Critical Analysis of LPL according to Articles 12 - 14 of the GDPR

Armin Gerl
University of Passau
Passau, Germany 94032
armin.gerl@uni-passau.de

Dirk Pohl
University of Passau
Passau, Germany 94032
dirk.pohl@uni-passau.de

ABSTRACT
On the 25th May 2018 the General Data Protection Regulation (GDPR) will enter into force implying new challenges to both legal and computer sciences. The Layered Privacy Language (LPL) is intended to model privacy policies to enforce policy-based, privacy-preserving processing. In this paper, we identify requirements for privacy policies based on Art. 12 - 14 of the GDPR, analyze LPL according to the derived requirements, and propose improvements for LPL accordingly.

CCS CONCEPTS
• Security and privacy  →  Domain-specific security and privacy architectures; Privacy protections; Social and professional topics  →  Privacy policies;

KEYWORDS
GDPR, LPL, Privacy Language, Privacy Policy, Privacy-Preservation

ACM Reference format:
DOI: 10.1145/3230833.3233267

1 INTRODUCTION
The General Data Protection Regulation (GDPR) [18] enters into force on 25th May 2018 (Art. 99 No. 2 GDPR). The GDPR is designed to harmonize data privacy laws across the European Union, to protect and empower all Data Subjects to ensure their data privacy and alter the way Controllers approach data privacy. Hereby, it emphasizes Privacy by Design and Privacy by Default, especially to protect Data Subject Rights.

This work critically assesses the Layered Privacy Language (LPL), which has the goal of modeling GDPR-compliant privacy policies. The LPL privacy policies are presented to Data Subjects either to fulfill the legal requirements for an informed and free consent (Art. 7 GDPR) or to provide the mandatory information in case another legal basis for data processing is available. Accepted privacy policies will be stored additional to the personal data. An overarching privacy framework enforces policy-based privacy-preserving processing utilizing anonymization methods and privacy models [7] [6].

Because a comprehensive analysis of LPL according to the complete GDPR is out of scope of this paper, we focus on Art. 12 - 14 GDPR. These denote some of the modalities of the execution of the Data Subject Rights (Art. 12 GDPR) and the information that has to be provided where personal data has been collected directly from the Data Subject (Art. 13 GDPR) or from other sources (Art. 14 GDPR). This focus has been chosen because these articles represent the information that has to be contained in a privacy language (or data model) representing a privacy policy. A privacy language or a data model aimed at representing a GDPR-compliant privacy policy should fulfill those requirements. Therefore, an in-depth analysis of Art. 12 - 14 GDPR to derive requirements for a machine-readable privacy policy will be conducted. The main contributions of this paper are:

• Identification of technical requirements based on Art. 12 - 14 GDPR
• Analysis of LPL according to the derived technical requirements
• Proposal of improvements for LPL

The remainder of the paper is structured as follows. Section 2 describes related works on privacy languages. Section 3 describes the legal requirements given by the GDPR. Section 4 denotes the concept, life-cycle and elements and attributes of LPL. Section 5 compares the retrieved requirements against the capabilities of LPL. Section 6 proposes improvements on LPL. Section 7 concludes the paper and presents future works.

2 RELATED WORK
In the following, we will give an overview of privacy languages that, unlike LPL, could not or did not consider the legal requirements of the GDPR. The intended purpose of the following privacy languages will be outlined to differentiate them from LPL.

Platform for Privacy Preferences (P3P) is a W3C Recommendation for describing privacy settings for websites and can be seen as the predecessor of most other privacy languages. Websites implementing P3P make their privacy policies explicit for the user. In combination with A P3P Preference Exchange Language (APPEL) it allows users to identify websites in compliance with their personal privacy preferences in a user friendly way. P3P has several shortcomings including missing semantics [24] [14] or missing definitions for anonymized data [12]. Naturally, P3P does not consider legal requirements of the GDPR, because it was developed earlier.

Primelife Policy Language (PPL) is an extension of XACML [5] defining policies on the usage of personal data of the Data Subject by the Controller. PPL deals with enforcing obligations, user privacy
preferences and trustworthiness [1]. PPL claims to consider the legal requirements in Europe. But because the proposal of the GDPR was released in 2012 [3], and the project had already ended in 2011 [20], the GDPR could not have been considered.

