2015 IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity

A Guide to End-to-End Privacy Accountability

Denis Butin* and Daniel Le Métayer†
*Technische Universität Darmstadt, Germany dbutin@cdc.informatik.tu-darmstadt.de
†Inria, Université de Lyon, France daniel.le-metayer@inria.fr

***Abstract*—Accountability is considered a tenet of privacy management, yet implementing it effectively is no easy task. It requires a systematic approach with an overarching impact on the design and operation of IT systems. This article, which results from a multidisciplinary project involving lawyers, industry players and computer scientists, presents guidelines for the implementation of consistent sets of accountability measures in organisations. It is based on a systematic analysis of the Draft General Data Protection Regulation. We follow a systematic approach covering the whole life cycle of personal data and considering the three levels of privacy proposed by Bennett, namely accountability of policy, accountability of procedures and accountability of practice.**

I. Context and Motivation

In circumstances of ever-increasing exchanges of personal data between systems and across countries, accountability is increasingly considered as a key requirement for personal data protection. Indeed, when personal data has been collected by a third party, the last resource for individuals is to get reliable information about the way this data has been used and confirmation that this use was consistent with legal requirements. By providing verifiability of actual data handling practice, accountability aims to empower individuals (directly or indirectly, e.g. through data protection authorities or independent trusted third parties) with means to check the compliance of organisations with their privacy requirements. The importance of accountability is also increasingly acknowledged in legal systems [1]. For example, the 2000 Canadian PIPEDA act includes a principle of accountability and the European Union law is expected to incorporate accountability in the upcoming General Data Protection Regulation. Its latest Draft [1] explicitly refers to the principle in two of its articles. Last but not least, accountability can also turn into a strong asset for companies: it can help them clarify their internal processes and level of compliance with legal rules (or their own policies). In addition, a solid accountability process puts a company in a better position to demonstrate its compliance in case of dispute.

Different definitions of accountability have been provided in the literature. Our working definition will be the one suggested by the Article 29 Working Party, which captures the critical aspects of accountability: "showing how responsibility is exercised and making this verifiable" [2]. In the context of data protection, accountability consequently surpasses mere compliance to include an aspect of proof (and burden of proof). Existing research on accountability for data protection can be roughly categorised in two strands: (i) Technical approaches, which focus on specific security properties which embody particular aspects of accountability such as authentication, non-repudiation, log security or the verification of privacy properties (see for instance [3]–[6]); and (ii) Policy-oriented perspectives, mainly for an audience of lawyers and decision makers, with a focus on organisational measures and legal compliance, placing less emphasis on technical issues (e.g. [7]–[9]).

As a result there is generally a gap between these two views of accountability to such extent that the meaning of the word itself can vary a lot from one community to the other [10]. But, for accountability to really meet expectations and effectively enhance privacy protection, it is necessary to be able to translate its general principles into practical measures and to take into account its various dimensions. This contribution is a guide to privacy accountability from the point of view of organisations collecting personal data. The accountability obligations incumbent on organisations can only be met by a combination of organisational, legal and technical measures, which in turn puts specific requirements on technology designers. In fact, accountability is a requirement that should be taken into account from the initial design phase of IT systems because of its strong impact on the implementation of its log architecture: the fact that the owner of the system will have to demonstrate the compliance of the processing necessarily impacts how the system should be designed [11].

In order to ensure the completeness of the accountability process, we describe the measures to be taken at each phase of the life cycle of personal data (*end-to-end accountability*), from its collection to its deletion, including its storage, usage and forwarding to third parties. This systematic scrutiny ensures that all processing stages and the corresponding privacy threats are taken into account. Furthermore, we analyse for each phase the three dimensions of accountability identified by Bennett [12], recalled in §II. Because accountability is defined with respect to a specific set of rules or regulations, we illustrate our approach with the current version of the General Data Protection Regulation [1][2] (hereinafter referred to as *the Regulation*). As a by-product, the systematic approach adopted here provides a new look at the Regulation itself, with a presentation of the precise obligations associated with each phase of the personal data life cycle. However, our approach does not depend on the specific privacy requirements under consideration and it can be applied to other regulations or specific privacy policies.

