Personal Data Management: An Abstract Personal Data Lifecycle Model

Majed Alshammari and Andrew Simpson

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford OX1 3QD, UK
firstname.secondname@cs.ox.ac.uk

Abstract. It is well understood that processing personal data without effective data management models may lead to privacy violations. Such concerns have motivated the development of privacy-aware practices and systems, as well as legal frameworks and standards. However, there is a disconnect between policy-makers and software engineers with respect to the meaning of privacy. In addition, it is challenging: to establish that a system underlying business processes complies with its privacy requirements; to provide technical assurances; and to meet data subjects' expectations. We propose an abstract personal data lifecycle (APDL) model to support the management and traceability of personal data. The APDL model represents data-processing activities in a way that is amenable to analysis. As well as facilitating the identification of potentially harmful data-processing activities, it has the potential to demonstrate compliance with legal frameworks and standards.

Key words: data privacy, data lifecycle model, privacy-aware data processing, compliance demonstration

1 Introduction

Privacy is typically articulated at a high level of abstraction. Thus, its concrete manifestations are ambiguous to those concerned with data protection and to those responsible for developing and maintaining systems [1, 2]. Further, incorporating privacy requirements into the early stages of the development process requires an appropriate interpretation of legal, social and political concerns [3]. These challenges lead to a disconnect between policy-makers and software engineers with regards to conceptualisations of privacy, its related concepts, and the ways in which systems can be developed to comply with legal frameworks and standards and to meet data subjects' expectations [4]. As such, there is a need for generalised techniques that support the effective translation of abstract privacy principles, models and mechanisms into implementable requirements [1, 4].

The dominant approach to embedding privacy into the early stages of the development process is Privacy by Design (PbD) [5]. The principles of PbD are given at a high level of abstraction, which leads to challenges with regards to translation into engineering activities [3]. Data minimisation has been proposed

as a necessary and foundational step to engineer systems in line with the principles of PbD [3] — but ensuring data minimisation is itself a challenge.

To achieve the aim of PbD, detailed privacy impact and risk assessments need to be conducted with the aim of identifying and addressing potential privacy risks [6]. A Privacy Impact Assessment (PIA) provides non-technical guidelines for stakeholders on identifying high level privacy requirements; however, it does not provide guidelines on translating these into technical system requirements [2]. In order for a PIA to be holistic and effective in supporting such translation, it needs to be complemented by an appropriate privacy risk management model; it also needs to be complemented by a sufficiently robust model that serves as the basis for the identification, analysis and assessment of potential privacy risks in a proactive, comprehensive and concrete manner. The representation of such a model tends to be relatively straightforward, capturing possible states and possible changes in these states brought about by operations [7].

Often, legal frameworks and standards are given at a high level of abstraction without relying on rigorous models that explicitly specify privacy-related concepts [8]: types and sensitivity of personal data; the purposes for, and the manner in which, this data is processed; involved actors; and assigned roles and responsibilities. An abstract data model can play a crucial role in providing a privacy-aware data lifecycle model in the context of data protection. Further, such a model can be a stepping stone for translating privacy requirements into system requirements by defining a foundation for contextual analysis.

The abstract data lifecycle model (ADLM) [9] was developed to serve as a generic data lifecycle model for data-centric domains, and can be used as a means to classify, compare and relate other data lifecycle models, as well as to provide the basis for new data lifecycle models [9]. It is the starting point for our contribution. We present an Abstract Personal Data Lifecycle (APDL) model that represents the personal data lifecycle in terms of lifecycle stages, along with associated activities and involved actors. The APDL model can be used to complement a PIA for describing the planned, actual and potential processing of personal data, which, in turn, helps facilitate the management and traceability of the flow of personal data, as well as the identification of data-processing activities that may lead to privacy violations or harms in a comprehensive and concrete manner. Furthermore, it has the potential to help demonstrate privacy compliance with legal frameworks and standards. Finally, it has the potential to underpin a conceptual framework for privacy engineering with the aim of helping stakeholders reason about design decisions.