Purpose-to-Use (P2U) is designed for secondary user data sharing, which is denoted as unintended processing or trading of data by Third Party Controllers. It assumes that Data Subjects want to share their data via social networks or Web 2.0 technologies. Policy negotiation (of retention period, price, and type of data) allows the Data Subject to influence the processing conditions. Introduction of new purposes in the privacy policies is considered to support personalized services [11]. A framework for privacy-aware user data trading, describing the policy negotiation and user compensation for data sharing, is shown [10]. P2U does not explicitly claim to consider legal requirements of the GDPR nor another legal basis.

3 LEGAL REQUIREMENTS OF THE GDPR

The GDPR stipulates a complicated and complex scheme of rules regarding the automated processing of data. [4, for an complete account in English ] This paper can only focus on some of the rules as contained mainly in Art. 12-14 GDPR. However, to understand those rules a short overview of other concepts of the GDPR is necessary.

While the GDPR is new and presents new challenges for any Controller, some of the main concepts where already well known under the the old regime of the Directive 95/46/EC [17]. Taking into account the advancement of digitalization in all areas of life, it may seem implausible, but the general rule within European Data Protection Law remains the same: Processing in general is forbidden, unless there is a lawful ground (Art. 6 GDPR). All data processing has not only to adhere to the more detailed rules found at various places within the GDPR, but always has to general principles of processing into account (Art. 5 GDPR).

Compliance with the rules of the GDPR – as with any legal regime – is crucial, especially for data-driven businesses. Furthermore, a Controller must be able to demonstrate such compliance in case of complaints, investigations or data breaches. Otherwise he may be held accountable (Art. 5(2) GDPR), which may lead to administrative fines (Art. 83 GDPR) or other means of compensation (Art. 84 GDPR). Proof of the adequate provision of information to the Data Subject is a particularly important topic when it comes to processing based on consent (Art. 7(1) GDPR).

3.1 Preparatory Work

While Art. 12-14 GDPR may regard the first direct contact between the Controller and the Data Subject as far as the processing of data is concerned, the Controller is obliged under other rules of the GDPR to take several steps before this may happen. Many of them are interconnected with the informational duties as stipulated in Art. 12-14 GDPR.

The GDPR is deemed to be ‘technology-neutral’ and shall apply to very different branches of data processing aiming at small companies as well as global players. Naturally with broad and wide provisions instead of carefully drafted and detailed rules for each specific processing purpose, many decisions about processing have ultimately to be prepared and made by the Controller. Most measures to be taken under the GDPR are dependent on the interests of the parties involved. This shall take into consideration that not any kind of data processing has the same potential consequences for the Data Subject and after all not any Controller can be held to the same high standard without severe consequences to some business models.

This regulatory approach requires a Controller to gather a huge amount of information about his potential duties before processing of data even starts[2]. Some of these information gathering is formalized by rules in the GDPR. The Controller or his Data Protection Officer has to get an overview of the most important legal frameworks – European and in his respective Member-State. He has to identify the main actors involved – Controllers, Processors, the Data Subject and the responsible Supervisory Authority. The Working Papers agreed upon by the Supervisory Authorities, provide helpful guidance in this regard [9, on transparency]. Each Controller has to maintain a record of his processing activities (Art. 30(1) GDPR), which, as opposed to the informations to be provided under Art. 12-14 GDPR is – at first – a purely internal document. Additionally, where there is the likelihood of a high risk to the rights and freedoms of natural persons when processing data, the Controller has to undertake a so-called ‘Data protection impact assessment’ (Art. 35 GDPR). Of course, whether this has to be done, or not, has to be assessed for any of the processing activities. Apart from these mandatory steps the GDPR contains rules for other optional instruments like Codes of Conduct (Art. 40 GDPR), Certification (Art. 42 GDPR) and Binding Corporate Rules (Art. 47 GDPR) that should be considered, but may not be explained in detail.

3.2 Privacy Languages from a Legal Perspective

At this point it has to be emphasized that the GDPR does not require any Controller to implement a privacy languages or similar concepts. Still, it seems to be a step worthy of careful consideration.