In the next section, we introduce the terminology and main concepts used in the remainder of the paper. The core of the paper is §III, which handles each phase of the the personal data life cycle in turn[3]. After a comparison with existing frameworks (§IV), we conclude with a synthesis and some remarks on the scope and limits of data protection accountability(§V).

II. Accountability and Privacy Requirements

We now set the stage by introducing some key words and notions used in this paper and clarifying the three types of accountability considered here.

[1] It was already introduced as a basic principle in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[2] As adopted by the European Parliament in March 2014.

[3] A longer version of this article will be provided as a research report.

978-1-4673-7097-4/15 $31.00 © 2015 IEEE
DOI 10.1109/TELERISE.2015.12

A. *Privacy Requirements and Policies*

We follow the terminology of the EU Data Protection Directive 95/46/EC and use the words *data controller* (DC) to denote the entities collecting personal data [4] and *data subject* (DS) to denote the person to whom the personal data relates. The *privacy requirements* for a DC can stem from a number of sources. Applicable laws have to be complied with, but many controllers aim to go above and beyond legal duty by setting higher standards for themselves in the form of specific *privacy policies*, which typically refer to declarative statements in natural language[5] or to corporate policies (often called "Binding Corporate Rules" for multinational companies). Privacy policies may also result from interactions with users expressing their privacy choices through appropriate interfaces and be translated into machine-readable, standardised data handling rules (hereinafter referred to as *technical privacy policies*). Actually a wide range of languages are available to express technical privacy policies. Some of them, such as XACML [13], are general purpose and solely concerned with access control. Others, such as UCON [14], include usage control, i.e. what can be done with the data after it has been accessed. A number of dedicated languages and frameworks have also been proposed to express privacy policies [15]–[21]. Technical privacy policies expressed in these frameworks can be used as a reference to assess the compliance of the data handling evidence provided by logs [11].

B. *Types of Accountability*

Bennett [12] introduced a three-tier terminology which simplifies discussion of accountability by distinguishing between the following facets:

Accountability of policy can be seen as the first level of accountability: the organisation should be able to demonstrate that it has defined a clear and properly documented privacy policy. Such privacy policies can be displayed on websites, or be defined in codes of practice or any other available document. Data handling obligations can also be defined more precisely than in natural language by using technical privacy policies in standardised formats. Accountability mechanisms based on accountability of policy analyse declarations of intent by DC and compare them to norms, for instance regulations (privacy policies should comply with any applicable law).

Accountability of procedures, which refers to the demonstration of organisational mechanisms such as documented processes to cope with user consent, to address complaints or personal data requests; staff training modules; risk assessments; evidence of internal structures (e.g. on intranet sites), and so on. The organisation must be in a position to demonstrate that its procedures are sufficient to implement its privacy policies.

Accountability of practice is the a posteriori demonstration of the effectiveness of the accountability of procedures: in other works, it is a proof that the privacy policies have effectively been met. The implementation of this level of accountability requires to record sufficient information about the operations of the system to prove compliance. Formalisation can be useful to tackle this level of accountability, by defining obligations and evidence such as to enable automated compliance checking [22].

Roughly speaking, the first type of accountability is purely declarative and provides at best a form of legal guarantee (binding commitment); the second type adds guarantees at the organisational level but only the third type can deliver the full promises of accountability. Bennett emphasises that excessive focus has been placed on the first and the second types of accountability so far, resulting in only superficial guarantees. These three types of accountability build on each other and they are all relevant for each phase of the personal data life cycle. In the next section, we consider every type of accountability at every step of data processing, fostering an exhaustive modus operandi that minimises omissions.

III. End-to-End Accountability

In this section, we look in turn at each stage of the personal data life cycle (respectively data collection, data storage, data usage, data forwarding and data deletion) with respect to the design and operation of accountable systems and illustrate them with precise requirements from the Regulation. Because accountability is about "showing how responsibility is exercised and making this verifiable", the production of evidence is essential in its implementation. Therefore, for each stage and each type of accountability, we make explicit the type of evidence to be produced by the DC. While many aspects of accountability are relevant to specific stages of the personal data life cycle, some of them (e.g. the existence of a precise privacy policy or general organisational measures) are common to all of them. We survey those aspects in the last subsection and focus on the specific aspects in the next subsections. The interested reader can find in Table I an overview of the key accountability evidence across all stages of the personal data life cycle.