2 Foundations

In the context of data-centric domains, data undergoes a variety of actions — including creation, use, publication and destruction — by several actors for various purposes. These actions in combination constitute a data lifecycle. It is understandable that each domain is concerned with a specific type of data and each data lifecycle model has its own specific focus. Most importantly, they all

consider the same item of interest — data, which is a "living thing" that moves though various stages during its lifecycle and is at the heart of these systems [9]. In the context of data protection, personal data often moves through various stages that are governed by laws, regulations or standard principles. Accordingly, personal data should be at the heart of methods, techniques and tools that systematically and proactively identify and address privacy risks at the early stages of the design process.

The Abstract Data Lifecycle Model (ADLM) [9] was derived from specific instances of data lifecycle models to ensure broad coverage and wide applicability [9]. For each domain, a list of models was analysed in terms of their lifecycle phases, features, roles, actor features and metadata features. By analysing, comparing and contrasting these models, the ADLM was derived as an abstract data lifecycle model for data-centric domains. It establishes five areas of classification: lifecycle phases, features, roles, actor features, and metadata features. The ADLM provides a means to classify, compare and relate other data lifecycle models, and provides the basis to develop new lifecycle models [9].

The ADLM considers some aspects pertain to data-centric domains, which are of central importance, such as metadata. It provides a set of features to describe the primary data in relation to its sources, contents and domains, with the aim of supporting data production, retrieval and consumption. Metadata features require additional features for characterising the data lifecycle and involved actors, such as those features explained in [9]. As such, we illustrate only the parts of the ADLM that are relevant to representing personal data processing activities in a way that is amenable for analysis: lifecycle phases and roles. The ADLM consists of the following lifecycle phases: ontology development, planning, creation, archiving, refinement, publication, access, external use, feedback and termination [9]. Further, the ADLM considers the following roles: ontology designers, data creators, metadata creators, administrators and end users.

3 The APDL Model

The APDL is an abstract model that represents personal data processing in terms of states (data items), operations (processing activities), and roles (actors). It identifies a set of stages through which personal data moves during its lifetime and indicates the order and depth in which associated activities can occur. We will use and adapt features of the ADLM as points of reference for analysis.

3.1 Lifecycle Stages

As there are obligations and limitations on the stages of the personal data lifecycle and associated activities, our analysis of the ADLM has to consider such concerns. Some stages will be combined — generalised — according to their characteristics and associated activities, while others will be defined — specialised — to limit associated activities to particular privacy principles. Those stages not relevant to personal data will be discarded.

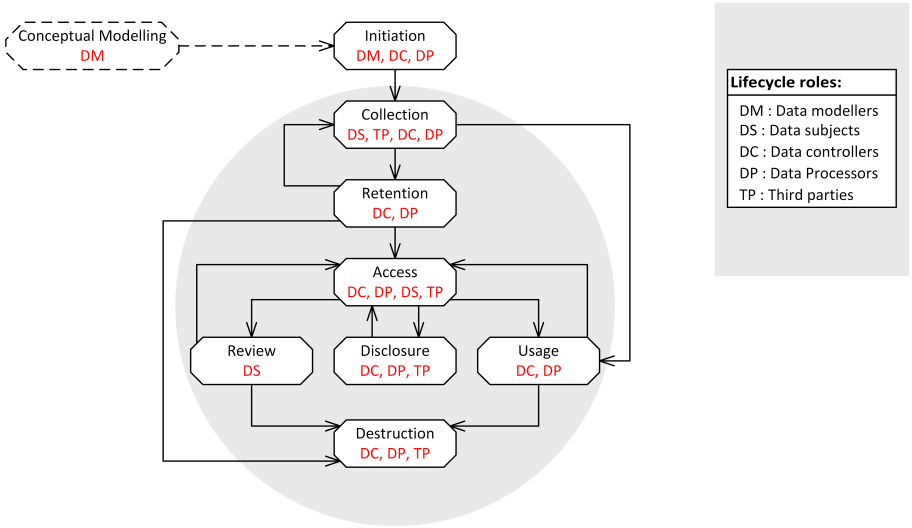

Fig. 1. The Abstract Personal Data Lifecycle (APDL) Model.

