Transparency Enhancing Tools and the GDPR: Do They Match?

Dayana Spagnuelo[1](✉), Ana Ferreira[2], and Gabriele Lenzini[3]

[1] Faculty of Science, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands
d.spagnuelo@vu.nl
[2] CINTESIS, University of Porto, Porto, Portugal
[3] Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, Luxembourg City, Luxembourg

Abstract. The introduction of the General Data Protection Regulation (GDPR) came to further strengthen the need for transparency—one of its main principles—and with it, the users' empowerment to make service providers more responsible and accountable for processing of personal data. The technological infrastructures are not yet prepared to fully support the principle, but changes are bound to be implemented in the very near future. In this work (1) we comprehensively elicit the requirements one needs to implement transparency as stated in GDPR, and (2) we verify which current Transparency Enhancing Tools (TETs) can fulfil them. We found that work still needs to be done to comply with the European Regulation. However, parts of some TETs can already solve some issues. Work efforts need to be put on the development of new solutions, but also on the improvement and testing of existing ones.

Keywords: Transparency · Transparency Enhancing Tools · General Data Protection Regulation · Compliance

1 Introduction

The General Data Protection Regulation (GDPR) is pushing data controllers and processors to review and rethink their procedures. According to the Regulation, data controllers and processors need to ensure data subjects (i.e., whom the personal data are about) that the processing is *lawful*, *fair* and *transparent*[1].

This paper is about the last of those principles, *transparency*. Differently from lawfulness and fairness, which express legalistic concepts, transparency is a *socio-technical* concept: intended socially, it means to empower data subjects to have the means to know whether their personal data are lawfully and fairly processed, and how; intended technically, means that ways to achieve transparency should be enforced in existing systems whenever appropriate [1].

The interest in a technical implementation of transparency was not born with the GDPR. For example, it was already discussed in cloud computing to enforce

[1] GDPR, Article 5.1.(a).

P. Mori et al. (Eds.): ICISSP 2019, CCIS 1221, pp. 162–185, 2020.
https://doi.org/10.1007/978-3-030-49443-8_8

accountability [3], and in this it shares a similar goal to the GDPR. Giving a full overview of the principle's history is beyond the scope of this article, but one important observation is that, simultaneously with the entering into force of the GDPR, there exist already tools for enhancing transparency. They are called Transparency Enhancing Tools (TETs), system-independent apps dedicated to inform her/him about how personal data are handled by an online service she/he is accessing.

Can they help improve a system's transparency according to the GDPR? The answer is unclear; as unclear is whether they can give, to who implements them, a presumption of compliance with the GDPR's legal transparency principle. At least in part, this uncertainty is due to the nature of the GDPR. Its legal provisions are expressed in a way that admits several interpretations. As other regulations, the GDPR has been thought for a broad audience and to be technology independent.

Thus, discussing whether a certain technology, like TETs, helps systems in the task of providing transparency requires a methodology. In this paper we apply one: leveraging on a previous study of ours about transparency for medical data systems [26], we elicit a list of requirements from GDPR Articles and provisions that talk about transparency. Then, we select a few TETs among those recently presented in the literature and we discuss whether they implement the requirements we extracted from the GDPR. In so doing, we systematically analyse transparency in support to identify the GDPR concepts still in need of more development.

This work extends our conference paper [25]: we give more explanation to our methodology, and revisit our results by exploring other technical and legal aspects of transparency. In this extended version, we give focus to the process of eliciting requirements from the GDPR and automatically comparing them with technical requirements. We also give more context to our work by appending the full categorisation of the 27 studied TETs, and the complete list of technical requirements.

2 Transparency and the GDPR

Transparency is a transverse principle in the GDPR, that is, it is referred directly or indirectly in several Recitals and Articles, but there is not a clear characterisation of it in the law. For that, we have to review the Articles of the Regulation, and we did by following a four round approach (see also Fig. 1): 1. Selection; 2. Filtering; 3. Revision; and 4. Validation. These rounds were conducted as follows:

1. Selection. Two of this paper's authors working independently made a list of Articles that, according to their understanding, were about transparency. Both authors had previous experience with transparency and TETs, so the expectation was that the combined knowledge covers the general perception of transparency in different technical domains.

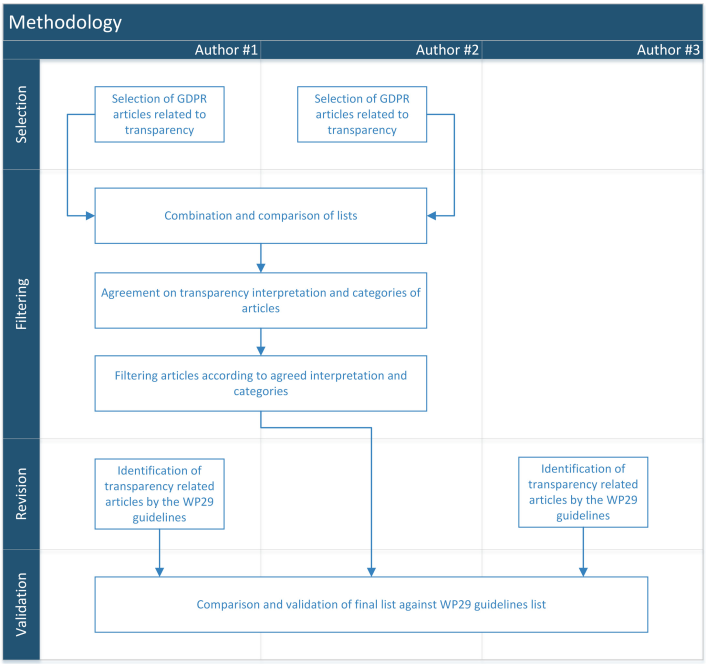
Methodology
Author #1
Author #2
Author #3
Selection
Filtering
Revision
Validation
Selection of GDPR articles related to transparency
Selection of GDPR articles related to transparency
Combination and comparison of lists
Agreement on transparency interpretation and categories of articles
Filtering articles according to agreed interpretation and categories
Identification of transparency related articles by the WP29 guidelines
Identification of transparency related articles by the WP29 guidelines
Comparison and validation of final list against WP29 guidelines list

Fig. 1. Methodology for selecting transparency related Articles from the GDPR.

2. Filtering. The two lists selected were compared and combined. One author at least reviewed all the Articles. Both authors defended their interpretation of transparency, agreed on a common understanding, and extracting categories of Articles covering that understanding, including those about properties and artefacts that support the implementation of the concept. The categories eventually selected by the authors are the following:

1. *Concerning data subjects* – Articles describing the knowledge that should be made available to the data subjects;
2. *Concerning authorities* – Articles describing the knowledge that should be made available to authorities (e.g., Data Protection Officers, or auditors);
3. *Empowerment*[2] – Articles mandating the provision of means for the data subjects to react (e.g., rectification, and erasure);
4. *Quality of transparency* – Articles which qualify transparency and describe how information should be presented to data subjects (e.g., concise, easy to understand);
5. *Certification* – Articles which foresee certification as a means to demonstrate the service's practices;
6. *Consent* – Articles commenting on the need for the data subjects to consent with usage and processing of data.

[2] Also know as intervenability [12].

3. Revision. To check whether our selection is in line with the state of the art, we selected one work which is considered authoritative in the matter, the *guidelines* by the Article 29 Working Party [1], and looked into what Articles therein are referred as being about transparency. We did so in the following way. Two authors (but not the same pair that executed the Filtering to reduce the risk of selection bias) independently selected the Articles that, according to their interpretation, are in the *guidelines* mentioned to be related to transparency. Both reviewers produced a very similar list. We believe this happened because the *guidelines* are more explicit about their interpretation of transparency.

