PRIPARE

PReparing Industry to
Privacy-by-design
by supporting its
Application in REsearch

PRIPARE: A New Vision on Engineering Privacy and Security by Design

Project:	PRIPARE
Project Number:	ICT-610613
Work Package:	WP1: Defining PRIPARE Methodology
Title:	PRIPARE: A New Vision on Engineering Privacy and Security by Design
Date:	10/04/2014
Confidentiality:	Public
Authors:	Antonio Kung (Trialog) Alberto Crespo Garcia (ATOS) Nicolás Notario McDonnell (ATOS) Inga Kroener (Trilateral) Daniel Le Métayer (Inria) Carmela Troncoso (Gradiant) José María del Álamo (UPM) Yod Samuel Martín (UPM)

Funded by the European Union's
Seventh Framework Programme

Table of Contents

1. Introduction

The Universal Declaration of Human Rights declares in Article 12 that "No one shall be subjected to arbitrary interference with his privacy. ... Everyone has the right to the protection of the law against such interference or attacks." [1] Recent revelations of mass surveillance have put privacy at the forefront of political and societal debate and uncovered serious violations and lack of effective respect for this human right. As it is impossible to think of a violation of human rights at such scale in the “offline world" without international condemnation, the UN has reacted to these events in the “digital world” by adopting a resolution that affirms “that the same rights that people have offline must also be protected online, including the right to privacy.” [2] The same resolution also calls on countries “To review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data including mass surveillance, interception and collection.” [2]

In the EU, the current legislative process to approve the EU Data Protection Regulation can be seen to be in line with this UN request and is aimed to effectively strengthen European citizens’ privacy, in particular in the area of personal data protection. As reality demonstrates, a strong and consistent legal framework on its own is not sufficient to guarantee that stakeholders will correctly adopt adequate privacy practices. The Privacy by Design (PbD) concept has been around since the 90’s and Cavoukian’s 7 Foundational Principles [3] of PbD are now widely acknowledged by data protection commissioners world-wide, and there is growing evidence that this truly transformative approach has the potential to create far-reaching impact and benefits for citizens, government and business, as well in several economic, industrial and ICT domains like health, energy, cloud, mobile/communications, NFC/RFID, geolocation, big data/data analytics, surveillance and authentication technologies, etc. While there is a unanimous consensus on the benefit of the principles in terms of privacy awareness, unfortunately there is still a lack of a systematic approach that would help businesses and organisations to include privacy-supportive processes and practices in their products and services. The new European Regulation on Data Protection, in its Article 23, states that controllers shall follow the data protection by design and by default principle, following the opinion of data protection authorities such as:

- The European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy [4],
- The Article 29 Data Protection Working Party: Opinion 01/2012 on the data protection reform proposals [5].

Whenever it is approved, compliance with the new Regulation on Data Protection will further spark interest in the need to follow PbD principles and approach. Some industries particularly vulnerable to privacy risks have anticipated proactively developing tools that address privacy concerns (i.e. the RFID industry and the EU RFID Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) Framework [6]).

PRIPARE (www.pripare.eu) has two important missions: 1) to design and facilitate the application of a Privacy-by-Design and Security-by-Design (SbD) methodology in the ICT research community in preparation for industry practice, and 2) to foster a risk management culture within organisations by preparing best practices material, supporting FP7 and Horizon

2020 research projects, providing educational material on approaches to risk management of privacy, and by identifying gaps and providing recommendations on Privacy and Security-by-Design (PSbD) practices.

The PRIPARE project will forge sustainable links between the different privacy stakeholders (regulators, educators, engineers and standardisation organisms) in order to set the necessary common grounds on which to build trustworthy and privacy-respectful systems. Increasing levels of public trust in ICT systems will:

- Facilitate faster adoption of new services and technologies that feature high and tangible levels of privacy and security embedded into their design and provided by default;
- Increase the speed of innovation and creation of added value for a more competitive European ICT industry;
- Contribute to the advent of unhindered usage of Internet against disruptions, censorship and surveillance.

Results of the project will be included in the Security Engine Forum where other researchers and experts will be able to discuss them: http://www.securityengineeringforum.org/.

2. Taking Privacy by Design One Step Further

The fast evolution of ICT-based systems and services broadens the amount, nature, and purposes for which data are collected. This situation raises serious concerns about the implications of the pervasiveness of ICT systems on users' privacy. According to recent reports from the Eurobarometer [29][30] or independent organizations [31] a majority of internet users are concerned about the uses given to the data they reveal to service providers and fear inferences on their behaviour via payment cards, mobile phones or mobile Internet. In fact, 62% of Europeans choose to provide the minimum required information. These conclusions coincide with those reached by academics, who demonstrate [32] [33] that users confronted with a prominent display of personal data not only prefer service providers that offer better privacy guarantees, but also are willing to pay higher prices to utilize more privacy protective systems.