It is essential to adopt a set of universal privacy principles that can be applied in a variety of contexts in various jurisdictions. As an example, the Fair Information Practice Principles (FIPPs) were developed as core principles of the Code of Fair Information Practice [10]. In 2006, at the 28th International Data Protection and Privacy Commissioners Conference, the Global Privacy Standard (GPS) [11] was accepted as a unified set of principles that reflects appropriate variants of the FIPPs. The GPS principles harmonise various sets of the FIPPs into universal privacy principles. We adopt the GPS principles to impose constraints on the stages of the lifecycle and associated activities.

Figure 1 illustrates the main stages of the APDL model, their logical dependencies on other stages, and relevant lifecycle roles. Table 1 summarises the personal data lifecycle stages, associated activities and dependencies in terms of inputs and outputs. We describe only the Collection stage in detail.

Conceptual Modelling constitutes a preliminary stage: it involves activities to develop a conceptual model that describes the problem and its solution in terms of the domain vocabulary. It represents key and relevant concepts, associated meanings, properties, relationships and constraints that restrict the semantics of the concepts and their conceptual relationships. Such a model can be used to facilitate communication with multiple stakeholders. It is represented by a dotted line to distinguish that it is not a core part of the personal data lifecycle.

Next, the *Initiation* stage involves activities to define a 'complete processing plan' that specifies the purpose for, and the manner in which, personal data is collected and processed in relation to the context. This is the basis for establishing a privacy notice to be communicated to data subjects.

The Collection stage involves activities pertaining to recording, capturing and collecting personal data values, whether these values are directly collected from

Table 1. The stages, associated activities and dependency of the APDL model.

#	Stage	Activities	Input	Output
0	Conceptual Modelling	Specification Conceptualisation Representation	Domain knowledge	A conceptual model
1	Initiation	Specification	A conceptual model Privacy policies and procedures	A processing plan A privacy notice
2	Collection	Specification Collection or Acquisition	A processing plan A set of data values	A set of collected data values
3	Retention	Specification Storage Archiving Backup	A processing plan A set of collected data values	A set of stored data values
4	Access	Specification Retrieval	A processing plan A set of data items	A set of retrieved data values
5	Review	Review Rectification	A processing plan A set of retrieved data values	A set of rectified data values
6	Usage	Specification Manipulation Presentation Use	A processing plan A set of retrieved data values	A set of manipulated data values
7	Disclosure	Preparation Dissemination or Transmission or Make available	A processing plan A set of retrieved data values	A set of disclosed data values
8	Destruction	Erasure or Disposal or Destruction or Anonymisation	A processing plan Retention policies Destruction policies A set of data values	A set of destroyed data values

data subjects or have been acquired from external sources. The most important aspects in this stage are the set of personal data values, associated sources (i.e. whether they are primary or secondary sources), and the methods of collection (i.e. whether they actively or passively collect data values). In terms of dependencies, the input is a data-processing plan from the Initiation stage, and the output is a set of recorded, captured or collected personal data values to be used as inputs to the Retention stage. The relevant GPS principles are: Openness, Purposes, Consent and Collection Limitation. According to these principles, we identify four essential assessment criteria: personal data items need to be adequate, relevant and not excessive in relation to the specified purpose; the specified personal data has been collected by lawful and fair methods; the privacy notice has been communicated to data subjects at or before the time of collection;

and the consent of data subjects have been obtained. If these are satisfied, data values can be recorded or collected; otherwise, corrective actions can be carried out. Depending on the unsatisfied criterion, the process will continue, either by specifying the minimum amount required of data items, specifying lawful and fair collection methods, communicating the privacy notice to data subjects at the collection time, or by obtaining their explicit or implicit consent.