4. Validation. The lists from Selection and from Revision were compared. The comparison intended to highlight the relevancy of our selection of Articles by calculating how many Articles mentioned in the guidelines were covered by us (in first and second rounds). We also compared our list with the one presented by the German Standard Data Protection Model (SDM)[3] regarding the protection goals of transparency and intervenability.

2.1 Transparency in GDPR's Articles

As a result, we compiled a list of selected transparency-related GDPR Articles (paragraphs and sub-paragraphs) that comprises 79 items. It can be found in Table 2. Our selection covers approximately 93% of the Articles in the *guidelines*. We consider our list sufficiently relevant. We comment here only on the Articles mentioned in the *guidelines* that we opted not to include in our study. Article 12.5 describes when the charge of a fee may (or may not) be applied when information is provided to data subjects regarding personal data. Even though this Article relates to transparency, it does not describe a technical feature of a TET or system. Article 20 describes the *right to portability*, which contains provisions on the characteristic of the information provided by transparency, and should be verified for compliance in every tool. Articles 25.1 and 25.2 are both regarding the implementation of *data protection by design and by default*. This concept is instead related to the security property of privacy. Hence those Articles were not selected in our list. However, we include Article 25.3, which foresees the use of certification mechanisms to demonstrate compliance with Articles 25.1 and 25.2. We understand that Article defends the right of data subjects to be aware of how their data are processed (in line with data protection principles), and as such, is in line with our interpretation of transparency.

Our selection does not contradict the list presented by the SDM, it is simply more detailed. The majority of Articles listed by the SDM are also considered in our selection. With the exception of Articles 5.1.(d), 5.1.(f), and 20—regarding accuracy of data, security of personal data, and portability of data. These Articles also contain provisions on the quality of the data provided by transparency, and should be verified for compliance in every tool. Article 40, referring to the design of codes of conduct for controllers and processors, which could hardly be

[3] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methodology_V1_EN1.pdf.

accomplished through the use of TETs. And Article 42, on certification mechanisms, which are considered in Sect. 3.

2.2 Technical Requirements for Transparency

We match the selected GDPR's Articles with a list of technical requirements for transparency presented in previous work from the authors [26]. Due to space limitations, in Appendix A we present a complete list of requirements to help the reader picture how they look like, but we do not give details on their specification and characteristics, we remand to the original work for full details.

To match the Articles from the GDPR and the technical requirements for transparency in medical systems, we developed a simplified parser based on natural language processing techniques.

Our process consists in (1) the *analysis of the text corpora* (2) *extraction of corpus-based glossaries* and *parsing of the corpora*, and (3) *final adjustments*.

We did not conduct any statistical analysis, nor part-of-speech tagging (techniques applied in more sophisticated natural language processing algorithms). Instead, we iterated a few times realising small adjustments in our glossaries, re-evaluating the results of the parsing and, whenever needed, manually adding or removing a match.

Our approach is indeed only possible as our glossaries are context-based, limited to the terminology found in the GDPR and our requirements. We are aware of existing efforts in interpreting and translating laws, regulations, and other legal documents (e.g., [2,16,30]). We do not mean to compete with them, but rather state that our parser, in the specific problem herein addressed, has given sufficiently accurate results.

Text Corpora Analysis. The first step was carried out manually. We first analysed the two text *corpora*: the Articles and provisions in the GDPR, and a set of technical requirements for transparency in the medical domain (see Appendix A). A text *corpus* is described as a "large body of linguistic evidence typically composed of attested language use", but has been used nowadays for a wide variety of text collections [13]. Our set of requirements is not a text *corpus* in its typical meaning, as they are not composed by standardised terms. In this sense, our requirements constitute a text *corpus* in its modern interpretation: a text collection tailored to one specific domain. The GDPR, on the other hand, represents better a classic text *corpus*, as it is stable, well-established and composed by standard legal terminology.

We analysed the text *corpora* and familiarised with the differences between the terminologies, as one *corpus* comprises technical terms and the other legalistic jargon. The terms found in one *corpus* were interpreted and linked to terms in the other. As a result of this task, we highlighted potential connections between requirements and GDPR Articles and established a preliminary list of matches.

Extraction of Corpus-Based Glossaries and Parsing. To ensure the consistency of our matching procedure, we automated the comparisons by extracting possibly-equivalent terms and structuring them in glossaries. Terms found in the GDPR were matched to their equivalent technical terms, found in the list of requirements. The knowledge base needed for realising this step came from revisiting the preliminary list of matches, from where we extracted the key-terms that seem to have triggered each match. We identify matches according to a few textual elements present in the GDPR Articles: the *information* to be provided to the data subject; the *rights* the data subject must have; the *techniques* described in the Articles; and few selected *keywords*. We organised each of these in hash tables that represent, in a way, simplified *corpus*-based glossaries (see Table 1).

Table 1. Glossary of equivalent terms (*GDPR terms* on the left, and *Technical terms* on the right). Information between brackets are contextual and do not constitute the key-term.

Information	
[action (not)] taken on a request	N/A
[identity] of the controller	Responsible for handling owned data
[identity] data protection officer	Who has the authority to investigate
Purpose of processing	Terms [of use]
Legal basis for processing	Policy; regulation
[conditions for] provision of data	Regulation; terms [of use]
Rights	
Rectification	N/A
Erasure [of personal data]	Revoked consent
Restriction [of processing]	N/A
Copy of the personal data	Mechanisms for accessing [personal data]
Object [process of data]	N/A
Not to be subject [to a decision]	N/A
Exercise his or her rights	N/A
Withdraw his or her consent	Revoked consent
Techniques	
[do not] permit identification	Data privacy; to protect [data]; [data] protection; [data is] protected; separation [of data]
Appropriate security	To protect
Withdraw	Revoke
Not in a position to identify	N/A
Automated decision-making	N/A
Obtaining [personal data]	Gather; infer; aggregate
Copy of personal data	Mechanism for accessing [personal data]
Automated means	N/A
Only personal data which are necessary	Data minimisation
Record of [processing of data]	Accountability; audit
Unauthorised	Without authorisation

(contniued)

Table 1. *(contniued)*

Unlawful	Vulnerability; breach
Accidental loss	Data loss; breach
Accidental destruction	N/A
Accidental damage	N/A
Profiling	N/A
Data minimisation	N/A
Existence of the right	Ownership
Shall not apply	N/A
Keywords	
Security	Security
Consent	Consent
Request for consent	N/A
Written declaration	Terms [of use]
Purposes of the processing	Terms [of use]
Concise [information]	N/A
Intelligible [information]	N/A
[information] easily accessible	N/A
[information] using clear [language]	N/A
[information using] plain language	N/A
Icons	N/A
Third party	Third party; third parties; sub-providers; whom it purchases services
Recipients	Who has access; sub-providers; third party; whom it purchases services
International	Other countries; extraterritorial; country
Adequacy decision by the commission	Comply with legal requirements; issues with respect to laws and regulations; legislative regimes
Period	N/A
Categories of personal data	Detailed information [on the data collected]
Source [from where of personal data originate]	[information on] data collected about [the data subject]
Not collected from the data subject	[information on] data collected about [the data subject]
Joint controllers	Different parties
Arrangement	Agreement
Responsibilities	Responsibilities
Respective roles	Responsibilities
Breach	Breach
Without undue further delay	Timely
Document comprising facts [that enables to verify compliance]	Evidence
Able to demonstrate	Evidence
Shall not apply	N/A

Some key-terms were intentionally marked as *not applicable* as they brought almost no contribution to the final list of matches. For example, the term “transparency” found in Article 5.1(a) “Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)”. This Article is comprehensive and should relate to every single requirement from our list, as it mandates data to be processed transparently. To ensure our list had only the most meaningful matches, we decided to explicitly mark this term as not applicable (N/A). The same applies to the term “shall not apply”, which is present in Articles (or paragraphs and sub-paragraphs) describing an exception to another Article. In other words, it presents the circumstances in which our requirements do not need to be implemented. Hence, any match with an Article of this sort is likely to be a false-positive. To avoid this, we marked the term as not applicable. It is important to note that terms marked like this are not the same as terms absent from our glossaries. While the first will force a mismatch between a GDPR Article with that term and any possible requirement in our list, the second will just be disregarded when computing the matches.

