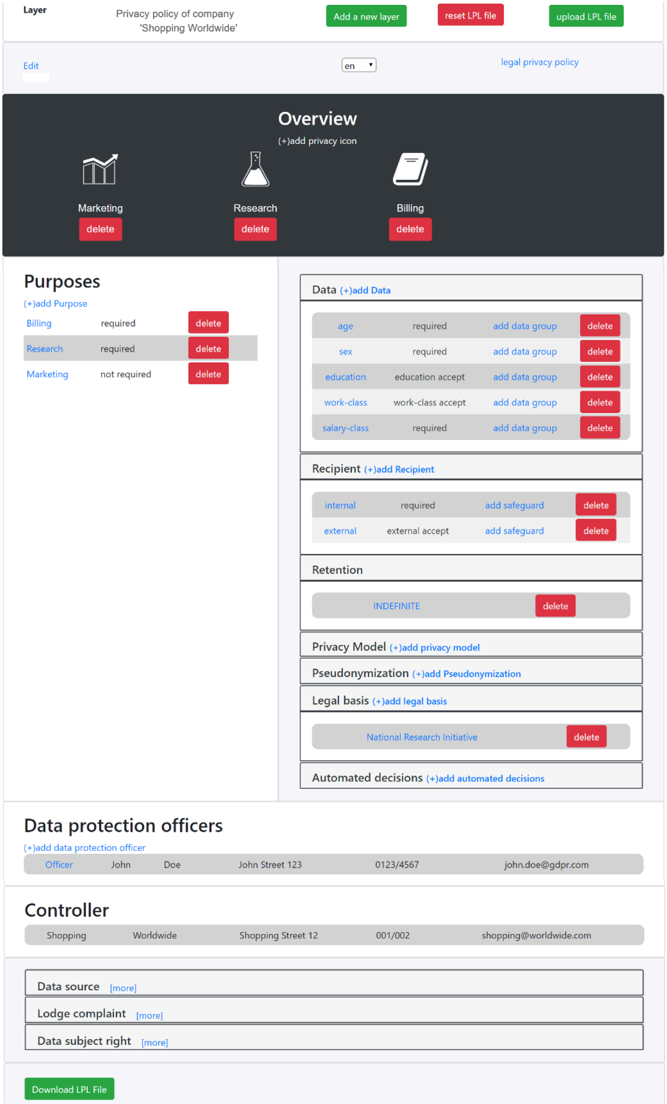
4 LPL Policy Creator

One of the tasks of the Controller is to create and manage privacy policies. Hereby, it can be a challenge to keep track of the fulfillment of all requirements given by the GDPR. The *LPL Policy Creator* is a prototype implementation, which supports the creation process for LPL privacy policies, while support for compliance with GDPR is given. For a better understanding we assume the following scenario.

The company 'Shopping Worldwide' operates a web shop. To comply with GDPR the company has to create a privacy notice according to Art. 13 and Art. 14 GDPR which will be integrated in the privacy policy to inform the users about the processing of their personal data. The company uses the collected data for the non-required purpose 'Marketing' and the required purposes 'Billing' and 'Research'. The later one requires the data 'sex', 'age' and 'salary-class' and the non-required data elements 'education' and 'work-class' belong to the last one. The collected data is processed by the data recipient 'internal', which is the company itself. The other data recipient, 'external', denotes that the data is analyzed by a third party (which should be denoted in detail for a real-life policy). The data recipient 'internal' is required, because the company itself has to process the data to provide the web shop. In contrast, the data recipient 'external' is non-required, such that the user has to actively consent to it. In this scenario we denote a fictional legal basis 'National Research Initiative' as the legal basis of the processing. Also a fictional retention with the deletion type 'INDEFINITE' was created. No de-identification (anonymization, pseudonymization, or privacy model) will be defined for this purpose, also no automated decision-making will be conducted. Further description of other purposes is omitted for the scope of this paper. These requirements can be modelled with the *LPL Policy Creator* using an interactive user interface (see Fig. 2). Individual elements are detailed in the following.

Header The *Header* provides three different functions: Add a new layer to the current privacy policy, reset the whole created privacy policy and the possibility to import a LPL privacy policy. Creating a new LPL policy layer enables further detailing or restriction of the policy, e.g. the user consented policy defines that data can be used for marketing, then an additional internal privacy policy layer can be added to further specify that only specific data is accessible by specific roles or departments within the company. Therefore, a LayeredPrivacyPolicy-element includes a set of UnderlyingPrivacyPolicies-elements, which are LayeredPrivacyPolicy-elements.