Many of the legal information needed to implement a privacy language concept are already available once the Controller has done its’ mandatory preparation (see section 3.1). Furthermore, as will be shown in the analysis of Art. 12-14 GDPR below, much of this information have to be provided to the Data Subject anyway, so a privacy language in combination with a well-designed user interface may in future become a best practice. Additionally, a privacy language may provide a helpful tool guiding the Controller through the complex process of creating a GDPR-compliant system, while furthermore – if carefully designed – make the Controller able to demonstrate compliance when necessary: Processing, consent, and information transfer can be logged, the logs may be used as evidence for compliance with the rules. A structured technical system is the best way to ensure that the Data Subject may access all the necessary information not only at the start of the processing but at any time in the future.

To conclude, a privacy language, like LPL, may become a powerful element to connect the preparatory steps at the beginning of setting up a GDPR-compliant system with the multiple informational duties towards the Data Subject during the whole life-cycle of Processing. It can aid the fulfillment of the other duties towards the Data Subject (Art. 15-22 GDPR) and helps to avoid liability and
fines by establishing evidence if needed. While on the one hand, some new efforts are needed to implement LPL, it on the other hand utilizes informational resources that have to be created anyway.

3.3 Transparency under the GDPR

Art. 12 GDPR states several general transparency requirements as well as procedural and requirements applicable to the rights of the Data Subject as contained in Art. 13 ff. GDPR [22, P. 105 ff.].

The duties contained in Art. 13 and 14 GDPR are to be fulfilled by the Controller without any request by the Data Subject. The information have to be concise, transparent, intelligible and in an easily accessible form, using clear and plain language. Art. 7 GDPR contains some additional requirements when the legal basis for processing is the consent of the Data Subject.

Some of those requirements are easily met by technical devices. Once concise information is saved it does not require any special effort from a technical perspective. Other requirements are particularly challenging and may not be met by a technical solution alone.

Transparent, intelligible information in a clear and plain language are essentially human categories. They are focusing on the understanding of the provided information by the individual. Based on objective factors as viewed from the position of the average Data Subject, the information has to meet the above requirements. The GDPR does not only set formal requirements as to which information has to be provided. The functional understanding of information in the GDPR requires the person to be informed. Thus, the requirements may change with the targeted audience. It may require several language versions of information to be presented to the Data Subject in his mother tongue or at least a familiar language; generally, complex sentences and language structures are to be avoided. Texts should not be so vague as to allow different interpretations. At the end it should be transparent to natural persons that personal data concerning them are collected, used, consulted otherwise processed and to what extent personal data are and will be processed (Recital 39 to the GDPR). Technical information has to be phrased in a way that the average Data Subject may gain a understanding of the processes. Children as a target audience may make this task even more difficult as it must be understandable to them. This conditions cannot be emphasized enough when it comes to informed consent (Art. 7(2) GDPR): If a Controller does not inform in a compliant way about any of the other legal reasons for processing, he obviously is in breach of his informational duties. However, the processing itself still remains lawful. But when consent was not informed, it is no legal basis of processing which may be considered a far more severe breach than a simple breach of informational duties alone.

At this point it should be clear that the GDPR requires more than mere lists of technical Information or endless legal texts, but a carefully considered approach not only involving Computer- and Legal scientists, but communication specialists. Information overflow is to be avoided, the understanding of the average data subject to be taken into account. Concise while also easily understandable information may be conflicting goals which require careful considerations when drafting a data policy.

4 LAYERED PRIVACY LANGUAGE

In the following we will give an overview on the general concept of LPL and describe the present elements and attributes shortly as shown by Gerl et al. [7]. The extension of LPL [6] is hereby considered.

4.1 Concept

The concept of LPL is to create a privacy language that models privacy policies (see Figure 1). Assuming a (web-) service of a Controller, the LPL privacy policy will be presented to the Data Subject. The Data Subject can inspect and in some cases alter the LPL privacy policy, e.g. accept/deny purposes or altering the settings for anonymization. By submitting the form, the Data Subject accepts or consents to the privacy policy, which then itself will be processed and stored with the data. Access to the data will only be granted through a Privacy Layer that verifies whether the requester has the rights to access the data for the intended purpose according to the LPL privacy policy. If necessary the data will be anonymized. This is done for each request of the Controller, but also for requests by Third Party Controllers. Furthermore, if the Controller transfers data to a Third Party Controller, the LPL privacy policy will be extended by additional policies ‘on-top’ agreed upon by the Controller and Third Party Controller.

4.2 Life-Cycle

To give a more detailed understanding of LPL the 6 steps of the LPL life-cycle (see Figure 2) will be described in the following.