Privacy of data is not only of relevance for citizens, but also of utmost importance for businesses and governments who increasingly carry out their activities online. The disclosure of mass surveillance programs on individuals, governments, and companies at a worldwide level (e.g. the PRISM[1] case [43]) creates a demand for new protection methods that safeguard sensitive personal data in ICT systems.

The need for privacy protection has been acknowledged by the new European regulation, which fosters the inclusion of Privacy Impact Assessments and Privacy by Design practices in business processes. This shall ensure that all relevant actors (public authorities, the private sector, and individual citizens) will take action and protect themselves in a coordinated manner to strengthen privacy and cyber security.

At the start of the PRIPARE project, it was realised that stakeholders use PbD and Security by Design with different definitions. PbD and SbD are defined as follows in Wikipedia:

[1] The Washington post revealed U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

- PbD is an approach to System Engineering which takes privacy into account throughout the whole engineering process.
- SbD, in software engineering, means that the software has been designed from the ground up to be secure.

We suggest redefining SbD as follows:

- Security by Design is an approach to System Engineering in which measures to protect ICT assets have been designed throughout the whole engineering process.

Consequently, a privacy and security by-design process can be defined as follows:

- An approach to System Engineering which takes into account privacy as well as measures to protect ICT related assets throughout the whole engineering process.

PbD is hailed as the solution to the digital world's privacy problems. It is usually presented as a set of principles that can be applied from the onset of systems development to mitigate privacy concerns and ensure compliance with Data Protection legislation. However, these principles often remain vague and rely on ambiguous concepts, and are hence difficult to apply to engineering systems [35]. There are many open questions and challenges that need to be addressed at both the management and development levels in order to define effective methods to integrate privacy into systems [34]. A variety of approaches are being used to address these privacy concerns throughout the lifecycle of products or systems.

- PIA and risk management processes: these will be discussed in more detail later in this paper.
- OASIS (Organization for the Advancement of Structured Information Standards) standardisation efforts. OASIS is as a non-profit consortium that drives the development, convergence, and adoption of open standards for the global information society. There are currently two Technical Committees (TC) related to PbD:
    - The PMRM TC (Privacy Management Reference Model and Methodology). The objective of PMRM (pronounced pim-rim) is to provide a methodology for developing operational solutions to privacy issues. The starting points are privacy principles, privacy laws and policies, and privacy control statements. The result of the methodology is a technical description of policy services (agreement on policies, control of policies), of assurance services (validation, certification, audit, enforcement) and of life cycle services (interaction, usage, agent, access). A specification of PMRM was issued in July 2013.
    - The PBD-SE TC (PbD Documentation for Software Engineers). The TC objective is to provide privacy governance and documentation standards for software engineers. The first document is planned for 2014.

Very often privacy is (or seems to be) in tension with other requirements, and the design space of data minimisation can be very wide, with different options providing different types of benefits and drawbacks. Therefore it is of prime importance to be able to make reasoned decisions and to be able to justify them. As far as privacy is concerned, these decisions must be based on a privacy risk analysis in which the privacy values at stake are clearly defined, as well as the sources of risks and their potential impact on these values. The result of this analysis should guide the choice of appropriate solutions (architecture and tools) and serve as justification for this choice. Sources like legislation, industry standards, and guidance produced by trade bodies, regulators, or other organisations working in their sector can be used to identify privacy and related risks that then can be minimised.

Once a piece of personal data has been introduced into a system it must be properly managed. Identity management refers to the set of processes that administers the life cycle (collection, authentication, use, and deletion of an identity), and the data linked to it, within an organization and across its boundaries. It has evolved from silo-like approaches, where all the identity information is kept and used within a single organization, to federated, or network-centric, approaches where the underlying infrastructure enables a participating entity to share their users' personal data with others, e.g. by means of the OASIS SAML, Liberty ID-WSF, or OpenSocial technologies, among others.

There is a strong relationship between privacy and identity management. Identity management systems designed to follow privacy and security principles will provide their users with tools that allow them to manage their privacy in a reliable, trustable, and usable way. Failing to follow these principles can lead to flawed systems that pose serious privacy threats like identity theft or unintentional disclosure of personal data.