The matches are based on an automatic parser. Initially, it parses each GDPR Article to identify all the key-terms they contain. Then the requirements are parsed, searching for the ones which present at least one equivalent term for each key-term found. Our criteria for a match between an Article and a requirement is that all key-terms from the first are represented in the second. The matching procedure is abstracted in Algorithm 1.

The computation of matches is realised in steps (as shown in Algorithm 2): we run the same parsing algorithm for each glossary, and later we merge the results of each comparison in one final list. By doing so, we maintained the matching criterion decoupled, which simplified the process of re-evaluation of the terms and their possibly-equivalents. It also helped in balancing the asymmetry between GDPR Articles and our technical requirements, as the Articles are generally more verbose and encompass too many key-terms. Separating the terms into four glossaries ensured our criterion is not too restrictive, and that Articles can be matched by one or several categories of textual elements.

Final Adjustments. After computing the matches based on the glossaries of terms, we reviewed the resulting list and compared with our preliminary list. Each match was analysed, but we focused on the discrepancies between the lists. For those, we semantically interpreted the Article and requirement matched to understand the context in which the key-terms appeared, and whether or not they had the similar meaning. We conducted this procedure in a peer review manner. The matches were adjusted accordingly. We highlight here a few of the manually adjusted matches.

According to our initial list, requirement 111.2 on information about how data are stored and who has access to them, should match with Article 15.1(c), which describes the rights of the data subject in obtaining from the controller the recipients of personal data. The requirement and the Article have a clear relation.

Algorithm 1. Match($articlesGDPR[n], requirements[m], glossary\{\}[]$)

```
Input: array $articlesGDPR$ with $n$ entries, array of $requirements$ with $m$ entries,
hash table of lists representing the $glossary$ of equivalent terms

$keys = glossary$.getKeys()
for each $i \in \{1, \dots, n\}$ do                                    ▷ For each GDPR Article
    for each $key$ in $keys$ do
        if $articlesGDPR[i]$.containsString($key$) then
            $keyTerms[i]$.add($key$)
    for each $j \in \{1, \dots, m\}$ do                                 ▷ For each requirement
        $matchFound$ = FALSE
        for each $term$ in $keyTerms[i]$ do
            $equivalentTerms[] = glossary\{term\}$
            for each $value$ in $equivalentTerms$ do
                if $requirements[j]$.containsString($value$) then
                    $matchFound$ = TRUE
                    break
                $matchFound$ = FALSE
            if $!matchFound$ then
                break
        if $matchFound$ then
            $matchedArticles[i]$.add($requirements[j]$)
Output: $matchedArticles$
```

Algorithm 2. Init()

```
Let: $articlesGDPR[n]$ be the list of $n$ selected GDPR Articles, $requirements[m]$ be
the list of $m$ technical requirements, $information\{\}[]$ be a glossary of information
that should be provided to the data subject, $rights\{\}[]$ be a glossary of the rights the
data subject has, $technique\{\}[]$ be a glossary of techniques mentioned in an Article,
$keywords\{\}[]$ be a glossary of keywords found in the Articles;

$resultI[]$ = Match($articlesGDPR[]$, $requirements[]$, $information\{\}[]$)
$resultR[]$ = Match($articlesGDPR[]$, $requirements[]$, $rights\{\}[]$)
$resultT[]$ = Match($articlesGDPR[]$, $requirements[]$, $technique\{\}[]$)
$resultK[]$ = Match($articlesGDPR[]$, $requirements[]$, $keywords\{\}[]$)

for each $i \in \{1, \dots, n\}$ do
    $finalMatch[i] = resultI[i] \cup resultR[i] \cup resultT[i] \cup resultK[i]$
Output: $finalMatch$
```

However, it was being disregarded by our parser as the Article contains the key-term "third countries" which does not appear in the requirement. As this key-term is responsible for several other well-fitted matches, we opted for adjusting this exception manually. Similarly, the matches involving requirement 111.18, on describing the ownership of the data, had to be adjusted. We understand that *describing the ownership* means to clarify what means to be the owner of a piece of data. In other words, to inform and describe the rights the data subjects have regarding the control of their data. In this sense, requirement 111.18 also relates to Articles 13.2.(c), 14.2.(c) and 21.4. Our parser captured a few relevant matches for this requirement, but not all of them. We manually added those remaining.

Some other matches were also considered for adjustments, as they were not present in our preliminary list, but were left untouched after a closer semantic analysis. For example, requirement 111.7, about describing procedures and mechanisms planned in cases of security breaches, matched to Articles 33.3 and 33.5, and requirement 111.15 about informing on who has the authority to investigate any policy compliance, which is also matched with 33.3. These Articles describe the information to be provided to data subjects in case of a data breach. Initially, the match was not considered as the requirements are ex ante (information to help the users understand what will happen to their data beforehand), and the Articles are, in a sense, ex post, as the data breach already happened. However, if the information described in the requirements is made available beforehand, in the event of a data breach, it will facilitate compliance with Article 33 from the GDPR. For this reason, we keep these matches.

Similarly, requirements 221.2,5,8 are matched with Article 5.2 of the GDPR (controller shall be accountable and responsible for demonstrating compliance with the lawfulness, fairness and transparency principles). The requirements, at first glance, seem unrelated to the Article, and to each other. However, the three requirements demand the users to be presented with evidence of security breaches, of recovery from them, and of permission history. As evidence, by definition, is a piece of information or data that is used to prove or disprove something, we understand they contribute to *demonstrate compliance*. Even though these matches were not identified in our initial list, we decided to keep them. Our final list of matches is shown in Table 2.

Table 2. Final list of matches between GDPR Articles and technical requirements. 72% of the requirements are matched (26 out of 36). (Table originally presented in [25])

GDPR	Requirements	GDPR	Requirements
5.1.(a)		14.3.(c)	
5.2	111.16, 111.20, 221.1, 221.2, 221.3, 221.4, 221.5, 221.7, 221.8	14.4	
6.1.(a)	221.7	15.1.(a)	111.19
7.1		15.1.(b)	221.6
7.2		15.1.(c)	111.2, 111.4
7.3	221.7	15.1.(d)	
9.2.(a)		15.1.(e)	111.18
11.2		15.1.(f)	
12.1		15.1.(g)	221.6

(*continued*)

Table 2. (*continued*)