Creation. During the Creation step, the responsible privacy officer creates a raw LPL privacy policy. This privacy policy contains the purposes of the data processing but not any information about the Data Subject. This reflects the Preparatory Work as described in section 3.1.

Negotiation. During the Negotiation step, the raw LPL privacy policy is presented to the Data Subject. Personalization of the privacy policy is possible. Eventually, the Data Subject decides to give accept or give consent to the personalized privacy policy.

Pre-Processing. Assuming the Data Subject accepted or gave consent to the personalized privacy policy, it will be validated as well as information about the Data Subject and its personal data added.

Storage. The validated personal privacy policy will be stored along with the regular data for each Data Subject.

Transfer. When data transfer to a third party was accepted and data are transmitted to a third party, an additional privacy policy can be added to the existing privacy policy. Hereby, it has to be verified that the added privacy policy is at least as strict as the underlying privacy policy, which prevents any conflicts in the
4.3 Privacy Language Elements and Attributes

For the description of the elements and attributes we consider LPL with its user interface extension (see Figure 3) [6].

UIElement. The UIElement is an element that, by itself, will not be used within the privacy policy, but is used to inherit human-readability to other elements. The elements LayeredPrivacyPolicy, Icon, Entity (DataSource and DataRecipient), Purpose, Retention, PrivacyModel, Data and AnonymizationMethod inherit from UIElement. It contains both a HeaderList and DescriptionList each containing a set of Label elements. A Label element consists of the attributes lang, describing the language (e.g. 'en' for English), and value for the human-readable text (e.g. 'Hello World!').

LayeredPrivacyPolicy. The LayeredPrivacyPolicy is the root element of LPL. The attributes version, name and privacyPolicyUri are contained. Hereby, version defines the version of LPL, name is a unique identifier for the privacy policy, and privacyPolicyUri represents a link to a regular privacy policy. This element contains a set of Icon elements, a set of Purpose elements, a DataSource element and a UnderlyingPrivacyPolicy. The UnderlyingPrivacyPolicy is a LayeredPrivacyPolicy that has been agreed on before.

Icon. The Icon element is used to denote privacy icons, that are displayed to the Data Subject as an abstract privacy policy. The various privacy icons will be hereby set and identified by the attribute name.

Entity. The Entity element describes DataSubjects and Controllers (including roles as well as individuals) that have a processing-right on the data. It has the attributes name, classification, authInfo and type. Hereby, name identifies the entity and is used for access control, classification distinguishes between 'Person' or 'LegalEntity', authInfo is used for authentication, and type distinguishes a Entity between 'DataSource' and 'DataRecipient', which both inherit from Entity. The DataSource denotes the current owner of the data, which can be a Data Subject from which the data origins or a Controller storing the data (having an previous privacy policy agreement with the Data Subject). The DataRecipient represents the authority that gets specific processing-rights granted.

Purpose. The Purpose element describes the processing purpose. It has the attributes name, optOut and required. Hereby, name identifies the purpose, optOut defines if the Data Subject has to actively deny this purpose or consent to it, and required defines if the purpose to be accepted by the Data Subject. A Data Subject not consenting to a required purpose cannot accept the whole privacy policy. Furthermore, the Purpose contains a set of DataRecipient elements, a set of Data elements, a set of PrivacyModel elements, as well as a Retention element.

Retention. The Retention element describes the moment when the data has to be deleted of the corresponding Purpose. It has the attributes type and pointInTime. Hereby, type describes the condition ('Indefinite', 'AfterPurpose' or 'FixedDate'), and pointInTime details the retention.

PrivacyModel. The PrivacyModel element describes the privacy properties of the data-set. Several privacy models have been researched and can hereby be defined on the data, e.g. k-Anonymity [23], f-Diversity [15] or t-Closeness [13], defining the properties a data-set must have to prevent re-identification. The attribute name hereby defines the privacy model (e.g. k-Anonymity), whereas a set of PrivacyModelAttribute elements defines the properties of the privacy model. Therefore, a key and value pair is used (e.g. ('k', '3')).

Data. The Data element represents one data field. It has the attributes name, dataGroup, dataType, required and privacyGroup. Hereby, name defines a data (e.g. column in a relational database) uniquely, dataGroup is a representation of a logical data group (e.g. 'location data'), dataType defines the type of data (e.g. 'Text' or 'Date'), required defining if the data has to be accepted or can be dissented by the Data Subject, and privacyGroup classifying the data as Explicit, Quasi-Identifier (QID), Sensitive or Non-Sensitive and thereby how the data will be treated by the privacy model [23]. Furthermore, the Data element contains a AnonymizationMethod element.