Several solutions have been proposed to develop a privacy-enhancing identity management infrastructure including the use of pseudonyms and attribute-based (or zero-proof) credentials, privacy policies negotiation, development of usable interfaces and privacy metaphors, etc. [7]. In addition, the identity management domain has begun to consider user-centric architectural and usability aspects, and to support user control to different extents, which is called user-centric identity management. For example, URL-based systems such as OpenID allow users to choose the entity storing their personal data, OAuth enables users to decide on what pieces of information to share, Kantara User Managed Access (UMA) lets an individual control the authorization of data sharing and service access made between online services on the individual's behalf, and card-based systems further allow users to include the pieces of information to be shared with a third party.

3. Converging to a Common Terminology

To enable the development of a methodology addressed to multiple stakeholders from different countries and industries, it is necessary to define a common terminology that facilitates communication to be straightforward and without ambiguities. There are many sources of terminology for the domains of privacy, security, and risk management. The most relevant sources for terminology for PRIPARE are:

- ISO (ISO 29100 [16], ISO 15480-2 [17], etc.: given the outreach of ISO standards, the terms defined are widely used and their meanings are commonly accepted internationally.
- EU Data Protection Directive [15][14]: the terms defined are widely used within Europe by stakeholders of various disciplines (advocacy, legal, engineering, business).
- EU Data Protection Regulation [14] (still in draft): this new regulation tries to unify data protection within the EU. It also endeavours to tackle some issues in the European Union Data Protection Directive (EU DPD), e.g. globalization and technological developments.
- PMRM [18]: PRIPARE is not the first project endeavouring to provide an engineering approach to PbD. OASIS PMRM TC has already drafted a first version of its reference model and methodology that includes terminology that can be used within PRIPARE. It provides not only specific terminology but an interesting approach that can be used as a basis for PRIPARE’s methodology.

Beyond the discussion of specific terminology, an initial decision was made in terms of terminology style. In the EU DPD [14], terminology is focused on the term “data” or “personal data”. It defines, in its principles and articles, responsibilities of data controllers, and data processors. It also defines sensitive categories of data. The European Data Protection Supervisor (EDPS), as expected, also follows that naming convention that is also endorsed by the Article 29 Data Protection Working Party [21]. On the other hand, ISO talks about Personal Identifiable Information (PII). Looking at the definitions, both terms refer to the same concept but the wording is different. All concepts in the ISO standards are defined in terms of the PII: PII controller, PII processor, in the same way as the EU DPD does with “data”. The OASIS PMRM [18] also makes use of the ISO wording.

Wording style had to be carefully chosen as only one style should be used within PRIPARE to avoid confusion. A survey among the participants of the consortium unanimously decided to adopt the EU wording style within PRIPARE.

A literature review conducted in the initial stages of the project revealed some terms that can be classified as elusive or controversial:

Accountability

Accountability is a much overloaded word with different meanings and interpretations. Its complexity is well documented in existing literature (e.g. [23], [19] and [20]). At present, the new European Data Protection Regulation Draft [14] includes the concept accountability as one of its new principles. There are several aspects of accountability that should be highlighted and that will be explained in more depth in the PRIPARE’s principles section below.

- Its external and internal dimension
- Legal compliance
- Responsibility.

Consent or Informed Consent

There are various definitions of consent from several sources. According to the Data Protection Directive [15], consent and informed consent are synonymous. The new EU Data Protection Regulation [14] will tighten the meaning of consent, and all consent will be required to be explicit (previously, only consent to processing sensitive data needed to be explicit), which compels the data controller to bear the burden of proof for the data subject’s consent.

Data, Personal Data, Personal Information, or Personal Identifiable Information

When referring to privacy, some sources use the terms "Data", "Personal data" and "PII" to define the same concept. Personal data is often understood as a very limited class of information. PRIPARE will aim to apply PbD to a wider range of data, including apparently harmless data that may leak private information.

Privacy

How to define a PbD methodology without stating the definition of privacy? It is very difficult to agree on a common definition as it is not a universal concept and depends on context. Rather than debate the term's definition, PRIPARE will use the taxonomy proposed by Finn et al. [22] to navigate through privacy issues. The taxonomy is fully detailed in PRIPARE’s principles section.

Proportionality

Proportionality is often used in the EU DPD [15] to dismiss the need to apply some principles or rules if a disproportionate effort is required. The question is how to measure proportionality. In the EU, there is a general doctrine that defines a “proportionality test” to verify the proportionality of a measure. This test includes four stages and could be adopted within PRIPARE’s methodology to self-evaluate the need to apply some of the security and privacy principles.