Policy Header The *Policy Header* is separated into general settings and the *Privacy Icon Overview* [Ge18a]. The general settings, accessed with the button 'Edit', allow to alter the language for international support. Additionally, a link (URL) to the regular legal privacy policy can be set, to comply with common practices. Also other elements of the policy can be set within the header, e.g. information about the Data Subject Rights or that the Data Subject can lodge a complaint. The *Privacy Icon Overview* enables the addition of privacy



Privacy policy of company 'Shopping Worldwide'

Purposes
(+)add Purpose

Billing	required	delete
Research	required	delete
Marketing	not required	delete

Data (+)add Data

age	required	add data group	delete
sex	required	add data group	delete
education	education accept	add data group	delete
work-class	work-class accept	add data group	delete
salary-class	required	add data group	delete

Recipient (+)add Recipient

internal	required	add safeguard	delete
external	external accept	add safeguard	delete

Retention

INDEFINITE	delete

Privacy Model (+)add privacy model

Pseudonymization (+)add Pseudonymization

Legal basis (+)add legal basis

National Research Initiative	delete

Automated decisions (+)add automated decisions

Data protection officers
(+)add data protection officer

Officer	John	Doe	John Street 123	0123/4567	john.doe@gdpr.com

Controller

Shopping	Worldwide	Shopping Street 12	001/002	shopping@worldwide.com

Data source [more]

Lodge complaint [more]

Data subject right [more]

Download LPL File

Fig. 2: *LPL Policy Creator* example creating a LPL privacy policy with the purposes ’Billing’, ’Research’, and ’Marketing’. The purpose ’Research’ is selected detailing further information on, e.g. the processed data, the data recipient, or retention. Furthermore, information on the Data Protection Officer, Controller, as well as required information for the Data Subject is presented.

icons [GD16, Art. 12(7)] to the privacy policy. These icons are intended to support the understanding of privacy policies by providing a quick overview over the processing of personal data [Ge18a]. The Controller is intended to select from a specified list of icons. Because no official privacy icons have been implemented, we use self-defined privacy icons as placeholders, until a European standard is in place. Based on the given scenario, icons for the purposes ’Research’ and ’Marketing’ would be specified (see Fig. 2).

Purpose Overview The *Purpose Overview* allows the management (create, update, delete) of purposes for the current privacy policy. The created purposes are listed, showing if they are required or not. For example the purpose ’Research’ is required and therefore a indicating text-field is shown. The non-required purpose ’Marketing’ is similarly denoted (see Fig. 2). For each purpose additional settings can be conducted by selecting it, e.g. adding a descriptive text for the purpose.

Purpose Detail For each purpose various information can or has to be provided. Therefore, for every purpose a set of data, set of data recipients, set of legal basis and retention has to be provided. Furthermore, pseudonymization and privacy models may optionally be defined, as well as information about automated decision-makings. Furthermore, for each data element an anonymization method can be defined, to allow for fine-grained de-identification rules, e.g. a postal-code may be anonymized for a marketing purpose using suppression. Both for data and data recipients it can be defined if they are required or optional, such that the user can decide on what data is processed for which purpose by whom. The data recipient can hereby be a company, department, role, or individual, while data represents the actual attribute, e.g. column of a table in a relational database. If a data recipient is not covered by the GDPR, e.g. a company in the USA, then safeguards have to be implemented and specified for the data recipient. Retention of data can be set as a fixed date, in relation of the ending of the purpose, or indefinitely. For privacy models, which define privacy guarantees for the whole data-set and not only a single record, common privacy models are supported, e.g. *k-Anonymity* [SS98] or *Differential Privacy* [Dw06]. Because the selection of the appropriate privacy model is non-trivial, we intend to support decision of with a questionnaire-based wizard in future works. Similarly, pseudonymization method can be defined to tokenize personal information like the name, e.g. hashing [Aa13].

General Information In the *General Information* section of the *LPL Policy Creator* common information on the privacy policy has to be created. This includes the contact details of the DPO or several DPOs iff applicable, the responsible Controller or a set of Controllers to allow for Joint Controllers [GD16, Art. 26], information on the data source i.e. the Data Subject after the acceptance of the privacy policy, and information on how to lodge a complaint as well as Data Subject Rights.