AnonymizationMethod. The AnonymizationMethod element represents the anonymization that is applied on the data. It has the attribute name specifying the anonymization method (e.g. Suppression or Generalization). Furthermore, the AnonymizationMethod
element contains a set of AnonymizationMethodAttribute elements and a Hierarchy element. The AnonymizationMethodAttribute has two purposes. On the one hand it specifies the parameters for the anonymization method. On the other hand a ‘MinimumLevel’ and ‘MaximumLevel’ of anonymization can be defined, whereas the maximum will be set during the Creation through the privacy officer and the minimum may be influenced by the Data Subject during the Negotiation. Therefore, the attributes key and value are utilized.

Hierarchy. The Hierarchy element defines all possible (anonymized) values for the data field, utilizing an ordered set of HierarchyEntry elements. The values are pre-calculated to allow a performance benefit during the query-based anonymization. Both the ‘MinimumLevel’ and ‘MaximumLevel’ reference a HierarchyEntry element.

5 LEGAL ANALYSIS

In the following we will compare the requirements of Article 12 - 14 GDPR to the capabilities of LPL (see Table 1).

In Art. 12(1) Sentence 1 GDPR states that a clear and plain language is used to achieve transparency. Although this cannot be directly achieved by LPL, because it does not verify it, the UIElement of LPL is intended to provide a human-readable description text for the Data Subject. Because, the UIElement is inherited by several other elements of LPL, the information will be structured and therefore should allow better readability.

The requirement of Art. 12(2) Sentence 2 GDPR, that information should be written or electronic, is therefore also fulfilled by the general concept of a machine-readable privacy language. Additionally, it is possible to reference a regular written privacy policy via the privacyPolicyURI of the LayeredPrivacyPolicy element.

Art. 12(2) GDPR defines that the Data Subject Rights have to be provided by the Controller. This is interpreted by the privacy framework overarching LPL as Regulated Purposes, which are intended to be processed automatically. Currently no proof-of-concept implementation is available to verify the functionality. But an automatic enforcement of the Data Subject Rights should decrease the overall response time, so that it is well within the time period of one month required by the GDPR (Art. 12(2)). Additionally, to fulfill the requirement under Art. 12(5) GDPR is has to be considered what excessive requests are if the requests can be processed automatically. On the one hand, technical solutions could be implemented within the privacy framework, namely a Data Subject specific counter for requests that rejects requests if a specific threshold is exceeded. On the other hand, it may be argued that such a restriction may be obsolete if requests may be processed automatically and just basic security features should be implemented to counteract threads like brute-force attacks.

Art. 12(7) GDPR proposals to represent the necessary information for the Data Subject in Article 13 and 14 via standardized icons. The presentation of such standardized icons is handled by LPL via the Icon element, that allows several icons to be defined for a privacy policy. The Icon element also inherits from the UIElement allowing to name and describe the icons. Note, that currently we are not aware of a standardized icon-set that fulfills the requirements of the GDPR, but there are several proposes [19] [21] [16] as well as an icon-set created for LPL [6].

Both Art. 13(1)(a) and Art. 14(1)(a) specify that the identity and the contact details of the Controller (or its representative) have to be disclosed to the Data Subject. It may be argued if this is implemented in LPL. On the one hand, it is possible to add a descriptive text to the LayeredPrivacyPolicy element containing exactly this information. On the other hand, it may be argued that the DataRecipient element defines for each purpose the recipient of the data and therefore also the Controller. Although both possibilities could probably fulfill this requirement, a distinct solution may be anticipated.

Both Art. 13(1)(b) and Art. 14(1)(b) specify that the contact details of the Data Protection Officer is provided to the Data Subject,
Table 1: Comparison of GDPR requirements of Article 12 - 14 with the capabilities of LPL.