These terms have undergone a discussion period after which a proposed definition was accepted by a majority of the partners within the consortium. The accepted definitions will be used within PRIPARE as a basis for further work.

4. PRIPARE's Principles

There are a variety of principles that are relevant for the PRIPARE project. The consortium has identified several sources (European Data Protection Directive [15], Proposal for a new General European Data Protection Regulation [14], OECD privacy principles [40] or FTC FIPPs) and had successful discussions regarding the most appropriate principles for the PRIPARE project. The main principles under discussion focused on security, privacy, and data protection. Within these areas, the focus was narrowed towards discussing ideas and principles of data minimisation, personal data, user-centricity, accountability, privacy and consent.

The security principles under discussion by the PRIPARE consortium included applying defence in depth, using a positive security model, avoiding security by obscurity, keeping security simple, and establishing secure defaults. The source for these principles is the OWASP project (Open Web Application Security Project) [42]. The project consortium has accepted these principles preliminarily. The security principles may be further debated with stakeholders as the project progresses

The principles of data protection included in the PRIPARE project for discussion came from the European Data Protection Directive 95/46/EC [15] and from the Proposal for a new General European Data Protection Regulation [14]. These principles include safeguarding personal data, proportionality and data minimisation, compliance with the data subject's right to access and amend their personal data accountability, and the right to deletion. These principles are important in terms of the data lifecycle, from the collection of personal data (and an individual consenting to this collection of their personal data), to processing (and the right of the individual to object to this processing and the principle of proportionality), to the deletion of personal data (and the right of the individual to have his data retained only for a set time period and to have his data erased after this time). To date, the project consortium has agreed on the principles listed. However there may still be a need for the PRIPARE project to include a reference to the use of state-of-the-art technologies and the need for engineers to build in new technological solutions to minimise privacy risks. The data protection principles, including issues such as "what is meant by consent?" will be further discussed with stakeholders as the project progresses. The new draft EU regulation, among multiple other changes, modifies the notion of consent to define it as explicit and informed, rather than implicit. The PRIPARE project will take these new developments into account.

The consortium has also discussed the notion of privacy. Privacy is certainly not a universal concept that can be applied across all technologies and all situations. Finn et al. argue that current attempts to capture the complexities of privacy issues in reactive frameworks are inadequate. They state that "Rights to privacy, such as those enshrined in the European Charter of Fundamental Human Rights, require a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions, infringements and problems." [22]. Finn et al. build upon Clarke's influential conceptualisation of privacy and his taxonomy of privacy based on four categories. They suggest that Clarke's taxonomy is no longer adequate for addressing the range of privacy issues that have arisen with regard to a new and emerging set of systems and technologies. They therefore suggest an approach that encompasses seven types of privacy: privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association. Under this taxonomy, privacy of the person is defined as the right to keep body functions and body characteristics private. Privacy of behaviour and action refers to sensitive issues such as political activities and religious practices. Privacy of communication relates to interception of communications such as recording and access to e-mail messages. Privacy of data and image involves the right of the individual to exercise control over personal data, rather than such data being available to organisations and others by default. Privacy of thoughts and feelings refers to the individual's right to not have to share her thoughts and feelings, or to have these revealed. Privacy of location and space encompasses the right of the individual to freely move about in public, or semi-public space, without being monitored or tracked. Privacy of association refers to the right of the individual to associate with others without being monitored. This approach is beneficial in terms of navigating the various definitions of privacy in the literature to date. Rather than focusing only on personal data and personal communications, as has been the case to date in data protection legislation, the taxonomy proposed ensures that different types of privacy are protected. This is important in relation to Privacy Impact Assessments, which should take into account all seven types of privacy. With regard to the PRIPARE project, it would be beneficial to keep this taxonomy in mind when thinking about Privacy by Design. Rather than getting caught up in the myriad and diverse definitions of privacy, basing the PRIPARE methodology on this taxonomy of seven types of privacy will move the debate forward as opposed to reinventing the wheel.