The *Retention* stage follows the Collection stage, and involves organising, structuring and storing personal data values for a specific period of time in repositories or digital storage media. The *Access* stage follows the Retention stage, and involves specifying and retrieving personal data.

The *Review* stage follows the Access stage, and involves activities for implementing the access right and rectifying personal data values by data subjects to ensure that their data is accurate, complete and up-to-date. The *Usage* stage follows the Access stage, and involves activities for manipulating and using personal data values in conformance with the specified purpose.

The *Disclosure* stage follows the Access stage, and involves activities for disseminating, making available or transmitting the previously accessed and retrieved personal data for external use by third parties. The *Destruction* stage follows the Retention, Collection, Review and Usage stages, and involves activities for erasing, destroying, redacting or disposing of personal data in accordance with relevant retention and destruction policies.

3.2 Lifecycle Roles

A lifecycle role is a set of logically related activities that are expected to be conducted together and assigned to different actors according to their capabilities. They define the ways in which actors participate in the activities of the lifecycle stages. We analyse the lifecycle roles of the ADLM and specialise these roles for the purposes of the APDL model. Each actor may be assigned to one or many roles and each role will typically be associated with one or more lifecycle stages.

1. *Data modellers* are involved in the Conceptual Modelling stage and establish the context in which personal data is processed. In addition, they are involved in the Initiation stage and are responsible for developing logical and physical models for the application domain.
2. *Data subjects* are involved in the Collection stage with the capability of providing their personal data. Such actors can actively participate in the collection of the personal data values. Data subjects may be involved in the Access and Review stages with the capability of accessing and rectifying their personal data. Actors with this ability can access, review, update or correct their personal data to ensure that the retained personal data is accurate.
3. *Data controllers* are actors who specify the purpose for, and the manner in which, personal data is to be collected and processed. They are involved in the Initiation, Collection, Retention, Access, Usage, Disclosure and Destruction stages with administrative capabilities. Such actors are responsible for handling personal data items without changing its format or meaning. If the

data controller is a data processor, administrators are responsible for archiving, making backup copies, disclosing and destroying personal data items. The administrative capabilities may also include other activities, such as those related to compliance monitoring and audit trails. Data controllers are also involved in the Access and Usage stages with different levels of user capabilities. Such actors manipulate and use the retained personal data items according to the purpose for which this data is collected. They perform data-processing activities, including classification, analysis, manipulation, combination or other actions as per the processing plan.

4. *Data processors* are actors who process the collected personal data on behalf of the data controller. They are involved in the Retention, Access and Usage stages and process personal data items without changing their format or meaning. Such actors are responsible for archiving, making backup copies and destroying personal data items according to the data controller instructions. The role of data processors may also include other responsibilities, such as those related to operations and performance monitoring.
5. *Third parties* are actors other than data subjects, data controllers or data processors. They may be involved in the Collection stage with data-providing capabilities, i.e. they may be secondary sources other than data subjects. Such actors actively participate in the collection of the personal data values. In addition, third parties may be involved in the disclosure stage of the lifecycle with data-receiving capabilities. Such actors receive and use the disclosed personal data items only for the purposes specified in the processing plan and with the consent or knowledge of data subjects.

4 Case Study

4.1 Overview

Our concern is the ePetition system, the aim of which is to implement the European Citizens' Initiative (ECI)[1]. The ECI is used to support a formal request to an authority for submitting a proposal for a legal act. It enables EU citizens to invite the European Commission to propose a legal act on issues where it has competence to legislate. The main purpose of the ePetition system is to verify and certify the number of valid signatures that support a certain initiative. In order for signatories to support a specific initiative, they need to provide 'identifying' personal data, which is typically retained in databases. In compliance with applicable regulations, data controllers are required to apply appropriate security measures to protect the collected personal data, and ensure that it is used only for the specified purposes and retained only as long as necessary.