GDPR	Requirements	GDPR	Requirements
12.3		15.1.(h)	
12.4		15.2	111.4, 111.11, 221.3
12.7		15.3	112.1
13.1.(a)	111.1	16	
13.1.(b)	111.15	17	221.7
13.1.(c)	111.19	18	
13.1.(d)	111.3, 111.4, 111.14	19	111.2, 111.4,
13.1.(e)	111.2, 111.3, 111.4	21.1	
13.1.(f)	111.4, 111.11, 221.3	21.2	
13.2.(a)		21.3	
13.2.(b)	111.18	21.4	111.18
13.2.(c)	111.18	21.5	
13.2.(d)		22.1	
13.2.(e)		22.2.(c)	
13.2.(f)		25.3	
13.3		26.1	111.14
14.1.(a)	111.1	26.2	111.14
14.1.(b)	111.15	26.3	111.14
14.1.(c)	111.19	30.1	221.5, 222.1, 232.1
14.1.(d)	221.6	30.2	221.5, 222.1, 232.1
14.1.(e)	111.2, 111.3, 111.4	30.3	
14.1.(f)	111.4, 11.11, 221.3	30.4	
14.2.(a)		32.3	
14.2.(b)	111.3, 111.4, 111.14	33.1	111.7, 211.1, 211.4, 221.8
14.2.(c)	111.18	33.2	111.7, 211.1, 211.4, 221.8
14.2.(d)	111.18	33.3	111.7, 111.15, 211.1, 211.4, 221.8
14.2.(e)		33.4	211.4
14.2.(f)	221.6	33.5	111.7, 211.1, 211.4, 221.8
14.2.(g)		34.1	111.7, 211.1, 211.4, 221.8
14.3.(a)	211.5	34.2	
14.3.(b)			

3 Transparency and Technology (TETs)

At least at an intuitive level, the most natural technology for transparency is represented by TETs. According to [18], TETs are tools to“make the underlying processes [of personal data or a subject] more transparent, and to enable data subjects to better understand the implications that arise due to their decision to disclose personal data, or that have arisen due to choices ‘made in the past”’.

This cited work already provide an extensive list of tools. We also reviewed other survey works about TETs and compiled a drafted list of such tools [4,7,17,22,31].

Besides, we browsed the literature for "transparency enhancing tools", looking for works that may have referred to the tools indirectly or within text. The search included works published since 2014, the year the GDPR started to be strongly supported by the European Parliament[4]. We selected 27 tools which can be potentially linked to the transparency principle. We categorised them using TETCat [31], a methodology to classify TETs according to their properties and functionalities, for instance, such as among others, *assurance level* (*not trusted*, *semi trusted*, or *trusted*), the *application time* of the tool (*ex ante*, *ex post* or *real time*) and *interactivity level* (*read-only* or *interactive*).

Our categorisation is summarised in Appendix B and described in the next paragraphs. Its full version is made available in [24].

Assertion Tools. Tools are classified as the assertion type whenever the correctness and completeness of the information they provide cannot be verified (*not trusted*), and they can only provide information on the controller's alleged processing practices. The TETCat does not further distinguish assertion tools, so tools of this type have diverse goals.

Examples of assertion tools are third-party tracking blockers, e.g., Mozilla Lightbeam[5] (ML), Disconnect me[6] (DM), and Privacy Badger[7] (PB); and tools that educate users on matters related to privacy protection, e.g., Privacy Risk Analysis (PRA) [5], Me and My Shadow[8] (MMS), Privacy Score[9] (PS) and Access My Info[10] (AMI).

Awareness Tools. This is the first type of tools providing information verifiable for completeness and correctness, for two assurance levels (i.e., *trusted* and *semi trusted*). Awareness tools provide *ex ante* transparency, and interactivity level of *read only*. Tools in this category help the user becoming aware of the privacy policy of the service provider but do not provide the users with controls over the processing of data. Examples of such tools are machine readable or interpreted policy languages, e.g., Platform for Privacy Preferences Project[11] (P3P). Another example of an awareness tool is the Usable Privacy Project[12] [20], which automatically annotates privacy policies. Finally, tools providing certification seals and marks such as the European Privacy Seal (EuroPriSe) [6] or the TrustArc (TArc) [27] are also examples of tools in this category.

[4] http://europa.eu/rapid/press-release_MEMO-14-186_de.htm.

[5] https://www.mozilla.org/lightbeam.

[6] https://disconnect.me/.

[7] https://www.eff.org/privacybadger.

[8] https://myshadow.org/.

[9] https://privacyscore.org/.

[10] https://openeffect.ca/access-my-info/.

[11] https://www.w3.org/P3P/.

[12] https://explore.usableprivacy.org/.

Declaration Tools. Only one tool falls under this category: PrimeLife Policy Language (PPL) [10], which is similar to awareness tools, comparable to the P3P tool, but offers some level of interactivity.

Audit Tools. Audit TETs present users with *ex post* or *real time* transparency. Tools in this category include those that allow for access and verifiability of data, but do not provide means for the users to interact and intervene with the data processing (i.e., *read only* tools), such as the Data Track[13] (DT) [9] and Personal Data Table (PDT) [22]. Another tool under this category is The Blue Button[14]. Which is an initiative to standardise the right to access personal medical data in the USA, and display a logo stating that users are allowed to visualise and download their data.

Finally, the Private Verification of Access (PVA) [11] proposes a scheme for *a posteriori* access control compliance checks that operates under a data minimisation principle and provides a private independent audit. This tool also falls under the audit tools category.

Intervention Tools. These tools allow users to verify properties about the processing of their data as well as to interact and control the terms of data collection and usage. Examples are: the Privacy Through Transparency (PTT) [21]—supporting Break-the-Glass (BTG) policies; and Privacy eSuite[15].

Remediation Tools. According to the TETCat these tools comprise functionality to exercise control over data collection and usage, and also to modify and delete personal data stored by a data controller. Tools belonging to this category are, for instance, PrivacyInsight (PI) [4] and GDPR Privacy Dashboard[16] (GPD) [19]—both privacy dashboards; and openPDS (oPDS) [14], and Meeco[17] (Mee) which are examples of data vault/marketplace applications.

4 TETs for the GDPR

Our goal is to select from our list of TETs, those which can presumably help achieve compliance with the provisions of the GDPR. We do this indirectly, by selecting those TETs which satisfy the requirements for transparency that we elicited from the analysis of Articles and Recitals of the GDPR

Methodology. The selected TETs have been compared against the technical requirements for transparency, in search for matches. A match is when a tool satisfies one or more requirements. Here, we first pre-select tools and requirements by their application time, distinguishing between *ex ante* and *ex post*/*real time*. Then we compared TETs and requirements one by one. We did this work manually, but having categorised TETs helped us to implement this task more systematically.

[13] https://github.com/pylls/datatrack.

[14] https://www.healthit.gov/topic/health-it-initiatives/blue-button.

[15] http://hipaat.com/privacy-esuite/.

[16] http://philip-raschke.github.io/GDPR-privacy-dashboard.

[17] https://www.meeco.me/.

4.1 Comparing TETs and Requirements: Results and Discussion

Table 3 summarises the findings (we have put in bold the requirements ex ante (1**), and in slanted those ex post (2**)). A full report of them may be found [24], where we expand the GDPR Articles into the paragraphs and sub-paragraphs relevant to this work.

Looking at the Table, two particular exceptions in this matching—exceptions with respect to what one would expect from the methodology we followed—that stand out and need a comment.

The first is concerning requirement 112.1 on the provision of mechanisms for accessing personal data. In the context of medical systems, data about the patients are typically generated by other users in the system. As a consequence, allowing these patients to access their data can be interpreted as pre-condition for them to anticipate what will happen to their data, hence *ex ante*. However, in the context of TETs, tools which allow for the access of personal data are considered *ex post*. We interpret requirement 112.1 and those tools as closely related, even if their application times do not match. The second is regarding certification seals, which we consider *ex ante*. Certification seals are tools which testifies that a system complies with a given criterion. If the criteria regards the processing of data, these seals can help a data subject to anticipate how their data will be processed. However, from the perspective of the system, when evaluated for the certification, the processing of data is already happening. For this reason, we accept the match between such tools and a few relevant *ex post* requirements.