<table>
<thead>
<tr>
<th>Article</th>
<th>GDPR Requirement</th>
<th>LPL Implementation</th>
<th>Fulfilled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 12(1) Sentence 1</td>
<td>Clear and Plain Language</td>
<td>LPL - UIElement</td>
<td>x</td>
</tr>
<tr>
<td>Art. 12(1) Sentence 2</td>
<td>Written or Electronic Information</td>
<td>LPL - LayeredPrivacyPolicy</td>
<td>x</td>
</tr>
<tr>
<td>Art. 12(2)</td>
<td>Data Subject Rights Realization</td>
<td>Framework - Regulated Purposes</td>
<td>x</td>
</tr>
<tr>
<td>Art. 12(3)</td>
<td>Response Time for Data Subject Rights</td>
<td>Framework - Regulated Purposes</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 12(5)</td>
<td>Excessive Data Subject Rights Requests</td>
<td>Framework - Regulated Purposes</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 12(7)</td>
<td>Standardized Icons</td>
<td>LPL - Icon</td>
<td>x</td>
</tr>
<tr>
<td>Art. 13(1)(a), Art. 14(1)(a)</td>
<td>Identity and Contact Details of Controller</td>
<td>LPL - LayeredPrivacyPolicy/DataRecipient</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 13(1)(b), Art. 14(1)(b)</td>
<td>Contact Details of Data Protection Officer</td>
<td>LPL - LayeredPrivacyPolicy</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 13(1)(c), Art. 14(1)(c)</td>
<td>Purposes and Legal Basis for Processing</td>
<td>LPL - Purpose</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 13(1)(d), Art. 14(2)(b)</td>
<td>Legitimate Interest</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Art. 14(1)(d)</td>
<td>Categories of Personal Data</td>
<td>LPL - Data.dataGroup</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 13(1)(e), Art. 14(1)(e)</td>
<td>Recipients of Personal Data</td>
<td>LPL - DataRecipient</td>
<td>x</td>
</tr>
<tr>
<td>Art. 13(1)(f), Art. 14(1)(f)</td>
<td>Third Country Transfer and Safeguards</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Art. 13(2)(a), Art. 14(2)(a)</td>
<td>Storage Period</td>
<td>LPL - Retention</td>
<td>x</td>
</tr>
<tr>
<td>Art. 13(2)(b), Art. 14(2)(c)</td>
<td>Information on Data Subject Rights</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Art. 13(2)(c), Art. 14(2)(d)</td>
<td>Information to Withdraw Consent</td>
<td>LPL - Purpose.optOut/Purpose.required</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 13(2)(d), Art. 14(2)(e)</td>
<td>Information to Lodge a Complaint</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Art. 13(2)(e)</td>
<td>Information on Required Data</td>
<td>LPL - Data.required</td>
<td>x</td>
</tr>
<tr>
<td>Art. 14(2)(f)</td>
<td>Source of Personal Data</td>
<td>LPL - UnderlyingPrivacyPolicy/DataSource</td>
<td>(x)</td>
</tr>
<tr>
<td>Art. 13(2)(f), Art. 14(2)(g)</td>
<td>Automated Decision-Making</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

if applicable. As for the contact details of the Controller, it may be argued if this information is added in the descriptive text of the LayeredPrivacyPolicy element. A distinct solution for this may be anticipated.

Both Art. 13(1)(c) and Art. 14(1)(c) specify that the purposes of the processing of the personal data and the legal basis have to be disclosed to the Data Subject. The purposes of the processing are represented by the Purpose element. But for the legal basis no attribute has been defined within the Purpose element, although it might be argued that are defined within the human-readable description. Following the previous argumentation a distinct solution for the legal basis should be introduced.

Both Art. 13(1)(d) and Art. 14(2)(b) GDPR specify that the legitimate interests have to be detailed if the legal basis for processing is Art.6(1)(f) GDPR. Such a description should be stored within the privacy language, but no such element can be found within LPL.

Art. 14(1)(d) GDPR specifies that the categories of personal data have to be defined. In LPL the Data element has the attribute dataGroup which can specify such a category. But a data field may be assigned to several categories of data, which is not possible. Therefore, we see this requirement only as partly fulfilled.

Both Art. 13(1)(e) and Art. 14(1)(e) GDPR specify that the recipients for the personal data have to be denoted to the Data Subject. This is represented by the DataRecipient element and therefore fulfilled.

Both Art. 13(1)(f) and Art. 14(1)(f) GDPR specify that it has to be denoted if personal data is intended to be transferred to a third country or international organization as well as suitable safeguards have to be described. This is not represented within LPL and therefore not fulfilled.