The first step involves establishing a citizens' committee of at least seven EU citizens. All of the committee's members need to be permanent residents or citizens of the EU Member States and old enough to vote in elections to the European Parliament. This committee acts in its capacity as the official organiser

[1] `http://ec.europa.eu/citizens-initiative/public/welcome`

of the initiative and is responsible for preparing and managing the initiative. Second, the organisers need to prepare an initiative and register it with the European Commission. The organisers also need to find a hosting provider when signatures are intended to be collected electronically by an online collection system — either using an instance of the open source software that is provided by the European Commission and hosting it at its site, or by developing their own collection system and using a hosting service provider. For both, organisers need to obtain a certificate from the competent national authority to verify its compliance with minimum technical requirements[2]. Then, the certificate should be posted in the online collection system. Next, individuals, who act as signatories, are able to submit their personal data and their statements of support. To give their support for the initiative, signatories need to provide the specified personal data. It is important to ensure that duplicate signatures by the same individual are avoided. Having reached the required number of signatures, organisers should send this personal data to relevant competent national authorities for verification and certification. Having received all certificates from competent national authorities, organisers should submit the initiative by sending these certificates to the European Commission.

In accordance with the EU Data Protection Directive[3] and the Regulation (EU) No. 211/2011 on the Citizens' Initiative[4], organisers and competent national authorities act as data controllers. In particular, organisers are required to notify the Data Protection Authority in the EU Member State where the personal data will be processed. They are also required to apply appropriate measures to protect personal data in compliance with the Directive and relevant regulations. This includes that personal data must be "adequate, relevant and not excessive" in relation to the purpose of supporting the initiative and verifying the statements of support. Accordingly, the organisers and the competent national authorities must ensure that collected personal data is not used for purposes other than those specified for supporting the initiative and verifying the statement of support respectively. In addition, the data controllers must destroy all statements of support and any copies one month after submitting the initiative to the Commission or issuing the certificate respectively.

4.2 Lifecycle Stages

Initiation. In accordance with the aforementioned EU Data Protection Directive and the Regulation (EU) No. 211/2011 on the Citizens' Initiative, organisers are required to notify the Data Protection Authority in the EU Member State where the personal data will be processed before the collection of statements of

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:301:0003:0009:EN:PDF

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02011R0211-20131008&from=EN

support. This requires a complete processing plan that may serve as the basis of developing a privacy notice. The processing plan needs to outline: the elements of personal data to be collected, along with its sources; the purposes for, and the manner in which, this data is processed; the methods of collection, retention, retrieval, disclosure and destruction; the choices available to data subjects and the consent to be obtained; the involved actors and their assigned roles and responsibilities; relevant regulations and standards; and the domain-specific constraints. The specification of the required data is driven by the specification of purposes for which personal data is to be processed. In this case, the main purpose of collecting and processing signatories' personal data is to verify and certify the valid number of the submitted statements of support. In addition, logical and physical models need to be developed.

Collection. Once an initiative's registration has been confirmed, the relevant Data Protection Authority has been notified and the online collection system has been certified, the organisers may use an online collection system to collect the specified personal data from at least one million EU citizens who act as signatories. The specified data is collected within a specific time limit (no longer than 12 months from the date of registration). Importantly, the collected personal data values must not exist in the lifecycle before the collection to prevent duplicate statements of support. In order for organisers to collect adequate, relevant and not excessive personal data, the collection system must generate statements of support in an appropriate form.