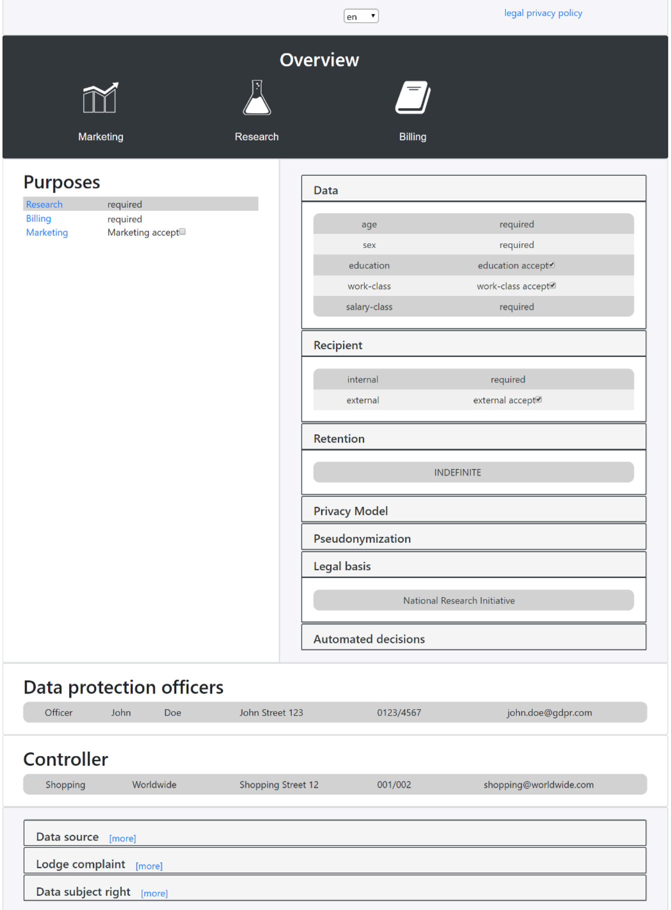
Footer After finishing the creation of a LPL privacy policy, it can be stored as a JSON or XML file, which allows for the integration in services using LPL and being presented by the *LPL Policy Viewer*. Furthermore, this functionality ensures the re-usability of privacy policies, which were created with the vocabulary of LPL.

5 LPL Policy Viewer

Next to the *LPL Policy Creator*, the first iteration of the *LPL Policy Viewer* [GP18b] with its Privacy Icon Overview [Ge18a] has been extended to incorporate all elements of the *LPL Art. 12 -14 GDPR Extension* as well as fine-grained consent management [GMB19]. The *LPL Policy Viewer* is hereby intended to give the user a fast overview over the processing of its personal data, while all necessary information is provided due to *layering*. In order to make the information even more comprehensible, the Visual Information Seeking Approach (VISA) – Overview first, zoom and filter, details on demand – is applied [Sh96]. Furthermore, the user is enabled to personalize the privacy policy by consenting to non-required elements i.e. purpose, data and data recipient. Further support for influencing the anonymization settings is anticipated for future work.

The initial concept of the *LPL Policy Viewer*, which consists of an overview over the purposes of the processing of the personal data both using privacy icons and an purpose overview, has not been altered. Only after interacting with the *LPL Policy Viewer* additional information is revealed. This is implemented by the so-called 'information overload' for the user, therefore it is important for the user to prepare the information in such a way that he can quickly and easily find relevant details without explicitly searching for them [MMG02]. This is especially important, because privacy policies are in general complex, such that the abstraction without loss of required information is essential.

Compared to the *LPL Policy Creator* the *LPL Policy Viewer* is structured similarly, but it lacks the functionality to create new elements, e.g. purposes, for the policy. Instead, it first presents the user with an overview of the privacy policy, then allows for browsing for specific information, e.g. the data recipient for personal data of a specific purpose or information on how to lodge a complaint. Due to the extension of LPL all required information according to Art. 12 - 14 GDPR is provided. But it should be noted that for Art. 13(2)(c) and Art. 14(2)(d) GDPR, which specify that the Data Subject has to be informed about his right to withdraw consent if the legal basis of processing was consent, is implemented implicitly by the *LPL Policy Viewer*. The user is informed to be able to withdraw consent using check-boxes next to the purpose, data or data recipient element, which is only possible for elements that have the 'required' attribute set to 'false'. This enables the user to personalize its privacy policy at any time, but the personalization does not only affect the privacy policy but also the corresponding business processes due to the machine-readability of LPL. Thus, the withdrawal of consent to specific data fields removes them also from being processed for the specific purpose, which allows personalized applications. Furthermore, the user can



Purposes

Research	required
Billing	required
Marketing	Marketing accept☐

Data

age	required
sex	required
education	education accept☑
work-class	work-class accept☑
salary-class	required

Recipient

internal	required
external	external accept☑

Retention

INDEFINITE

Privacy Model

Pseudonymization

Legal basis

National Research Initiative

Automated decisions

Data protection officers

Officer	John	Doe	John Street 123	0123/4567	john.doe@gdpr.com

Controller

Shopping	Worldwide	Shopping Street 12	001/002	shopping@worldwide.com

Data source [more]

Lodge complaint [more]

Data subject right [more]

Fig. 3: Example for the LPL Policy Viewer

experience notable changes to the application [GMB19], which may give certainty that personal data is processed only according to its personal privacy policy.