Accountability in relation to privacy and data protection has also become a widely debated topic in recent years. EU discussions on accountability suggest that current legal regulations for protecting privacy are inadequate and that without a change in the current direction, the problems of data protection are set to continue. Furthermore, commentators in the field have suggested that "Accountability can form the focus for dealing with issues of scale in regulation, privacy risk assessment, self-regulation through certification and seals and foster an environment for the development of new technologies for managing privacy." [36]. Finally, accountability is tied together with legal compliance and the idea that those who control data should, on request, be able to show compliance with data protection legislation. Although these discussions place accountability at centre stage, the practicalities of achieving accountability in practice are left open to further debate. The definition of accountability is also widely debated. Bennett argues that accountability means more than responsibility and suggests that it "implies a process of transparent interaction, in which [an external] body seeks answers and possible rectification." [39]. The involvement of an external body is therefore imperative – a means by which the other body is called to account. For Mulgan, there is a clear distinction between "having to account to someone else for one's actions and not having to do so." [23]. For the purpose of the PRIPARE project, the definition of accountability that will be used is the one that appears in the EDPS glossary: "The principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities" [20]. However, the consortium is aware that there is much more to accountability than that which is listed in the quote (as already outlined in this paragraph).

The starting point of PRIPARE's methodology is the idea of minimising the trust that users need to place on the data controllers or data processor which will be collecting, storing and processing their personal data. This principle implicitly ensures that the data minimisation principle is fulfilled, since the best approach to minimise trust is to minimise the amount of data that needs to be entrusted[2]. The methodology will seek to minimise the amount personal data distributed to potentially untrustworthy parties, which in turn minimises the risk of privacy breaches

5. Adopting Best Practices on PIAs and Risk Management in PRIPARE PSbD Methodology

PRIPARE will adopt identified best practices on PIAs and risk management processes to provide an unobtrusive methodology that will complement existing system development and project management methodologies. This way PRIPARE's methodology or reference model will ensure and ease the process of building privacy-friendly systems, bridging the gap between the abstract notion of Privacy by Design and the concrete system designing and building process.

PRIPARE's PSbD methodology aims to be holistic. This means that:

- It can be applied to systems or subsystems that compose it, even those being designed separately.
- It must be adaptable to the specific aspects of each domain specific standard.
- It must also take into account the various types of systems, from the small to huge applications.

PRIPARE will propose a simple typology of projects based on the positioning of the focus:

- Projects focusing on application features, i.e. features that are useful to the customer, for instance a smart meter application,
- Projects focusing on technology or platform features, i.e. platform features that are useful to the application designer, for instance an operating system or a protocol system.

It is at this point that different guidelines for PbD are needed depending on the type of project.

A recent PIA framework developed for RFID has been cited as being a "landmark PbD document" [8]. The framework is the first of its kind to be sector-specific and developed by industry. It provides guidelines on how to process data specifically related to RFID applications, and how to assess privacy and data protection issues through PIAs. Spiekermann states that the framework "suggests concrete privacy goals and describes a method to reach them." [9] In order to be effective, PIAs need to move beyond legal compliance checks in order to "offer a prospective identification of privacy risks before systems and programmes are put in place," and that they "have to consider privacy risks in a wider framework which takes into account the broader set of community values and expectations about privacy." [10]

PIAs should not be considered as simply legal compliance checks, which ask: If we did X, would we be in compliance with the law and the fair information principles upon which the law is based? Nor should they be considered to be privacy audits used to assess existing technologies,

[2] "Protecting privacy by minimizing trust" is an on-going work from some of PRIPARE partners that will be published in the future.

although, as Wright argues, a PIA can enable an organisation to demonstrate compliance with legislation in the case of a privacy audit or complaint. Undertaking a PIA can “provide evidence that the organisation acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.” [11]. A 2007 Linden Consulting report [10] for the ICO states that they are most useful for new programmes, services or technologies. However, they are not simply used to warn against potential risks but also to mitigate these risks, and to change the development process accordingly. PIAs, therefore, move beyond the legal compliance to assess and address the “moral and ethical issues posed by whatever is being proposed” [12]. The Ontario Data Protection guidance states that the “cyclical nature of the information life cycle must be supported by appropriate policies, practices, procedures, tools and contracts”. With reference to this life cycle of information, the guidance states that “risk must be properly identified, minimised to the extent possible and appropriately managed where it can't be eliminated” and “a proper contemplation of the information life cycle includes these concepts”. A privacy impact assessment is one of the ways that the information life cycle can be managed and privacy risks minimised [13].

Wright suggests that there is currently a “growing interest in Europe in privacy impact assessment” [11]. The UK introduced the first PIA methodology in 2007, although PIAs have been used in Australia, Canada, New Zealand and the United States since the mid-1990s. Conducting a PIA is now mandatory for government agencies in the UK, Canada and the US. It has been found that “unless they are mandatory, many organisations may not undertake them even though their projects, technologies or services have serious privacy impacts” [11]. In terms of best practice, Wright concludes that a PIA process should include:

- An assessment of privacy risks an organisation might face in relation to a new project (although he cautions that a PIA on its own will not highlight all privacy risks and/or issues associated with a new project),
- A process of engaging stakeholders (including external stakeholders);
- Examples of specific risks,
- Recommendations and an action plan,
- Third party reviews,
- Benchmarks that organisations could use to test how well they are following the process,
- Publication of the PIA report,
- PIA updates if there are changes in the project.