In what follows, we comment on our findings.

Requirements *vs* TETs: What Matches and What Does Not. Three requirements regarding terms and conditions seem not to be addressed by any TET: 111.1 on information regarding the physical location where data is stored; 111.4 on the existence of third-party services and sub-providers; 111.14 on clarifications of responsibility in case of the existence of third-party services.

We believe this information could be provided together with the terms and conditions of the service. Even though the tool provided by Usable Privacy Project (UP) aims at facilitating the reading of these, we did not identify tags for the requirements above. For this reason, we do not consider these requirements as addressed. There are other relevant developments on this subject, such as the CLAUDETTE project[18], which makes use of artificial intelligence to automatically evaluate the clauses of a policy for clarity and completeness in the light of the GDPR provisions. Another relevant tool in this regard is the Me and My Shadow (MMS), which provides a functionality called Lost in Small Print[19]. It reveals and highlights the most relevant information of a given policy. We do not include those tools in our study as the first only evaluates the quality of the policy, without necessarily easing the understanding of its contents, and the second for only providing few selected examples of policies of popular services.

[18] https://claudette.eui.eu/.

[19] https://myshadow.org/lost-in-small-print.

Table 3. From [25]. Transparency Enhancing Tools (TETs), technical requirements, and the GDPR Articles they help realising (* added manually).

TET	Requirements	GDPR Articles
Mozilla Lightbeam	*211.5*, *221.6*	14, 15
P3P	**111.2**, **111.3**, **111.16**, **111.18**, **111.19**	5, 13, 14, 15, 19, 21
PrimeLife Policy Language	**111.2**, **111.3**, **111.16**, **111.18**, **111.19**	5, 13, 14, 15, 19, 21
Data Track	**112.1**, *221.5*, *221.6*, *221.7*	5, 6, 7, 14, 15, 17, 30
Privacy Insight	**112.1**, *221.4*, *221.5*, *221.6*, *221.7*	5, 6, 7, 14, 15, 17, 30
Privacy Risk Analysis	**111.9**, **111.13**	
GDPR Privacy Dashboard	**112.1**, *222.1*, *221.4*, *221.6*, *221.7*	5, 6, 7, 14, 15, 17
Personal Data Table	**112.1**, *211.2*, *211.3*, *222.1*, *221.4*, *221.6*, *221.7*	5, 6, 7, 14, 15, 17
Disconnect me	*222.1*, *221.6*	14, 15
Me and My Shadow	**111.8**, **111.13**, **111.16**, **111.19**	5, 13, 14, 15
EuroPriSe	**111.16**, *221.1*, *221.3*, *221.4*	5, 13, 14, 15
Privacy Score	**111.6**, **111.12**, **111.13**	
Google Dashboard	**112.1**, *222.1*, *221.6*, *221.7*	5, 6, 7, 14, 15, 17
Privacy Evidence	*221.1*, *221.4*, *221.5*, *222.1*, *232.1*	5, 30
TAMI Project	*211.2*, *211.3*, *222.1*, *221.1*, *221.4*, *222.1*, *232.1*	5, 14, 30
Privacy Through Transparency	*211.2*, *211.3*, *221.1*, *221.4*, *221.5*, *222.1*, *232.1*	5, 30
Private Verif. of Access	*211.2*, *211.3*, *221.1*, *221.4*, *222.1*, *232.1*	5, 30
Privacy Badger	*222.1*, *221.6*	14, 15
Access My Info	**112.1**, *221.6*	14, 15
TrustArc	**111.16**, *221.1*, *221.3*, *221.4*	5, 13, 14, 15
openPDS	*222.1*, *221.6*, *221.7*	5, 6, 7, 14, 15, 17
Digi.me	*221.6*, *221.7*	5, 6, 7, 14, 15, 17
Microsoft Dashboard	**112.1**, *222.1*, *221.6*, *221.7*	5, 6, 7, 14, 15, 17
Privacy eSuite	*221.1*, *221.5*, *221.7*, *222.1*, *232.1*	5, 6, 7, 9*, 17, 30
Meeco	*221.6*, *221.7*	5, 6, 7, 14, 15, 17
Blue Button	**112.1**, *221.6*	14, 15
Usable Privacy	**111.5**, **111.10**, **111.11**, **111.15**, **111.17**, **111.19**	13, 14, 15, 33

Nevertheless, they indicate that this matter is already subject of attention. We expect to see a different scenario concerning tools for terms and conditions in the future.

We also observed a lack of tools covering technical aspects of data processing. For example, requirement 111.5 about informing how the system ensures data is not accessed without authorisation, and requirement 111.20 on evidence of separating personal data from metadata, are not addressed by any of the tools we studied. The reason for this is not clear, as other requirements about the use of specific security mechanisms (111.12), and how to protect data (111.13) also cover technical aspects and seem to be the subject of attention of TETs. We speculate this lack of attention may be due to the target audience, which in general has no technical education and would not value such information. Another possible explanation is that this sort of information is provided together with others, and we missed to identify them in our selected tools.

Finally, requirements regarding security breaches and attacks also seem to have gained less attention. They constitute the majority of requirements not addressed by any TET: 111.7, 211.1, 211.4, 221.2, and 221.8. As security breaches are unforeseen events, it does not come as a surprise that there are no tools for aiding the understanding of issues related to them. Nonetheless, it is important to notice that the GDPR reserves two Articles to provisions on personal data breaches (Art. 33 and 34), one of which is dedicated to describing how to communicate such matters to the affected data subjects. Being the health-care industry among the ones with most reported breaches, and being medical data in the top three most compromised variety of data (for more details, see results of the data breach investigation [28]), we consider this to be an area in need of further development.

TETs *vs* Articles: Which Suggests Compliance and Which Does Not. Only a few Articles from the GDPR are not related to any of the selected transparency tools: meaning that none of its paragraphs or sub-paragraphs is matched to a TET. These concern the Articles about data protection mechanisms and certification. Article 25 regards data protection by design and by default, and Article 32 has provisions on security of processing; both mention that compliance with such Articles may be demonstrated through the use of approved certification mechanisms referred to in Article 42.

Despite having included two certification seals in our list of TETs (i.e., EuroPriSe, and TrustArc), EuroPriSe's criteria catalogue has not been approved pursuant to Article 42(5) GDPR. The reason is that they have not been accredited as a certification body pursuant to Article 43 GDPR yet[20]. While for TrustArc, we cannot confirm it is an approved certification mechanisms, we did not find enough information about this matter.

A few transparency quality and empowerment related Articles are also not addressed by our selected tools. Article 12, for example, qualifies the communications with the data subject and states that it should be concise, easily accessible, using clear and plain language, and by electronic means whenever appropriate. In our understanding, this Article does not match to any specific tool because it is transverse to all of them. This Article has provisions regarding the quality of communications; all tools communicating information to data subjects should be affected by it. In [23] we discuss metrics for transparency which, in line with this reasoning, consider the information provided to final users "being concise", or "being easily accessible" as indicators that transparency is properly implemented.

With regard to empowerment related Articles, while a few Articles do relate to some tools (e.g., Art. 17, 19 and 21), they are either partially addressed by transparency tools, or not addressed at all. In fact, empowerment and transparency are different properties [12,26], and this may explain why only a few of those Articles are addressed by TETs. But at least with regard to Articles describing the rights of the data subject towards the processing of personal data (e.g., Art. 22, and 26), we believe policy, and terms and conditions tools could also address them, but we found no tool addressing those subjects.