In the following, we will describe the features provided by the *LPL Policy Viewer* based on the previously detailed example scenario (see Fig. 3). Due to the same base structure as the *LPL Policy Creator*, we will only highlight features that are essential for the presentation and negotiation of the privacy policy in the following.

Policy Header The *Policy Header* the user is presented the *Privacy Icon Overiew* [Ge18a], displaying individual icons for the purposes ’Marketing’, ’Research’, and ’Billing’ giving the user an overview over the processing of its personal data ’at a glance’. Assuming standardized privacy icons will be introduced, the GDPR stating that privacy icons may be provided in combination with the remaining privacy policy information, will be fulfilled [GD16, Recital 60]. Furthermore, the *Policy Header* provides the user with the capability to change the language of the privacy policy allowing for internationalization support. Lastly, the link for the legal privacy policy is provided to comply with the current state-of-the-art representation of privacy policies.

Purpose Overview On the left side of the user interface the *Purpose Overview* is located giving the user a textual list of the purposes for the processing of personal data. For each purpose it is indicated whether it is required and therefore necessary to agreed upon, or optionally accepted via interacting with the provided check-box. To comply with GDPR, the withdrawal of consent is as easy as giving it by clicking on the check-box [GD16, Art. 7(3) Sentence 3]. Clicking on the name of the purpose, e.g. 'Research', its details are given within the *Purpose Detail* section of the user interface. This interaction corresponds to the *Visual Information Seeking Approach* denoting that further details should be given on-demand after filtering [Sh96].

Purpose Detail Depending on the selected purpose additional information is shown within the *Purpose Detail*. Thus the user gets informed about which of its personal data is processed by which data recipients, when the data is deleted, if the data is protected by any de-identification techniques, and if any automated decision-makings are conducted for the specific purpose. Furthermore, the user can withdraw its consent to specific data or the processing by specific data recipients, iff they are not required. Given our example scenario, the data fields 'education' and 'work-class' are not required as well as the data recipient 'external', therefore consent can be withdrawn by interacting with the check-box (see Fig. 3).

General Information Lastly, in the *General Information* section of the user interface, the remaining required information regarding Art. 12 - 14 GDPR is represented, which has been missing in the first iteration of the user interface. The responsible DPO and Controller are hereby prominently presented, while information on Data Subject Rights or how to lodge are complained are accessible after interaction with the corresponding element. The reasoning behind this is, that the user should be aware of the Controller and the responsible Data Protection Office and their contact details before additional actions are taken, e.g. making use of a Data Subject Right.

6 Conclusion and Future Work

This work compared the current implementation of the Layered Privacy Language (LPL) with all its extension to the requirements given by in Art. 12 -14 GDPR for privacy policies demonstrating full coverage. To demonstrate the coverage of the extension of LPL we introduced the *LPL Policy Creator* to support companies in the creation of privacy policies. Additionally, we extended *LPL Policy Viewer* to incorporate the extensions of LPL, allowing for a concise presentation of the privacy policy utilizing privacy icons and several interaction possibilities to enable fine-grained consent management.

Future works will extend the consent management pattern to incorporate the influence of anonymization properties for the Data Subject, as well as supporting with the selection of suitable de-identification methods. Also other user groups like children or elderly people have to be considered for future user interface concepts. Furthermore, the realization of Data Subject Rights as an semi-automated system utilizing LPL is subject of research, such that only minimal required actions from the DPO are necessary to respond. The goal is hereby to create a holistic approach to handle privacy intra and inter Controllers, while privacy guarantees can be given for Data Subjects.

Bibliography

[Aa13] Aamot, Harald; Kohl, Christian Dominik; Richter, Daniela; Knaup-Gregori, Petra: Pseudonymization of patient identifiers for translational research. BMC Medical Informatics and Decision Making, 13(1):75, Jul 2013.

[An11a] Angulo, J.; Fischer-Hübner, S.; Pulls, T.; Wästlund, E.: Towards usable privacy policy display & management-The primelife approach. In: Proceedings of the 5th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2011. pp. 108–118, 2011.