Retention. The statements of support that have been submitted by signatories are required to be persistently stored in a primary storage media for operational purposes. One might also assume the existence of copies of the original personal data for operational recovery purposes. Once the collection period is finished and the personal data is sent for verification and certification, competent national authorities have three months to certify the number of valid statements of support. During this period, the retained data is no longer needed for regular use by the organisers and can be archived as historical data for compliance purposes. Having submitted the received certificates, organisers have one month to destroy the retained personal data and any copies thereof or 18 months from the date of the registration of the initiative, whichever is the earlier. Signatories' personal data or any copies thereof may be retained beyond the specified retention time for the purpose of legal or administrative proceedings relating to an initiative. This requires retaining statements of support and any copies thereof for one week after the date of conclusion.

Access. During the collection period, organisers need to monitor the collection of statements of support that have been submitted. Once the collection of the statements of support have been de-activated at the end of the collection period, organisers need to export signatories' personal data from statements of support and display the current signatures distribution, which are classified according to the Member State of signatories or the date of submission. These activities

require specifying and retrieving the retained statements of support. In particular, signatories' personal data needs to be made accessible for use by involved actors, in this case, internal users who acting as organisers.

Review. Data subjects cannot access their personal data once they have submitted their statements of support. Thus, the ePetition system that implements the ECI does not provide signatories with full control over their personal data.

Usage. Signatories' personal data is collected and processed for verifying and certifying the number of valid statements of support. In this case, organisers manipulate, classify and use this data to fulfil the specified purpose. These include monitoring, deleting, exporting, preparing and sending statements of support to relevant competent authorities. The actual use of signatories' personal data is accomplished by relevant competent authorities as they conduct the verification process and produce certificates for valid statements of support.

Disclosure. Statements of support are used only for verification and certification; they cannot be disclosed to any other parties.

Destruction. Removing statements of support is the final stage. Signatories' personal data are required by law to be destroyed after a specific time limit. Statements of support need to be completely and permanently erased, and digital storage media needs to be destroyed. Original, archived or backup copies of the retained statements of support need to be disposed in accordance with relevant retention and destruction policies.

4.3 Lifecycle Roles

The *data modeller* role may be assigned to capable actors who are able to define appropriate conceptual, logical and physical data models for the context of participatory democracy and, in particular, for the ePetition system.

Citizens or permanent residents of the EU Member States act in their capacities as *data subjects* who are able to provide their personal data. They actively participate in the collection of personal data with the aim of supporting an initiative. However, data subjects are not able to access and review their personal data once they have submitted statements of support. Data subjects are mainly involved in the Collection stage. Organisers and competent national authorities act in their capacities as *data controllers*. Organisers are responsible for specifying the purpose for the required personal data, and the manner in which it is to be collected and processed. They are responsible for collecting, monitoring, preparing and sending personal data to competent national authorities. The competent national authorities are responsible for verifying and certifying the number of valid statements of support for an ECI.

Data controllers may act in their capacity as data controllers and processors at the same time if they are capable of operating the online collection system. Second, the European Commission may act in its capacity as a hosting service

provider by providing the OCS. The third case is a third party that acts in its capacity as a hosting service provider. In all cases, data processors are responsible for handling personal data without changing its format or meaning. They are responsible for archiving, making backup copies and destroying this data according to the data controllers' instructions.

5 Conclusions

The integration of privacy into the early stages of the design process of business processes and their underlying systems is increasingly important — PIAs and PbD are now mandated by, for example, the EU General Data Protection Regulation (GDPR)[5]. Crucially, a PIA needs to be complemented by a sufficiently robust model that represents data-processing activities in a way that is amenable to risk analysis and compliance checking. To this end, we have introduced the APDL. Each stage is an abstraction of a set of logically related data-processing activities. This classification is based on the GPS principles, the nature and order of processing activities, and the role type of involved actors and their possible responsibilities. This gives the APDL model the possibility to be applied to various domains, including dynamic and interconnected scenarios where data is collected from different sources with different formats. In addition, it supports the applicability of the model when there is more than one domain, as well as when data is collected and processed collaboratively by multiple stakeholders by determining who is responsible for which lifecycle stage and their level of authority with respect to the decisions and activities performed.