A. *Data Collection*

The Regulation defines the following obligations for controllers relative to data collection:

A1 When personal data of a DS is collected by a DC, the DS must be informed of: (i) her rights over the collected data (objection, access, rectification, deletion etc), (ii) the identity and contact details of the DC, (iii) the purpose of processing, (iv) the retention period, (v) the recipients of the data and who it may be forwarded to, (vi) whether providing the personal data is required, (vii) whether the data is stored in encrypted form — these rights must be easy to exercise; (*Recital 38 & 47 & 48 & 51, Article 13a & 14*)

A2 Personal data must be collected for a purpose which is "specified, explicit and legitimate". In particular, data collection must be fair, i.e. the stated purpose may not mislead DS; (*Art. 5*)

A3 Only personal data necessary for stated purposes of processing may be collected. The amount of collected data must be proportional to the purposes of processing; (*Art. 5*)

A4 Specific and informed consent is needed for data collection. If consent is required in response to a request by DC, this request must be concise; (*Rec. 25, Art. 4*)

A5 Records of data collection must be kept by DC so as to enable the exercise of the rights of information mentioned above at a later time, either by DS or by supervisory authority. (*Art. 14*)

[4] More precisely, the DC is "the entity that determines, alone or jointly with others, the purposes and the means of the processing of personal data."

[5] Sometimes also called *fair processing notices*.

We now analyse each of these requirements in turn from the accountability perspective.

Privacy policies play a key role in the data collection phase. They must clearly define all the information required in the above articles, in particular in **A1**. They also form the basis of accountability of practices for data collection: to demonstrate the adequacy of collected data, samples of (possibly pseudonymised) collected data should be provided to prove that the categories of data collected in practice correspond to the categories declared in the privacy policy.

A1 & A2: As far as accountability of practice is concerned, since DC must demonstrate that the right of information of DS was respected, systems should keep a history of informative messages that were sent to DS. Considering these messages are usually sent electronically, existing processes can be linked with a database listing (possibly pseudonymised) DS and the type of information contained in the messages sent to them. The types of information mentioned above must be included in the messages. In particular, the purpose of processing must be included explicitly and plainly to prevent misleading DS through ambiguity. If DS are informed through a statement on a web page, the page can be used as evidence. Samples of messages sent to DS also help demonstrating that their rights are easy to exercise, for instance by directing them to an HTML form. In addition, quality assurance mechanisms for DS access requests provide accountability of procedure for this aspect.

A2 & A3: Privacy Impact Assessments (PIA) [23] can provide useful arguments for DC to show the legitimacy and proportionality of personal data processing. PIA should be performed before the design of a system. They constitute an introspective process, performed in an optic of risk prevention, and are often not mandatory by themselves (the Regulation introduces the obligation of performing PIAs for certain types of processing though). However, their proactive nature strongly contributes to accountability by demonstrating the fact that risks were evaluated, how the evaluation was performed, what results the assessment yielded and how they have been taken into account (countermeasures).

A4: Consent by DS must also be shown, hence recorded by the DC. Various levels of consent can be considered, ranging from full electronic signatures (only available in specific settings) to simple online forms with a box to click. In all cases, DC should be able to provide a sample of the device used to establish consent and show that consent resulted from a deliberate action from the DS (and not just an oversight). Since conciseness of consent requests is a requirement, lengthy legal texts would not fit this criteria. Similarly, vague purpose definitions are not acceptable because consent would not be considered “specific”.

A5: The recording of data collection can be systematised by including as a feature of the system a dedicated database, updated with collection metadata on the fly. To comply with regulation, records of collection should include not only a trace of the collection itself but also the associated purpose(s) of processing, retention period and potential recipients in case the data may be forwarded later.