There are developments in this topic of empowerment though [12]. In this work empowerment (referred to by the authors as intervenability) is discussed

[20] See https://www.european-privacy-seal.eu/EPS-en/Criteria.

as a privacy goal, and it is compared to transparency. In this context, Article 12 relates to their requirement T4 and T5, and Article 17 relates to requirement I10. However, the full implementation of empowerment, as it requires providing ways for users to exercise their rights regarding personal data, may not be suitable for a TET. The analysis of the requirements proposed in [12] and their relationship with TETs falls out of this work's scope.

It is important to notice that a few Articles which appear not to be covered by any TET, are not considered in this analysis because they do not match by key-terms with any of our requirements. We investigate two of them manually: Articles 11, and 9. Article 11 has provisions on processing which does not require identification. We consider this Article in our study as its paragraph 2 states that the controller shall inform the data subjects when it is not in a position to identify them. It also further states that in such a case, Articles 15 to 20 (on the exercise of data subject's rights) shall not apply. In this sense, Article 11 describes a case when empowerment tools (related to Articles 15 to 20) are not required. It does not make sense to discuss the relationship of this Article and TETs in our list.

Article 9, on the other hand, has provisions on data subject's consent for data processing of special categories of personal data, including data concerning health. Privacy eSuite tool (PeS) is a web-service consent engine specifically tailored to collect and centralise consent for the processing of health data. Hence, it is connected with Article 9. In the interest of completeness, we manually added this match in Table 3. However, PeS is a proprietary tool designed in line with the Canadian regulations. We found no means to determine to which extent this tool can help achieving the provisions in the GDPR.

Being *consent* described in the GDPR as one of the basis for lawful processing of personal data, the number of tools addressing this subject seems suspiciously low. This fact does not imply that medical systems and other services are currently operating illegally. We are aware that collecting consent for processing data is a practice. However, we are interested in tools designed to facilitate the task of collecting consent and to help users to be truly informed of the consequences of giving consent.

We investigated this more closely, among our findings there are mostly tools and frameworks aiding the collection of informed consent for digital advertising[21]. We also found mentions to the EnCoRe (Ensuring Consent and Revocation) project, which presents insights on the role of informed consent in online interactions [29]. The project appears finalised, and we found no tool proposed to address the collection of informed consent.

One could claim that tools proposed for terms and conditions, or privacy policies (e.g., P3P, PPL, and UP), can also help collecting consent. While this is a possible solution, special attention is required that the request for consent is distinguishable from other matters (as per GDPR Article 7). It is also important to note that consent to the processing of personal data shall be freely given,

[21] See Conversant, IAB Europe, and ShareThis.

specific, informed, and unambiguous[22]. Implicitly collecting consent for data processing is arguably against the provisions in the GDPR [29]. In that work, the authors discuss to which extent terms and policies are even read and understood. In this sense, consent is unlikely to be truly informed and freely given.

5 Related Works

To the best of our knowledge, only a few works discuss matters of compliance with the GDPR principles (i.e., [4,12,19]). In [12], the authors derive technical requirements from the international standard ISO/IEC 291000 and the GDPR. Even though in this work technical (international standard) and legal (GDPR) documents are used, those are not compared. The requirements studied in this work are instead extracted from these documents.

In [4] the authors propose a Transparency Enhancing Tool (TET) in the form of a privacy dashboard. To define the relevant features to be implemented, they derived eight technical requirements from the *right of access* presented by the GDPR, the previous European Data Protection Directive, and the Federal Data Protection Act from Germany. Similarly, Raschke *et al.* propose a GDPR-compliant dashboard in [19]. In this work, however, only four high-level features are extracted from the GDPR: the right to access data, obtaining information about involved processors, rectification and erasure of data, and consent review and withdraw. Both works extract requirements from data protection laws, but do not compare them with any other sources.

Four works review TETs [7,15,17,31]. The work by Murmann and Fischer-Hübner [15] surveys the literature searching for transparency tools, and explores aspects of usable transparency—derived from legals provisions in the GDPR, and well accepted usability principles. The authors identify meaningful categories of tools and propose a classification based on functionalities and implementation, for instance. Although this work is comprehensive in exploring the characteristics of usable TETs, it does not explicitly map technical aspects of the tools with the GDPR provisions they help accomplishing.

There are works, however, which compare and map legal and technical requirements, principles and designs. In particular, [8] reviews usability principles in a few selected TETs. To this aim, the authors gather requirements from workshops and by reviewing documents related to data protection, such as the proposal of the GDPR (document available at the time), and the opinions from the Article 29 Data Protection Working Party. These requirements are mapped to three Human-Computer Interaction (HCI) concepts, which in turn are discussed in the context of the TETs. Even though the mappings presented in this work are thoroughly discussed, the authors do not present a structured procedure followed when defining them. It is our interpretation that those mappings were identified manually.

[22] GDPR Article 4 (11).

The SDM[23] also classifies GDPR's provision in terms of *data protection goals* (e.g., availability, transparency, intervenability), and comments on *technical measures* that help to guarantee transparency, such as, documentation of procedures, logging of access and modifications. These measures relate to our requirements, but are more high-level. We believe our requirements could be classified according to them, allowing us to select TETs that can accomplish transparency as described by the SDM. We leave this task to future works.

6 Discussion and Conclusion

Even since before the GDPR entered into force, several activities and initiatives bloomed with the aim to provide advice, guidance, instruments, or all of those services, to enterprises concerned about the high fines that were promised to follow a provable lack of compliance with the Regulation.

In this paper we focus on one particular aspect of the compliance, that about the Regulation's principle of transparency. Despite the principle being only transversely referred in the GDPR—that is, it is not subject of one Article or one Recital in particular, but it is rather referred across many items—compliance with it is a serious matter. In January 2019, this statement could not become clearer, when The French data protection authority, the Commission National de l'Informatique et des Liberte (CNIL), condemned Google to pay an impressively high penalty, in the order of about 50 Million euros, because of lack of transparency. CNIL concluded in fact that users of services like Google Search, YouTube, Google Maps, Play Store etc., are not in the position to have a fair perception of the nature and volume of the collected data[24]. The CNIL also objected the transparency of the consent form that Google offers to its users, arguing that the consent form is not informative enough because it is stated in a way which is unclear and ambiguous, in addition to the fact that users have no choice but to accept it.

Discussing the full extent of this famous legal case is beyond our goal and it is not our business either to speculate on the reasons why Tech Giants like Google fail to be compliant with a Regulation, but at least, in part, one could question whether this might be due to the lack of instruments to inform users. In this paper, we looked into what could be the most natural choice, that is Transparency Enhancing Tools (TETs), while at the same time discussing the technical requirements that emerge from a technical reading of the GDPR's provisions.

This comprehensive analysis of transparency helps identifying current and future developments to better comply with transparency and related GDPR requirements by using TETs. The tools were proposed to protect users' privacy in general and thus not designed specifically for the GDPR; rather they have been tailored for one specific use case or goal, or thought to fulfil a specific legislation or regulation according to what were the priorities of who designed

[23] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf.
[24] See https://www.cnil.fr/en/node/25137.

and developed them. Consequently, they cannot be immediately available to be included in most systems nor mindlessly considered ready to interpreting the GDPR's provisions. But our analysis highlights which TETs match the GDPR's requests on transparency, and according to which aspect they do that. However, adapting the tools to become instruments of compliance to the specifics of transparency in GDPR is something that needs to be developed or discussed in a near future. We are not there yet but this paper started to identify and clarify the way towards that goal, so that any future development will not be necessarily built from a blank board, but can be leveraged already by the 12 out of the 21 GDPR Articles that we studied and discussed here. At least partially, those Articles are addressed by the selected/presented TETs.