[An11b] Angulo, Julio; Fischer-Hübner, Simone; Pulls, Tobias; König, Ulrich: HCI for Policy Display and Administration. In (Camenisch, Jan; Fischer-Hübner, Simone; Rannenberg, Kai, eds): Privacy and Identity Management for Life. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 261–277, 2011.

[Bi15] Bitkom: , Stimmen Sie den Aussagen voll / eher zu? Datenschutzerklärungen... `https://de.statista.com/statistik/daten/studie/467075/umfrage/beurteilung-der-datenschutzerklaerungen-von-online-diensten-in-deutschland/`, 2015.

[CAG02] Cranor, Lorrie Faith; Arjula, Manjula; Guduru, Praveen: Use of a P3P User Agent by Early Adopters. In: Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society. WPES '02, ACM, New York, NY, USA, pp. 1–10, 2002.

[CGA06] Cranor, Lorrie Faith; Guduru, Praveen; Arjula, Manjula: User Interfaces for Privacy Agents. ACM Trans. Comput.-Hum. Interact., 13(2):135–178, June 2006.

[Dw06] Dwork, Cynthia: Differential Privacy. In (Bugliesi, Michele; Preneel, Bart; Sassone, Vladimiro; Wegener, Ingo, eds): Automata, Languages and Programming. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–12, 2006.

[GB19] Gerl, Armin; Bölz, Felix: Layered Privacy Language (LPL) Pseudonymization Extension for Health Care. In: Proceedings of MedInfo 2019. 2019.

[GD16] GDPR: , General Data Protection Regulation, April 2016. Regulation (EU) 2016 of the European Parliament and of the Council of 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.

[Ge18a] Gerl, Armin: Extending Layered Privacy Language to Support Privacy Icons for a Personal Privacy Policy User Interface. In: Proceedings of Brithish HCI 2018. BCS Learning and Development Ltd., Belfast, UK, p. 5, 2018.

[Ge18b] Gerl, Armin; Bennani, Nadia; Kosch, Harald; Brunie, Lionel: LPL, Towards a GDPR-Compliant Privacy Language: Formal Definition and Usage. In (Hameurlain, Abdelkader; Wagner, Roland, eds): Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVII. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 41–80, 2018.

[GMB19] Gerl, Armin; Meier, Bianca; Becher, Stefan: Let Users Control their Data – Privacy Policy-based User Interface Design. In: Human Interaction and Emerging Technologies 2019 - Proceedings of the 1st International Conference on Human Interaction and Emerging Technologies (IHIET 2019) conference. Université Côte d'Azur, Nice, France, August 2019.

[GP18a] Gerl, Armin; Pohl, Dirk: Critical Analysis of LPL according to Articles 12 - 14 of the GDPR. In: Proceedings of International Conference on Availability, Reliability and Security. ARES 2018, Hamburg, Germany, p. 9, August 2018.

[GP18b] Gerl, Armin; Prey, Florian: LPL Personal Privacy Policy User Interface: Design and Evaluation. In: Mensch und Computer 2018 - Tagungsband. Gesellschaft für Informatik e.V., Bonn, 2018.

[Gr18] Greger, Sebastian: , User-centred transparency design for privacy – Part I: The layered approach. https://sebastiangreger.net/2018/08/user-centred-transparency-design-the-layered-approach/, August 2018.

[MC08] McDonald, A. M.; Cranor, L. F.: The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, 4, 2008.

[MMG02] Melgoza, Pauline; Mennel, Pamela A.; Gyeszly, Suzanne D.: Information overload. Collection Building, 21(1):32–43, 2002.

[PB17] P.A. Bonatti, S. Kirrane, I. Petrova L. Sauro E. Schlehahn: Deliverable D2.1 - Policy Language V1. Technical report, Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance - SPECIAL, December 2017.

[PRK17] Philip Raschke, Axel Küpper, Olha Drozd; Kirrane, Sabrina: Designing a GDPR-compliant and Usable Privacy Dashboard. In: IFIP Advances in Information and Communication Technology. IFIP Summer School 2017, Springer, September 2017.

[Sh96] Shneiderman, B.: The eyes have it: a task by data type taxonomy for information visualizations. In: Proceedings 1996 IEEE Symposium on Visual Languages. pp. 336–343, Sep. 1996.

[SS98] Samarati, Pierangela; Sweeney, Latanya: Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical report, technical report, SRI International, 1998.

[St16] Steinfeld, Nili: "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. Computers in Human Behavior, 55:992–1000, 2016.