B. Data Storage

The Regulation defines the following requirements:

B1 Storage security (personal data “availability, authenticity, integrity and confidentiality”) — this includes limiting access to data; (*Rec. 39, Art. 30*)

B2 Mechanisms for the periodic review of the need for the storage of personal data. (*Rec. 30, Art. 5 & 17*)

In cases the data is processed exclusively for special research purposes (“historical, statistical or scientific”), it may be stored longer than normally. (*Rec. 53*)

B1: Demonstrating personal data storage security can be done in several ways. Firstly, as far as policies are concerned, DC must document precisely their adopted security measures (including the cryptographic algorithms in use, key management, access control, definition of authorised persons, etc.). On the procedural side, a proactive approach involves performing security audits and keeping records of the results. Physical security should be taken into account too, and appropriate procedures put into place for the protection of sites where personal data is stored. This requirement is much more difficult to respect if cloud storage, web applications or mobile devices are used by DC, a first option being in this case to store only (locally) encrypted data to avoid any leakage on the server side. Assets such as printers and removable media devices create additional privacy threats and must be included in risk assessment procedures. Incident management should be in place both for physical and logical security. In cases where manual records are used, special care is required for their security. It is also important to maintain precise policies and procedures relative to personal data access by individuals working for the DC. Roles and responsibilities must, at the least, be defined clearly in documents. DC can demonstrate stronger accountability in this respect by maintaining role-based access control on data processing platforms. If employees are allowed to work from home, special security measures and procedures should exist and be documented in a dedicated risk assessment to account for the additional privacy threats.

B2: The existence of mechanisms for periodic need review can be made verifiable by explaining their operation, including dedicated sessions in staff schedule, or automatically locking the system if a review report has not been entered for too long.

C. Data Usage

The Regulation defines the following requirements:

C1 Information of DS about details of mechanised data handling (“logic [of] automated processing”), the occurrence and consequences of profiling[6], the purposes of data usage, and their right to receive a copy of the processed personal data; (*Rec. 51, Art. 14 & 15*)

C2 The (demonstrated) compliance of data processing with the Regulation; (*Rec. 60 & 65, Art. 5 & 22*)

C3 The implementation of compliance procedures and policies that “persistently respect the autonomous choices of” DS, and the review and update of these policies at least every two years; (*Art. 22*)

C4 That personal data is only used for the purposes for which it was initially collected. (*Rec. 30, Art. 5 & 6*)

C1: C1 is close to **A1** as far as accountability is concerned, with the additional requirement related to the information of the DS about “the logic [of] automated processing” and “the occurrence and consequences of profiling”.

[6] “automated processing of personal data intended to evaluate certain personal aspects relating to a natural person (. . .)”.

C2: The accountability requirements stemming from **C2** are very broad as they concern the whole Regulation. Generally speaking, in order to make accountability measures more systematic and more reliable, it is possible to use a technical privacy policy language such as PPL, SIMPL FLAVOR, etc. [15]–[21], [24]. To take full advantage of technical privacy policies, evidence about data handling should be generated as well, in the form of system logs. The existence of logs also answers the requirement of record-keeping of data "alteration, consultation and combination", and the demonstration of compliance with this requirement is simply the record itself. Provided these logs are adequate, compliance can be demonstrated mechanically using a log analyser checking the logs against the technical privacy policy in force. To make system logs fit for accountability of practice, they can be translated into a form easier to relate to privacy policies, abstracting away from system internals and focusing on categories of personal data rather than on filesystem details [22]. The question of adequacy is important because the presence of data handling logs in itself is no sufficient guarantee of meaningful data usage accountability of practice. Perhaps surprisingly, log design [25]–[28] is more difficult than it seems and missing details can be enough to render logs useless for compliance checking, or only partly usable. In the case of the PPL logs discussed in [11], the lack of pointers from action events to trigger events breaks the mapping between obligations and log events, propagating ambiguity to the level of the compliance analysis and ultimately preventing comprehensive accountability. This kind of mistake is trivial to fix in the design of a log format, but once it is used in an up and running system, modifications can become much harder to implement. Even if logs are adequate, important issues have to be considered:

1) *Trustworthiness*. Measures are needed to guarantee that logs reflect actual system behaviour. Partial formal modeling, i.e. the modeling of only the most critical components (those directly involved in log generation) may provide a satisfactory benefits-cost trade-off [22].
2) *Storage security*. Access to logs should be strictly monitored to protect the sensitive, personal data-related information they contain. Existing techniques such as forward integrity [26] prevent tampering with existing logs.
3) *Minimisation*. The principle of data minimisation prescribes that no extraneous data should be kept [22].
4) *Comprehensiveness*. Provided the above criteria are fulfilled, logs must still be semantically rich enough to be useful for compliance analysis. The information they contain, and its level of detail, must be adequate for the considered technical privacy policy language.