PRIPARE will embrace and incorporate this view of PIAs in its procedure and reference model approaches.

Ideally, a PIA should include (or be complemented by) a privacy risk analysis. Inspiration can be drawn from the security area which has a long experience in risk analysis. Risk analyses in this area typically includes well identified steps such as the definition of assets, the identification of threats, vulnerabilities, attacks, etc., leading to a decision making phase (risk acceptance, mitigation, avoidance, etc.). In the case of privacy, the decision should involve the choice of specific architectures and technologies (PETs). However PIAs differ from traditional security analyses in several ways: privacy properties are not similar to security properties (even if related), privacy itself is more difficult to grasp than security, and the decision making phase should involve all stakeholders. So the transposition of security risk analysis to privacy analysis is not straightforward and warrants serious thought.

In general, the PIA should be followed up with the recommendation that a third party review and/or audit of an organisation's PIA be conducted as "it is all too easy for project proponents to say initially that they accept and will implement suggested changes, only to find reasons later to back-slide, and either partially or wholly abandon their initial commitment" [11]. In terms of best practice, Wright also suggests that, in addition to a third party review, accountability mechanisms, such as mandatory reporting requirements, should be implemented. Finally, Wright argues that tying PIAs to budget submissions for new projects and programmes can ensure that a greater number of PIAs are actually undertaken, as well as enhancing accountability.

6. Embedding PbD (and SbD) into Current Methodologies

Until the 20th century, engineering projects were usually managed by the engineers themselves. It was not until the 1950s that project management appeared as a specific discipline that would provide tools and techniques to engineer complex projects.

From the beginning of a system until its disposal there are several phases that are considered as the *System Lifecycle.* The management of the different phases of the lifecycle usually follows some methodology. Different methodology types can be used to manage this life cycle and often project management and system development methodologies are mixed to provide an ad-hoc methodology that can be used through the entire system lifecycle. Figure 1 depicts the usual stages that can be found in project development methodologies.

PRIPARE will have to provide a way to integrate its methodology steps into existing and widely-adopted project management methodologies as it will involve a series of tasks that affect not only the engineering process itself but also resource allocation and organizational requirements. Special focus will be made on the most extended PM methodologies: PMBOK and PRINCE2.

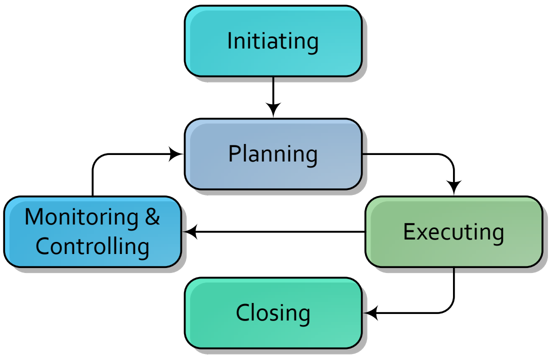

Figure 1: Usual project development stages.

By addressing the integration of the PSbD methodology with the most extended system development and project management methodologies, PRIPARE will embed its principles (from the EU DPD, the new EU Data Protection Regulation Draft, Cavoukian's PbD Foundational Principles, OWASP security principles, etc.) and best practices (in PIAs, risk assessment, Security by Design) into new to-be-developed ICT systems.

As it is impossible to address integration with all existing system development methodologies, this integration will be focused on methodology families or similar methodologies. The integration of methodologies will be addressed by using the general description of a methodology family (e.g. waterfall, iterative, incremental, prototype), or by using a representative methodology of the family (scrum as representative of agile methodologies).

Complementing some of the methodologies may be quite easy as they have similar stages that can be matched. However, others (i.e. scrum) pose great challenges, such as:

- How to implement PbD in a methodology that has no design stage?
- How to reflect privacy requirements in a methodology that only uses user stories?

These issues will have to be tackled during the methodology design in order to provide an effective and applicable privacy and security-by-design software and systems engineering methodology. PRIPARE's methodology will have to be as unobtrusive as possible to encourage adoption. This can be achieved by making some steps optional or by being less prescriptive in *how* things should be done (however, an idea or an example of "how" should always be provided to ease the adoption process).