Acknowledgments. Spagnuelo and Lenzini's research is supported by the Luxembourg National Research Fund (FNR), AFR project 7842804 TYPAMED and CORE project 11333956 DAPRECO, respectively. Ana's research is supported by FCT through the Project TagUBig - Taming Your Big Data (IF/00693/2015) from Researcher FCT Program funded by National Funds through FCT - Fundação para a Ciência e a Tecnologia.

A Transparency Requirements

(See Table 4).

Table 4. Transparency requirements as originally presented in [26]. IDs refer to the original numbering, those indexed 1** are ex ante, those 2** are ex post.

Req.	Specification
111.1	The system must provide the user with real time information on physical data storage and data storage location of different types of data
111.2	The system must inform the user on how data are stored and who has access to them
111.3	The system must inform the user from whom it purchases services, and about any conflict of interest towards data
111.4	The system, in case of using services from third parties, must inform the user about the existence of sub-providers, where they are located and whether they comply with the legal requirements of the country of the user
111.5	The system must inform the user how it is assured that data are not accessed without authorisation
111.6	The system should make available a document that describes the adopted mechanisms for securing data against data loss as well as data privacy vulnerabilities
111.7	The system should make available a document that describes the procedures and mechanisms planned in cases of security breaches on the user's data
111.8	The system should make available the technical documentation on how data are handled, how they are stored, and what are the procedures for accessing them
111.9	The user must be made aware of the consequences of their possible choices in an unbiased manner
111.10	The system must inform the user about who is responsible for handling owned data

(*continued*)

Table 4. (*continued*)

Req.	Specification
111.11	The system must inform the user about storage in other countries and compliance issues related to this storage with respect to laws and regulations of both the other country and their own country
111.12	The system should inform the user about the use of specific security mechanisms
111.13	The system must inform the user on how to protect data or how data are protected
111.14	In case of using services from third parties, The system must inform the user on the responsibilities of the different parties involved in the agreement
111.15	The system must inform the user about who has the authority to investigate any policy compliance
111.16	The system must provide the user with evidence of data collection practices
111.17	The system must make available a document explaining the procedures for leaving the service and taking the data out from the service
111.18	The system must make available a document that describes the ownership of the data
111.19	The system must provide the user with disclosure of policies, regulations or terms regarding data sharing, processing and the use of data
111.20	The system must provide the user with evidence of separating personal from meta data
112.1	The system must provide the user with mechanisms for accessing personal data
211.1	The system, in case of security breaches, must inform the user on what happened, why it happened, what the procedures The system is taking to correct the problem and when services will be resumed as normal
211.2	The system must inform the user when the authorities access personal data
211.3	The system must notify the user in case the policy is overridden (break the glass)
211.4	The system must provide the user with timely notification on security breaches (Art. 33 says, within 72 h after one becomes aware of the incident)
221.5	The system must inform the user if and when data is gathered, inferred or aggregated
221.1	The system must provide the user with evidence that policies, regulations and practices have been applied correctly
221.2	The system must provide the user with evidence of the recovery from security attacks
221.3	The system must provide evidence of compliance with respect to extraterritorial legislative regimes
221.4	The system must provide evidence that the data is being maintained in the correct way
221.5	The system must provide the user with evidence regarding permissions history for auditing purposes
221.6	The system must provide detailed information on the data collected about the user, and what information The system has implicitly derived from disclosed data
221.7	The system must provide the user with evidence that revoked consent has been executed
211.8	The system must provide the user with evidence of security breaches
222.1	The system must provide the user with audit mechanisms
232.1	The system must provide the user with accountability mechanisms

B Transparency Enhancing Tools (TETs)

(See Table 5).

Table 5. Transparency Enhancing Tools (TETs) classified according to their characteristics. (T)TP = (Trusted) Third Party; C = Collection; U = Usage; M = Modification; D = Deletion; A = Analysis; 2^{nd}U = Second Usage.

TET	Applic. time	Exec. envir.	Data type	Auth. level	Interac. level	Assur. level	Transp. dim.	TETCat
Mozilla Lightbeam (ML)	Real-time, Ex-post	Client-side	Obs.	Data-subject	Read-only	Not Trusted	C	Assertion
P3P	Ex-ante	Server-side	Policy	Anonym.	Read-only	(Semi) Trusted	C/U/2^{nd}U	Awareness
PrimeLife Policy Language (PPL)	Ex-ante	Hybrid	Policy	Anonym.	Interac. (C/U)	(Semi) Trusted	C/U/2^{nd}U	Declaration
Data Track (DT)	Ex-post	Hybrid	Volunt., Obs., Incid., Deriv.	Full Id.	Read-only	(Semi) Trusted	C/A	Audit
PrivacyInsight (PI)	Ex-post	Hybrid	Volunt., Incid., Obs., Deriv.	Full Id.	Interac. (C/U/M/D)	(Semi) Trusted	C/A/U/2^{nd}U	Remediation
Privacy Risk Analysis (PRA)	Ex-ante	(T)TP-based	Policy	Anonym.	Read-only	Not trusted	C/A/U/2^{nd}U	Assertion
GDPR Privacy Dashboard (GPD)	Ex-post	Server-side	Volunt., Incid., Obs., Deriv.	Full Id.	Interac. (C/U/M/D)	(Semi) Trusted	C/A/U/2^{nd}U	Remediation
Personal Data Table (PDT)	Ex-post	Server-side	Volunt., Incid., Obs., Deriv.	Full Id.	Read-only	(Semi) Trusted	C/A/U/2^{nd}U	Audit
Disconnect me (DM)	Real-time, Ex-post	Client-side	Obs.	Anonym.	Interac. (C/U)	Not trusted	C/2^{nd}U	Assertion
Me and My Shadow (MMS)	Ex-ante	(T)TP-based	Policy	Anonym.	Read-only	Not trusted	C/A/U/2^{nd}U	Assertion
EuroPriSe	Ex-ante	(T)TP-based	Policy	Anonym.	Read-only	(Semi) Trusted	C/A/U/2^{nd}U	Awareness
Privacy Score (PS)	Ex-ante	(T)TP-based	Policy	Anonym.	Read-only	Not Trusted	2^{nd}U	Assertion
Google Dashboard (GD)	Ex-post	Server-side	Volunt., Incid., Obs., Deriv.	Full Id.	Interac. (C/U/M/D)	(Semi) Trusted	C/A/U/2^{nd}U	Remediation
Privacy Evidence (PEv)	Ex-post	Hybrid	Policy	Full Id.	Read-only	(Semi) Trusted	C/U	Audit
TAMI Project	Ex-post	Hybrid	Volunt., Incid., Obs., Deriv.	Full Id.	Read-only	(Semi) Trusted	U	Audit
Privacy Through Transp. (PTT)	Ex-post	Server-Side	Volunt.	Full Id.	Interac. (C/U)	(Semi) Trusted	C/U	Intervention
Private Verif. of Access (PVA)	Ex-post	Hybrid	Volunt., Obs., Incid., Deriv.	Anonym.	Read-only	(Semi) Trusted	C/U	Audit
Privacy Badger (PB)	Real-time, Ex-post	Client-side	Obs.	Anonym.	Interac. (C/U)	Not trusted	C	Assertion
Access My Info (AMI)	Ex-post	Client-side	Volunt., Incid., Obs., Deriv.	Full Id.	Read-only	Not trusted	C/A	Assertion
TrustArc	Ex-ante	(T)TP-based	Policy	Anonym.	Read-only	(Semi) Trusted	C/A/U/2^{nd}U	Awareness
openPDS	Real-time, Ex-post	Client-side	Volunt., Incid., Obs., Deriv.	Full Id.	Interac. (C/U/M/D)	(Semi) Trusted	C/A/U	Remediation
Digi.me	Real-time, Ex-post	Hybrid	Volunt., Incid., Obs.	Full Id.	Read-only	(Semi) Trusted	C	Audit
Microsoft Dashboard (MD)	Ex-post	Server-side	Volunt., Incid., Obs., Deriv.	Full Id.	Interac. (C/U/M/D)	(Semi) Trusted	C/A/U/2^{nd}U	Remediation
Privacy eSuite (PeS)	Real-time, Ex-post	Hybrid	Volunt., Incid.	Full Id.	Interac. (C/U)	(Semi) Trusted	C/U	Intervention
Meeco (Mee)	Real-time, Ex-post	Hybrid	Policy, Volunt.	Full Id.	Interac. (C/U/M/D)	(Semi) Trusted	U	Remediation
Blue Button (BB)	Ex-post	Server-side	Volunt., Obs., Incid., Deriv.	Full Id.	Read-only	(Semi) Trusted	C	Audit
Usable Privacy (UP)	Ex-ante	(T)TP-based	Policy	Anonym.	Read-only	(Semi) Trusted	C/A U/2^{nd}U	Awareness