C3: Provided that policies and procedures have been defined as discussed above, the only additional requirement is to have in place a procedure to ensure that periodic reviews and updates are effectively conducted (similarly to **B2**).

C4: If the necessary information is stored in the accountability logs, it is possible to use a log analyser to justify the fact that data was only used for purposes authorised in the privacy policy. The analyser should provide some form of interaction with the auditor to allow for human verification of the obligations that cannot be check automatically. For instance, in case of special situations (e.g. medical emergencies), different rules may apply (e.g. access to the medical records of a patient may be wider than normally) [29]. When data is used for a specific purpose, justifications in natural language should be provided by the DC and integrated in data handling logs. The log analyser should then output, in addition to the result of the purely deterministic verification, the list of purposes for which the data was declared to be used and the associated justifications. It is then the task of a human analyst to decide whether the justifications are convincing. This kind of integration fosters the active demonstration of compliance by distinguishing clearly between formal compliance and informal aspects, and laying bare what remains to be checked. See [22] for a formal perspective on this kind of integration.

D. Data Forwarding

The Regulation defines the following requirements:

D1 DS must be informed if personal data forwarding is to be carried out; (*Rec. 49 & 51, Art. 14 & 15*)

D2 Data disclosure records must be kept by DC; (*Art. 28*)

D3 Data must not be transferred beyond European borders without an "adequate level of protection". (*Rec. 63 & 82, Art. 22 & 41*)

D4 Data forwarding must be carried out in a secure way (this includes confidentiality, integrity and so on); (*Rec. 39 & 60 & 66, Art. 23 & 30*)

D5 In case deletion is requested by a DS, DC must also take steps to have the data erased by third parties; (*Rec. 54, Art. 13 & 17*)

D1: D1 is similar to **A1** and **C1** as far as accountability is concerned.

D2 & D3: System designers ought to make data disclosure traceable. At the level of policy, a list of third parties to which personal data may be forwarded should be maintained, together with the territories under the jurisdiction of which the third parties operate and associated legal justifications. Procedures must be in place to execute contracts with third parties. At the system level, logs can help again by giving a complete picture of all data disclosures occurring for each individual. Since obligations relative to the forwarding of data can also be specified in technical privacy policies, the approach outlined earlier, based on log analysis, can sustain accountability of practice for data forwarding also provided that the identities of the receiving parties are kept in the logs. In addition, DC should state explicitly to the receiving parties the privacy requirements associated with the data. Ideally the privacy policy should be attached to the data (which is sometimes referred to as "sticky policies").

D4: PIA help evaluate the risks created by third-party data forwarding and are therefore contribute to the accountability of procedures for data forwarding.

D5: Explicitness is also required for third party personal data deletion orders. Those orders should be recorded with the right level of detail so as to not create additional privacy threats. In case logging can be used in the system, both the forwarding of personal data and deletion or update requests to third parties should be included in the execution logs.

E. Data Deletion

The Regulation defines the following requirements:

E1 Personal data must carry retention period limits decided by DC, and kept to "a strict minimum". DC must implement mechanisms to make sure that retention period limits are respected; (*Rec. 30, Art. 17*)

E2 DC must keep records of personal data erasure so as to demonstrate compliance with the above requirements; (*Rec. 60 & 65, Art. 5 & 22*)

E3 Inaccurate data must be either rectified, or deleted. (*Rec. 30, Art. 5 & 16*)

E1: The privacy policy should include retention limits and justifications that the limits are not excessive. In practice, maximum retention periods should be implemented in the information system, either as part of a technical privacy policy or through other technical means. To ensure that global deletion delays are respected, system logs can be checked with respect to the delays specified in the technical privacy policy. To make sure all versions of data are actually erased, a number of aspects must be taken into account: (i) Not only the initially collected data but also all of its local copies must be deleted; (ii) If data aggregation is used, new personal data aggregated from the data that is meant to be erased may have to be deleted as well; (iii) If data has been disseminated to third parties, DC must send deletion requests to those third parties, and ask the third parties to also delete copies. Compliance on these points may be demonstrated by storing the result of log analysis with respect to a technical privacy policy mentioning retention limits. Semantics of log compliance should be provided as well to demonstrate how complete deletion is defined in the framework.