7. Conclusion

PRIPARE will consider existing PETs, risk management methodologies, PIA frameworks and other approaches to engineer and operationalize PbD (i.e. OASIS PMRM [18]) with the objective of providing an easily applicable methodology suitable for different stakeholders (engineers, decision makers etc.). This will defuse some of the worst PbD critics regarding its chances of adoption [26] such as: "More aspirational than practical or operational" and "Difficult to be implemented into engineering practices."

It will also ensure that systems developed with the methodology will follow PRIPARE's security and EU Data Protection Directive and Draft Regulation's data protection principles and privacy best practices.

PRIPARE will develop a truly positive-sum methodological approach for engineering privacy into ICT Systems software design and development lifecycles that will be:

- Short, easy-to-understand, and easy-to-use,
- Principles-based,
- Provisioned with risk assessment standards,
- Designed to cover the whole system lifecycle,
- Flexible so it can adapt depending on the nature of the project and the information collected,
- Useful for different stakeholders,
- Engaged with engineering practices.

To achieve this, PRIPARE's methodology will embrace current PIA practices, extending them with the best PIA practices as determined by different studies and projects (e.g. [27] and [28]). It will include a complete and standard risk assessment process to minimise privacy and security risks. The methodology will be designed to provide tasks, inputs, outputs and best practices that will cover complete lifecycle of systems, from its inception to its disposal, by complementing existing system development methodologies. Later the proposed methodology will be consolidated with feedback from stakeholders during training, presentation, and dissemination events, seminars and workshops of the initially defined methodology. In order to ensure the success of PRIPARE's methodology, several other initiatives other than the methodology definition itself will be carried out in parallel:

- Liaison with other EU projects,

- Provision of information and reference material for the general public, ICT educators, policy makers, and governmental and non-governmental bodies acting for human rights protection.

Abbreviations and Definitions

Abbreviation	Definition
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
EC	European Commission
EDPS	European Data Protection Supervisor
EIA	Ethical Impact Assessment
EU	European Union
FIPPs	Fair Information Practice Principles
FTC	Federal Trade Commission
ICO	Information Commissioner's Office
ICT	Information and Communication Technologies
ID-WSF	Identity Web Services Framework
ISO	International Standards Organization
LIBE	Civil Liberties, Justice and Home Affairs
NFC	Near Field Communication
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
OWASP	Open Web Application Security Project
PbD	Privacy by Design
PbD-SE	Privacy by Design Documentation for Software Engineers
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PMBOK	Project Management Body of Knowledge
PMRM	Privacy Management Reference Model
PRINCE2	Projects in Controlled Environments, version 2
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch
PSbD	Privacy and Security by Design
RFID	Radio Frequency IDentification
SAML	Security Assertion Markup Language
SbD	Security by Design
TC	Technical Committee
UMA	User Managed Access
URL	Uniform Resource Locator

References

[1] United Nations General Assembly*, The Universal Declaration of Human Rights,* Paris, 1948. http://www.un.org/en/documents/udhr/

[2] United Nations General Assembly, *The right to privacy in the digital age. Resolution A/C.3/68/L.45/Rev.1*. http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

[3] Ann Cavoukian, “7 Foundational Principles of Privacy by Design”, Information & Privacy Commissioner, Ontario, Canada. http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[4] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 2010. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf

[5] Article 29 Data Protection Working Party, Opinion 01/2012 Opinion 01/2012 on the data protection reform proposals, March 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

[6] RFID Industry, *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, January 2011, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

[7] Camenisch,Jan , R. Leenes, and D. Sommer, *Digital Privacy*, Springer Berlin Heidelberg, Berlin, 2011.

[8] Privacy by Design, “PbD based RFID PIA”. http://www.privacybydesign.ca/index.php/pbd-based-rfid-pia/

[9] Spiekermann, Sarah, “The Challenges of Privacy by Design”, *Communications of the ACM,* Vol. 55, Issue 7, July 2012, pp. 38-40.

[10] Linden Consulting Inc., “Privacy Impact Assessments: International Study of their Application and Effects”, Information Commissioner’s Office, UK, 2007. http://www.ico.org.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf

[11] Wright, David, “The State of the Art in Privacy Impact Assessment”, Computer Law & Security Review, Vol. 28, No. 1, Feb 2011, pp. 54-61.