Both Art. 13(2)(a) and Art. 14(2)(a) GDPR denote that the storage period, or the conditions that specify it, of personal data has to be specified. This is handled by the Retention element that can both specify an exact date but also conditions that specify the relative date.

Both Art. 13(2)(b) and Art. 14(2)(c) GDPR denote that the Data Subject has to be informed about its Data Subject Rights. No element or attribute in LPL distinctive fulfills this requirement.

Both Art. 13(2)(c) and Art. 14(2)(d) GDPR specify that the Data Subject has to be informed about his right to withdraw consent, if the legal basis of processing was the consent of the Data Subject. This is done rather implicitly by LPL, that uses the attributes optOut and required to specify if the purposes can be withdrawn in general (required) and if a consent is necessary optOut. During the Negotiation step of the life-cycle the Data Subject is able to dissent to single purposes. But a more explicit way is to be anticipated, that distinguishes between a processing based on consent and therefore has to inform the Data Subject about his right to withdrawal (Art. 13(2)(c), Art.14(2)(d)) and a processing based on a balance of interests (Art. 6(1)(f)) with the corresponding information about the legitimate interests (Art. 13(1)(d), Art. 14(2)(b)).

Both Art. 13(2)(d) and Art. 14(2)(e) GDPR specify that the Data Subject has to be informed about his right to lodge a complaint. No such information is modeled within LPL and therefore this requirement is not fulfilled.

Art. 13(2)(e) GDPR specifies that the Data Subject has to be informed about required data that is necessary to form a contract. This requirement is covered by the attribute required of the Data element.
Art. 14(2)(f) GDPR specifies that the source of personal data has to be specified as well as if the data source is publicly available. This is handled by the DataSource element for each privacy policy. Due to the layering of the privacy policies by the UnderlyingPrivacyPolicy element it is possible to track the data source even if the data is transferred several times. But the DataSource element is lacking the possibility to define if it is publicly available.

Both Art. 13(2)(f) and Art. 14(2)(g) GDPR specify that the Data Subject has to be informed about the existence of automated decision-making processes, their logic, significance, and envisaged consequences. This is not represented by LPL and therefore the requirement is not fulfilled.

6 PROPOSED IMPROVEMENTS

In the following we propose possible changes or extensions to LPL and the privacy framework to be compliant to Article 12 - 14 of the GDPR.

6.1 Layered Privacy Language

The LPL should be extended by several elements and attributes which inform the Data Subject (see Figure 4). As mentioned before the information may be presented with existing means but explicit machine-readable elements should be preferred.

The identity and the contact details of the Controller or its representative should be added. Therefore, a new element Controller could inherit from the Entity element. This new Controller element would probably be contained by the LayeredPrivacyPolicy element. A set of Controller elements may be necessary in some cases, as Art. 26 GDPR explicitly introduced the model of Joint Controllers. The DataProtectionOfficer element should be created accordingly, whereas also a set of elements should be contained by the LayeredPrivacyPolicy element.

The DataSource element should be extended by the attribute public specifying if the received has been publicly available.

A LegalBasis element should be introduced that inherits from the UIElement. Assuming the legal basis is 'Consent', then the Data Subject has to be informed about his right to withdrawal (Art. 13(2)(c), Art.14(2)(d)). Otherwise, if the legal basis is a 'BalanceofInterests' (Art. 6(1)(f)), then the Data Subject has to be informed about the legitimate interests (Art. 13(1)(d), Art. 14(2)(b)). The information will be stored utilizing the inherited attributes of the UIElement. For each Purpose a set of LegalBasis elements should be definable.

The attribute dataGroup of the Data element should be substituted with a set of DataGroup elements, which inherit from the UIElement. This will provide human-readability as well as the possibility to assign several data groups to a Data element.

The information that data is transferred to third countries should be assigned as an attribute thirdCountryTransfer to the DataRecipient element. Additionally, a Safeguard element should be introduced which inherits from UIElement. A set of Safeguard elements should be referenced by the DataRecipient element. Therefore, the Data Subject can be informed in detail about the conditions. Furthermore, the DataRecipient could be extended by a required attribute, allowing the Data Subject to decide on the processing, like it is done with the Data element.

The information on the Data Subject Rights and that the Data Subject can lodge a complaint are general informations that can be added to the LayeredPrivacyPolicy element as a distinct element, which inherits from the UIElement to allow human-readability.