E2: Deletion of data itself must be traceable, too. If logs are used, compliance of data deletion can then be demonstrated through a log analyser, similarly to the demonstration of data usage compliance described earlier.

E3: The right of DS to request the rectification of inaccurate data should also be spelled out. To support these rights, standardised procedures must be put in place to facilitate rectification requests by DS; in particular, the DS should be supplied with contact details to this end. Moreover, DC should proactively ensure that data is accurate, for instance by periodically contacting DS to ask them if their data is still up-to-date. This behaviour can be demonstrated by keeping records of such messages sent to DS.

F. Common Mechanisms

Generally speaking, accountability of procedures is strengthened by proof of existence of a data protection officer, as evidenced e.g. by that individual's job description. To ensure staff perceives the sensitivity of personal data handling, training sessions should be performed and refresher trainings scheduled periodically. E-training is also an option. Regardless of how awareness training is conducted, evidence such as detailed minutes or course material should be retained to ensure demonstrability. As shown in the previous subsections, two other mechanisms are recurrent among the stages of the personal data life cycle: PIA and privacy policies. As far as accountability of procedures goes, PIA results are a key element of evidence. Since all data processing stages feature threats to privacy, the measures taken to address these risks should be justified with respect to the PIA. In terms of practice, the analysis of data handling logs with respect to technical privacy policies is a key global accountability component. Insofar data processing can be formalised without ambiguity, its compliance with technical privacy policy can be checked automatically, thereby offering strong guarantees. As mentioned earlier, this approach entails appropriate security measures for log generation and storage.

IV. Related Frameworks

The expression *end-to-end accountability* is also used in [30], albeit with a different meaning: there it refers to accountability about data usage independently of its online distribution, whereas our idiom emphasises the inclusion of all personal data life cycle stages. In [31], the same expression refers to accountability across all nodes of a grid computing system. No systematic guidelines for accountability across personal data life cycle stages exists to the best of our knowledge, but a number of related frameworks are worth mentioning. Internal tools supporting accountable privacy management are sometimes used by companies to help employees make decisions affecting personal data. HP uses a decision support engine called the Privacy Advisor [32], used for the assessment of privacy risks. Staff are helped to make decisions regarding data handling after filling out a questionnaire, including criteria such as handled information types, the handling of specific types of sensitive information and so on. Accountability frameworks can also be outsourced. Nymity's Accountability Scorecard [33] is a standardised, freely available spreadsheet meant to help organisations evaluate their privacy management in a systematic way; it is mostly focused on policy and procedures. By generating an overall accountability score, it fosters a quantitative perspective on privacy management. The French DPA (CNIL) has published a certification reference describing audit procedure requirements with regards to the processing of personal data [34]. The aim of this reference is to prescribe required elements of privacy audits. A similar — though non-legally binding — document has been published by the UK DPA [35]. It notably includes example evidence that organisations can produce to account for their data processing.

V. Conclusions

We systematically analysed accountability requirements for DC (and, indirectly, for system designers) across the personal data life cycle. Each of these requirements leads to a number of key fragments of evidence, which should be gathered to present a convincing narrative to potential auditors. Table I synthesizes key accountability evidence across personal data life cycle stages. Great care should be taken to ensure that these fragments of evidence (the "accounts") required for the implementation of accountability (e.g. audit logs) do not introduce by themselves new privacy risks. Several measures can be taken to address this requirement, including the minimisation of the data stored in the records (see e.g. [22] for "personal data free" audit logs) and the security measures to ensure the protection of the logs themselves (see [25]–[27]). Accountability is often seen as a burden for organisations because of the extra care needed to generate, organise and store relevant evidence. Such costs can be minimised by including provisions for accountability right from the start, in particular for information systems handling personal data (extending the "privacy by design" principle to "accountability by design"). Moreover, accountability also produces added value for organisations themselves, by clarifying internal processes, encouraging quantification and fostering staff responsibilisation. As pointed out by de Hert [7], the "qualitative dimension of accountability should not be underrated". Even end-to-end, rigorous accountability cannot offer absolute privacy guarantees. Rather, accountability is meant to increase trust in the organisation by combining a number of measures with an existing basis of minimal trust. While evidence can be forged or twisted in many ways, increasing the array of required accounts and the level of detail in which they are analysed is the best realistic bet to increase the protection of individuals.