[12] Flaherty, David, “Privacy Impact Assessments: An Essential Tool for Data Protection”, Canada, 2000 http://aspe.hhs.gov/datacncl/flaherty.htm

[13] Cavoukian, Ann, “Privacy Risk Management: Building Privacy Protection into a Risk Management Framework to Ensure that Privacy Risks are Managed by Default”, Information and Privacy Commissioner, Ontario, Canada, 2010 [p. 12]. http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf.

[14] European Commission, INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE PROVIDED BY THE RAPPORTEUR Proposal for a 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), Brussels, 22.10.2013.

[15] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[16] International Organization for Standardization (ISO), *Information technology – Security techniques – Privacy framework, ISO/IEC 29100:2011, First edition*, Geneva, 15 Dec 2011.

[17] International Organization for Standardization (ISO), *Information technology – Security techniques – Evaluation criteria for IT security, ISO/IEC 15408-2, First edition*, Geneva, 01 Dec 1999.

[18] Organization for the Advancement of Structured Information Standards (OASIS) *Privacy Management Reference Model and Methodology (PMRM),* Version 1.0. July 2013. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

[19] Alhadeff, Joseph, Brendan Van Alsenoy and Jos Dumortier. “The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions*”*, *Privacy and accountability international conference*, Berlin, 2011.

[20] European Data Protection Supervisor (EDPS), “European Data Protection Supervisor Glossary”. https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary

[21] Article 29 Working Party. http://ec.europa.eu/justice/data-protection/article-29/

[22] Finn, Rachel, David Wright and Michael Friedewald, “Seven Types of Privacy” in Serge Gutwirth, Yves Poullet et al. (eds.), *European data protection: coming of age?*, Springer, Dordrecht, 2013.

[23] Mulgan, Richard, “Accountability: An Ever-Expanding Concept?”, *Public Administration*, Vol. 78, No. 3, 2000, pp. 555-73 [p. 555].

[24] Raab, Charles, “The Meaning of ‘Accountability in the Information Privacy Context” in Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds.), *Managing Privacy through Accountability*, pp.15-32 [p.16], Palgrave Macmillan, Basingstoke, 2012,

[25] Article 29 Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

[26] Rubinstein, Ira, and Nathan. Good, “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents”, *Berkeley Technology Law Journal*, August 2011, Berkeley, California.

[27] Wright, D., “Making Privacy Impact Assessment More Effective*”, The Information Society: An International Journal*, Vol. 29, Issue. 5, 2013, pp. 307-315.

[28] European Commission - Directorate General Justice, Recommendations for a privacy impact assessment framework for the European Union, Brussels – London, November 2012. http://www.piafproject.eu/ref/PIAF_D3_final.pdf

[29] European Commission, Attitudes on Data Protection and Electronic Identity in the European Union – Special Eurobarometer 359. TNS Opinion & Social. June 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[30] European Commission, Cyber security – Special Eurobarometer 390. TNS Opinion & Social. July 2012. http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

[31] L. Rainie, S. Kiesler, R. Kang, and M. Madden, “Anonymity, Privacy, and Security Online. Pew Internet Report”. September 2013. http://pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

[32] Janice Y. Tsai, Serge Egelman, Lorrie Faith Cranor, Alessandro Acquisti, “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study”. *Information Systems Research* Vol. 22, Issue 2, June 2011, pp.254-268.

[33] S. Egelman, A. P. Felt, and D. Wagner. *Choice architecture and Smartphone privacy: There's a price for that.* University of California, Berkeley, 2012. http://weis2012.econinfosec.org/papers/Egelman_WEIS2012.pdf

[34] Sarah Spiekermann, “The challenges of privacy by design”. *Communications of the ACM*, Vol 55m No. 7, 2012, pp 38-40.

[35] S. F. Gürses, C. Troncoso, and C. Diaz, "Engineering Privacy by Design," In Computers, Privacy & Data Protection, 2011. http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf

[36] Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, Basingstoke, 2012,.

[37] Viseu, Ana, Andrew Clement and Jane Aspinall, “Situating Privacy Online”, *Information, Communication and Society*, Vol. 7, Issue 1, 2004, pp. 92-114.

[38] Solove, Daniel, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale University Press, New Haven & London, 2011.

[39] Bennett, Colin, “The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats”, in Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, Basingstoke, 2012, pp. 33-48.

[40] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[41] U.S. Congress, “Privacy Act of 1974 §552a”, U.S.A., 1974.

[42] OWASP Application Security Principles. https://www.owasp.org/index.php/Category:Principle

[43] Barton Gellman and Laura Poitras, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program”, *Washington Post*, Washington, June 6, 2013.