Lastly, the information if the data is utilized for automated decision-making (and its details) should be added to each Purpose element as a distinct element. Therefore, a set of AutomatedDecisionMaking elements should be referenced. The existence of such an element or a set of elements denotes that the existence of automated decision-making processes. The logic, significance, and envisaged consequences of the automated decision-making should be described unstructured (due to the possible high variance) utilizing the inheritance of UIElement.

6.2 Privacy Framework

With the implementation of the Data Subject Rights two things have to be considered. First, the response time has to be within the allowed time-frame and therefore an adequate technical solution for monitoring the response time has to be applied. Second, it has to be ensured that excessive requests can be detected and possibly blocked. Hereby, a threshold for excessive requests has to be defined.

Additionally, it is essential that the provisions concerning Data Subject Rights are analyzed to identify all the information that has to be provided that is not contained within the privacy policy or more explicitly is not modeled within LPL. Furthermore, the exercise of some Data Subject Rights is dependent on the legal basis for processing. This shall be represented in LPL as well.

6.3 Discussion

Based on the proposed improvements for LPL and its overarching privacy framework following statements can be made: The structure of LPL allows the definition of privacy policies that are both machine-readable and human-readable. The core aspects of a privacy policy have been considered and modeled. But also several aspects, which are mostly informative for the Data Subject, have not been modeled explicitly or at all.

Furthermore, the privacy framework has to be implemented and evaluated to show possible open requirements. We assume that the main challenges will be first to identify all the information that is required to be able to answer the requests. Secondly, the collected information has to be provided in a format that can be either human-readable for the Data Subject or machine-readable to be further processed. For example, the right to data portability will require a data format that allows the transfer of data between Controllers [8].

7 CONCLUSION AND FUTURE WORKS

This paper provided an analysis of the Layered Privacy Language (LPL) including its overarching framework according to the Articles 12 - 14 of the GDPR. LPL is intended to formalize privacy policies both machine- and human-readable to present and enforce them. The GDPR is considered as the legal framework. Both, the Layered Privacy Language and the GDPR requirements have been introduced. For LPL an overview over the concept, life-cycle and the elements and attributes are given. The general concepts of the
GDPR were explained and the articles 12-14 GDPR are analyzed in detail individually, as well as requirements extrapolated and summarized. The requirements are subsequently matched against the existing capabilities of LPL, showing both fulfilled and unfulfilled requirements. The unfulfilled requirements are further discussed to show possible future improvements for LPL. In summary, it is shown that LPL fulfills several key concepts of the GDPR, but still lacks several points that are required to completely inform the Data Subject about the processing of its personal data.

In future, LPL has to be extended and updated to fulfill the missing requirements of the Articles 12-14 of the GDPR. On the one hand, this requires existing features to be extended like the definition of the categories of personal data or an attribute indicating that the source of personal data is publicly accessible. On the other hand, new features have to be added, like the definition of the legal basis for the processing or information on the Data Subject Rights. These may either be added to the privacy language itself or the overarching framework. The steps of the life-cycle of LPL have to be modified to cope with the new features. For example a privacy policy user interface has to be developed representing the required features to inform the Data Subject in human-readable language during the Negotiation step. The impact of the proposed changes to LPL during the Usage, e.g., anonymization process have to be considered accordingly.

Furthermore, additional articles of the GDPR, as well as the related recitals to the GDPR have to be analyzed to identify all requirements for more complex situations and create a complete requirements catalog that can be matched against technical solutions. For example, the Art. 15-22 GDPR should be analyzed to identify all processes and information to be stored to allow a possible automated fulfillment of the Data Subject Rights or to unveil further research questions. Such a requirements catalog could further be utilized as a guideline for both authorities and companies to verify the compliance with the GDPR.

Also there are challenges that have to be tackled by both the legal and computer science, for example the handling of data that refers to more than one Data Subject. From a computer science perspective this could be solved by referencing personal data to the provider of the data. However, this is not always the Data Subject. Therefore, a initial legal decision on this point has to be made before appropriate technical solutions can be defined.

8 ACKNOWLEDGEMENT

The publication of this paper has been funded by FREDI (Forschungsstelle für Rechtsfragen der Digitalisierung), a project of the Zentrum Digitalisierung.Bayern at the University of Passau.

REFERENCES


Critical Analysis of LPL according to Articles 12 - 14 of the GDPR