References

1. Article 29 Working Party: Guidelines on transparency under regulation 2016/679 (April 2018). http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Accessed Aug 2018
2. Bartolini, C., Giurgiu, A., Lenzini, G., Robaldo, L.: A framework to reason about the legal compliance of security standards. In: Proceedings of the 10th International Workshop on Juris-Informatics (2016)
3. Berthold, S., Fischer-Hübner, S., Martucci, L., Pulls, T.: Crime and punishment in the cloud: accountability, transparency, and privacy. In: International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (2013)
4. Bier, C., Kühne, K., Beyerer, J.: PrivacyInsight: the next generation privacy dashboard. In: Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (eds.) APF 2016. LNCS, vol. 9857, pp. 135–152. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44760-5_9
5. De, S.J., Le Métayer, D.: Privacy risk analysis to enable informed privacy settings. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE (2018)
6. EuroPriSe: Europrise certification criteria (v201701) (January 2017). https://www.european-privacy-seal.eu/EPS-en/Criteria. Accessed Oct 2018
7. Ferreira, A., Lenzini, G.: Can transparency enhancing tools support patient's accessing electronic health records? In: Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P. (eds.) New Contributions in Information Systems and Technologies. AISC, vol. 353, pp. 1121–1132. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16486-1_111
8. Fischer-Hübner, S., Angulo, J., Pulls, T.: How can cloud users be supported in deciding on, tracking and controlling how their data are used? In: Hansen, M., Hoepman, J.-H., Leenes, R., Whitehouse, D. (eds.) Privacy and Identity 2013. IAICT, vol. 421, pp. 77–92. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55137-6_6
9. Fischer-Hübner, S., Angulo, J., Karegar, F., Pulls, T.: Transparency, Privacy and trust – technology for tracking and controlling my data disclosures: does this work? In: Habib, S.M.M., Vassileva, J., Mauw, S., Mühlhäuser, M. (eds.) IFIPTM 2016. IAICT, vol. 473, pp. 3–14. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-41354-9_1
10. Fischer-Hübner, S., Martucci, L.A.: Privacy in social collective intelligence systems. In: Miorandi, D., Maltese, V., Rovatsos, M., Nijholt, A., Stewart, J. (eds.) Social Collective Intelligence. CSS, pp. 105–124. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-08681-1_6
11. Idalino, T.B., Spagnuelo, D., Martina, J.E.: Private verification of access on medical data: an initial study. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds.) ESORICS/DPM/CBT-2017. LNCS, vol. 10436, pp. 86–103. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-67816-0_6
12. Meis, R., Heisel, M.: Computer-aided identification and validation of intervenability requirements. Information **8**(1), 30 (2017)
13. Mitkov, R.: The Oxford Handbook of Computational Linguistics. Oxford University Press, Oxford (2005)
14. de Montjoye, Y.A., Shmueli, E., Wang, S.S., Pentland, A.S.: OpenPDS: protecting the privacy of metadata through safeanswers. PloS One **9**(7), e98790 (2014)

15. Murmann, P., Fischer-Hübner, S.: Tools for achieving usable ex post transparency: a survey. IEEE Access **5**, 22965–22991 (2017)
16. Nejad, N.M., Scerri, S., Auer, S.: Semantic similarity based clustering of license excerpts for improved end-user interpretation. In: Proceedings of the 13th International Conference on Semantic Systems, pp. 144–151. ACM (2017)
17. OPC: Privacy Enhancing Technologies - A Review of Tools and Techniques (November 2017). https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. Accessed Aug 2018
18. Murmann, P., Fischer-Hübner, S.: Usable transparency enhancing tools - a literature review (working paper). Universitetstryckeriet, Karlstad 2017 (2017)
19. Raschke, P., Küpper, A., Drozd, O., Kirrane, S.: Designing a GDPR-compliant and usable privacy dashboard. In: Hansen, M., Kosta, E., Nai-Fovino, I., Fischer-Hübner, S. (eds.) Privacy and Identity 2017. IAICT, vol. 526, pp. 221–236. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-92925-5_14
20. Sathyendra, K.M., Wilson, S., Schaub, F., Zimmeck, S., Sadeh, N.: Identifying the provision of choices in privacy policy text. In: Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing, pp. 2774–2779 (2017)
21. Seneviratne, O., Kagal, L.: Enabling privacy through transparency. In: 12th Annual International Conference on Privacy, Security and Trust, pp. 121–128. IEEE (2014)
22. Siljee, J.: Privacy transparency patterns. In: Proceedings of the 20th European Conference on Pattern Languages of Programs, p. 52. ACM (2015)
23. Spagnuelo, D., Bartolini, C., Lenzini, G.: Modelling metrics for transparency in medical systems. In: Lopez, J., Fischer-Hübner, S., Lambrinoudakis, C. (eds.) TrustBus 2017. LNCS, vol. 10442, pp. 81–95. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-64483-7_6
24. Spagnuelo, D., Ferreira, A., Lenzini, G.: Accomplishing transparency within the general data protection regulation (auxiliary material) (2018). http://hdl.handle.net/10993/37692
25. Spagnuelo, D., Ferreira, A., Lenzini, G.: Accomplishing transparency within the general data protection regulation. In: 5th International Conference on Information Systems Security and Privacy (2019)
26. Spagnuelo, D., Lenzini, G.: Transparent medical data systems. J. Med. Syst. **41**(1), 1–12 (2016). https://doi.org/10.1007/s10916-016-0653-8
27. TrustArc: Enterprise privacy & data governance practices certification assessment criteria (September 2018). https://www.trustarc.com/products/enterprise-privacy-certification/. Accessed Oct 2018
28. Verizon: 2018 data breach investigations report (2018). https://www.verizonenterprise.com/verizon-insights-lab/dbir/. Accessed Oct 2018
29. Whitley, E.A., Kanellopoulou, N.: Privacy and informed consent in online interactions: evidence from expert focus groups. In: ICIS, p. 126 (2010)
30. Wilson, S., et al.: The creation and analysis of a website privacy policy corpus. In: Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics, vol. 1, pp. 1330–1340 (2016)
31. Zimmermann, C.: A categorization of transparency-enhancing technologies. arXiv preprint arXiv:1507.04914 (2015)