TABLE I. SYNTHESIS OF EVIDENCE FOR PRIVACY REQUIREMENTS ACROSS PERSONAL DATA LIFE CYCLE STAGES

	Requirement	Account. of policy	Account. of procedures	Account. of practice
Collection	DS information	Privacy policy	Interaction workflow description	DS information message samples
	Legitimate purpose & fair collection	Privacy policy	PIA results & rationale	External audit result
	Purpose limitation & proportionality	Privacy policy	Internal assessment	Collected data samples
	Specific and informed DS consent	Privacy policy	DS interaction specification	Consent record samples
	Record-keeping of data collection	Privacy policy	Workflow documentation	Data collection forms
Storage	Storage security, including access	Measures notice	PIA results & rationale	RBAC, security protocol specifications
	Mechanisms for periodic reviews	Privacy policy	Staff schedule, job descriptions	System implementation
Usage	DS information of processing logic	Privacy policy	Inclusion in interaction workflow	DS email samples
	Processing compliance	Privacy policy	PIA results & rationale	Technical privacy policy
	Compliance implementation; review	Privacy policy	Operational schedule	Logs (+ analysis) & justifications
	Purpose limitation	Privacy policy	Workflow documentation	Log analysis & justifications
Forwarding	DS information of forwarding	List of third parties	Workflow description	Online statement or email sample
	Record-keeping of data disclosures	List of third parties	Contracts with third parties	Logs & log analysis result
	Transfer restriction	Privacy policy	PIA results & rationale	IP headers, justifications
	Transfer security	Measures notice	PIA results & rationale	Security protocol specification
	Third party deletion	Privacy policy	Notification sending mechanism	Logs & log analysis result
Deletion	Retention limits & mechanisms	Privacy policy	Information system specification	Technical privacy policy & log analysis
	Record-keeping of data erasure	Privacy policy	Information system specification	Log analysis result, erasure certificates
	Inaccurate data rectification	Privacy policy	Standardised procedure	DS interaction sample

ACKNOWLEDGMENT

This work was partially funded by PARIS/FP7-SEC-2012-1.

REFERENCES

[1] European Commission, "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), inofficial LIBE version," 2013.

[2] Article 29 Working Party, "Opinion 3/2010 on the principle of accountability," 2010.

[3] R. Jagadeesan *et al.*, "Towards a Theory of Accountability and Audit," in *ESORICS*, ser. LNCS, vol. 5789. Springer, 2009, pp. 152–167.

[4] J. Cederquist *et al.*, "Audit-based compliance control," *Int. J. Inf. Secur.*, vol. 6, no. 2, pp. 133–151, 2007.

[5] A. Haeberlen, "A Case for the Accountable Cloud," *Operating Systems Review*, vol. 44, no. 2, pp. 52–57, 2010.

[6] A. Datta, "Privacy through Accountability: A Computer Science Perspective," in *Distributed Computing and Internet Technology*, ser. LNCS, R. Natarajan, Ed. Springer, 2014, vol. 8337, pp. 43–49.

[7] P. De Hert, "Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law," in *Managing Privacy through Accountability*. Palgrave Macmillan, 2012, pp. 193–232.

[8] C. Raab, "The Meaning of 'Accountability' in the Information Privacy Context," in *Managing Privacy through Accountability*. Palgrave Macmillan, 2012, pp. 15–32.

[9] Center for Information Policy Leadership, "Data Protection Accountability: The Essential Elements," 2009.

[10] D. Butin, M. Chicote, and D. Le Métayer, "Strong Accountability: Beyond Vague Promises," in *Reloading Data Protection*, S. Gutwirth, R. Leenes, and P. De Hert, Eds. Springer, 2014, pp. 343–369.

[11] D. Butin, M. Chicote, and D. Le Métayer, "Log Design for Accountability," in *4th International Workshop on Data Usage Management*. IEEE Computer Society, 2013, pp. 1–7.