The APDL model distinguishes between the types of operations that can be performed on personal data. For each operation, it outlines various distinct activities in relation to the GPS principles with the aim of governing the behaviour of these operations. The separation is important for several reasons: it helps support the manageability and traceability of the flow of personal data during its lifecycle; it is necessary for ensuring and demonstrating compliance with legal frameworks and standards; it reflects the extent to which the flow of personal data is appropriate in terms of involved actors and their assigned roles and responsibilities; and it facilitates the identification of data-processing activities that may lead to privacy violations or harms.

We limit our model to those terms that are necessary to define the fundamental concepts of the personal data lifecycle. These might be further refined and extended by developing a conceptual model that precisely represents all relevant concepts, associated meanings, properties and relationships. For example, the lifecycle may be characterised by properties that help support its application in various domains, such as the type of the lifecycle, the openness of the processed data, and the centrality of the underlying system. Furthermore, the APDL model has been informally represented, which, in turn, affects the pos-

[5] `http://www.eugdpr.org/`

sibility of integrating such a model into an appropriate engineering process to elicit and model system requirements and to provide technical assurance.

We will next define a conceptual model that describes the problem and its solution in terms of the domain vocabulary as a prerequisite to any data lifecycle n the context of data protection. We intend to define a profile that allows the APDL model to be represented in the Unified Modeling Language (UML)[6] to illustrate how to address the complexity of practice, provide technical assurance and facilitate reasoning about compliance. Such a UML profile for the APDL model has the potenital to complement the contributions of [3], [12] and [13], by providing foundations for analysing functional requirements and assessing potential privacy risks. We also plan to use additional case studies with the aim of further validating the applicability of the model.

References

1. Shapiro, S.S.: Privacy by Design: Moving from Art to Practice. Communications of the ACM **53**(6) (2010) 27–29
2. Kost, M., Freytag, J.C., Kargl, F., Kung, A.: Privacy Verification using Ontologies. In: Proceedings of the Sixth International Conference on Availability, Reliability and Security (AReS 2011), IEEE (2011) 627–632
3. Gürses, S., Troncoso, C., Diaz, C.: Engineering Privacy by Design. Computers, Privacy & Data Protection **14** (2011)
4. Spiekermann, S.: The Challenges of Privacy by Design. Communications of the ACM **55**(7) (2012) 38–40
5. Cavoukian, A.: Privacy by Design ... Take the Challenge. Office of the Information and Privacy Commissioner of Ontario (2009)
6. Cavoukian, A.: Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. `https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=953` (2010)
7. Cavoukian, A., Shapiro, S., Cronk, R.J.: Privacy Engineering: Proactively Embedding Privacy by Design. `https://www.privacybydesign.ca/content/uploads/2014/01/pbd-priv-engineering.pdf` (2014)
8. Antignac, T., Scandariato, R., Schneider, G.: A Privacy-Aware Conceptual Model for Handling Personal Data. In Margaria, T., Steffen, B., eds.: International Symposium on Leveraging Applications of Formal Methods (IsoLA 2016), Springer (2016) 942–957
9. Möller, K.: Lifecycle Models of Data-centric Systems and Domains: The Abstract Data Lifecycle Model. Semantic Web **4**(1) (2013) 67–88
10. United States Department of Health, Education and Welfare: Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens: Report. MIT Press (1973)
11. Cavoukian, A.: Creation of a Global Privacy Standard. `https://www.ipc.on.ca/images/Resources/gps.pdf` (2006)
12. Spiekermann, S., Cranor, L.F.: Engineering Privacy. IEEE Transactions on Software Engineering **35**(1) (2009) 67–82
13. Hoepman, J.H.: Privacy design strategies. ICT Systems Security and Privacy Protection (2014) 446–459

[6] `http://www.omg.org/spec/UML/`