[12] C. J. Bennett, "Implementing Privacy Codes of Practice," *Canadian Standards Association*, 1995.

[13] The OASIS technical commitee, "XACML: eXtensible Access Control Markup Language," 2005.

[14] J. Park and R. Sandhu, "Towards Usage Control Models: Beyond Traditional Access Control," in *SACMAT*. ACM, 2002, pp. 57–64.

[15] A. Barth, A. Datta, J. Mitchell, and H. Nissenbaum, "Privacy and contextual integrity: Framework and applications," in *IEEE S&P*. IEEE Computer Society, 2006, pp. 184–198.

[16] M. Backes, B. Pfitzmann, and M. Schunter, "A Toolkit for Managing Enterprise Privacy Policies," in *ESORICS*, ser. LNCS, E. Snekkenes and D. Gollmann, Eds. Springer, 2003, vol. 2808, pp. 162–180.

[17] M. Jafari *et al.*, "Towards defining semantic foundations for purpose-based privacy policies," in *CODASPY*. ACM, 2011, pp. 213–224.

[18] G. Karjoth, M. Schunter, and E. Herreweghen, "Translating privacy practices into privacy promises -how to promise what you can keep," in *POLICY*. IEEE, 2003, pp. 135–146.

[19] D. Le Métayer, "A formal privacy management framework," in *Formal Aspects in Security and Trust*, ser. LNCS, P. Degano, J. D. Guttman, and F. Martinelli, Eds., vol. 5491. Springer, 2008, pp. 162–176.

[20] N. Li, T. Yu and A.I. Antón, "A semantics based approach to privacy languages," *Comput. Syst. Sci. Eng.*, vol. 21(5), 2006.

[21] R. Thion and D. Le Métayer, "FLAVOR: a Formal Language for A posteriori Verification of Legal Rules," in *POLICY*. IEEE Computer Society, 2011, pp. 1–8.

[22] D. Butin and D. Le Métayer, "Log Analysis for Data Protection Accountability," in *FM 2014: Formal Methods*, ser. LNCS, C. B. Jones, P. Pihlajasaari, and J. Sun, Eds., vol. 8442. Springer, 2014.

[23] D. Wright and P. Hert, "Introduction to Privacy Impact Assessment," in *Privacy Impact Assessment*, D. Wright and P. Hert, Eds. Springer Netherlands, 2012, pp. 3–32.

[24] S. Trabelsi, A. Njeh, L. Bussard, and G. Neven, "PPL Engine: A Symmetric Architecture for Privacy Policy Handling," *W3C Workshop on Privacy and data usage control*, 2010.

[25] B. Schneier and J. Kelsey, "Secure Audit Logs to Support Computer Forensics," *ACM Trans. Inf. Syst. Secur.*, vol. 2, pp. 159–176, 1999.

[26] M. Bellare and B. S. Yee, "Forward Integrity for Secure Audit Logs," University of California at San Diego, Tech. Rep., 1997.

[27] B. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an Encrypted and Searchable Audit Log," in *The 11th Annual Network and Distributed System Security Symposium*, 2004.

[28] D. Le Métayer, E. Mazza, and M.-L. Potet, "Designing Log Architectures for Legal Evidence," in *SEFM*. IEEE Computer Society, 2010, pp. 156–165.

[29] Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), "Break-Glass: An Approach to Granting Emergency Access to Healthcare Systems," 2004.

[30] D. J. Weitzner *et al.*, "Transparency and End-to-End Accountability: Requirements for Web Privacy Policy Languages," *Proceedings of the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, 2006.

[31] E. Bertino *et al.*, "End-to-End Accountability in Grid Computing Systems for Coalition Information Sharing," in *CSIIRW '08*. ACM, 2008, pp. 29:1–29:3.

[32] S. Pearson, "Privacy Management in Global Organisations," in *Communications and Multimedia Security*, ser. LNCS, B. Decker and D. Chadwick, Eds. Springer Berlin Heidelberg, 2012, vol. 7394, pp. 217–237.

[33] Terry McQuay, "Demonstrating Accountability With a Scorecard Framework," 2013.

[34] CNIL, "Délibération 2011-316," *Journal officiel de la République française*, vol. 0255, 2011.

[35] ICO, "Auditing data protection — a guide to ICO data protection audits."