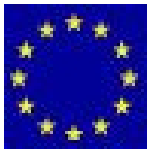
PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Deliverable D5.3
Recommendations and Research agenda

Project:	PRIPARE
Project Number:	ICT-610613
Deliverable:	D5.3
Title:	Recommendations and Research Agenda
Version:	V1.0
Date:	30/09/2015
Confidentiality:	Public
Author:	Carmela Troncoso (Gradiant)
	Pagona Tsormpatzoudi (KULeuven)
	Fanny Coudert (KULeuven)
	Nicolas Notario (ATOS)
	Daniel Le Metayer (INRIA)
	Gergely Acs (INRIA)



Funded by the European Union's
Seventh Framework Programme

Table of Contents

Document History

Version	Status	Date
v0.1	Table of Contents	14/04/2015
v0.2	First draft	18/06/2015
v0.3	First complete draft	11/08/2015
v0.4	Integrated ATOS comments on complete draft	18/08/2015
v0.5	Integrated ICRI comments on complete draft	28/08/2015
v0.6	Integrated INRIA comments on complete draft	07/09/2015
v1.0	Integrated quality review comments on complete draft	28/09/2015

Approval		
	Name	**Date**
Prepared	Carmela Troncoso	07/09/2015
Reviewed	All Project Partners	20/09/2015
Authorised	Antonio Kung	30/09/2015
Circulation		
Recipient		**Date of submission**
Project partners		09/09/2015
European Commission		30/09/2015

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
API	Application Program Interface
DPA	Data Protection Authority
DPO	Data Protection Officer
EDPS	European Data Protection Supervision
ENISA	European Network and Information Security Agency
EU	European Union
FOSS	Free and Open-Source Software
HCI	Human Computer Interaction
HSM	Hardware Software Module
ICT	Information and Communication Technologies
IPEN	Internet Privacy Engineering Network
IT	Information Technology
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
OWASP	Open Web Application Security Project
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PET	Privacy Enhancing Technology
SbD	Security by Design
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in Research
PSbD	Privacy and Security by Design
R&D	Research and Development
ROI	Return of Investment
RPAS	Remotely Piloted Aircraft Systems
TPM	Trusted Platform Module
TRL	Technology Readiness Level

Executive Summary

The goal of WP5 is to study issues and gaps that hinder the wide deployment of Privacy by Design practices in ICT systems. The firsts task in this work package reviewed the state of the art related to Privacy by Design application, encompassing the range of technical solutions, legal instruments and industrial practices; and the second task studied gaps in this state of the art that prevent full adoption and deployment of privacy protection mechanisms.

This deliverable presents the results of the analysis undertaken by the PRIPARE consortium on possible solutions to address the identified gaps. The deliverable contains recommendations for industry, recommendations for policy makers, recommendations for researchers and research programmes, and recommendations for standardization bodies.

Finally, the deliverable contains a summary of the results of the survey on Privacy by Design gaps carried out within WP5. This deliverable aims at validating the findings in previous tasks within this work package, that serve as starting point for the recommendations.

1 Introduction

This deliverable summarizes conclusions of PRIPARE Work Package 5: Gaps and Recommendations. The content of this deliverable builds on the Gap analysis performed in Deliverable 5.2 (PRIPARE 2015), which in turn is based on the state of play identified in Deliverable 5.1 (PRIPARE 2014), in order to put forward recommendations to strengthen the application of Privacy by Design in ICT practices.

As the previous deliverables, we follow a structure in which we consider recommendations related to industry, we then delve in recommendations for policy makers, and finally recommendations for researchers and research programmes. Additionally, we provide recommendations for standardization bodies, and a summary of the results of the survey on Privacy by Design gaps carried out within WP5.

The recommendations for industry, outlined in Section 2, aim at addressing the main issues identified in Deliverable 5.2: the lack of incentive from the legal framework; the limitations on the technical side; the lack of pressure from society, and the variety of misconceptions existing in industry with respect to privacy, Privacy by Design, and privacy-preserving technologies. We provide guidance to industry on practices that shall help clarifying the misconceptions and to improve privacy expertise in organizations, both at the technical and legal levels. The recommendations aim at bridging the gap between business incentives, technical solutions, and user needs, in order to create an environment in which embedding privacy in ICT developments becomes natural and systematic.

Secondly, in Section 3, we examine the gaps identified in Deliverable 5.2 with respect to Privacy/Data Protection by Design, and provide recommendations to policy makers for further development of the legal framework in order to provide better incentives to embed these principles in ICT products. This recommendations aim at helping policy makers to provide clear and unambiguous formulation that incentivizes industry to embed stronger privacy-preserving mechanisms in their developments.

Third, we provide recommendations to researchers and research programs in Section 4 aimed at addressing the technical limitations of current developments in privacy-preserving technologies that hinder their uptake by industry in commercial developments. These recommendations deal with new functionalities needed by real systems, ease of integration and better implementations that can be directly used by industry.

In Section 5, we provide recommendations to standardization bodies. These recommendations aim at guiding standardization processes towards incentivizing the use of strong privacy-preserving mechanisms and pave the way to the application of Privacy by Design in ICT engineering.

Finally, we offer a summary of the results of the survey ‘Gaps in the application of privacy by design’ carried out within WP5 in which companies were asked about their privacy-oriented practices, and what obstacles they find when trying to go beyond current practices with respect

to privacy. The results of this survey validate the findings of this work package with respect to the state of play and gap analysis.

2 Recommendations for industry

Within the previous deliverables (PRIPARE 2014) (PRIPARE 2015) we have identified the following causes that prevent the uptake of privacy by design principles and privacy enhancing technologies (PETs) within Industry:

- Lack of incentive from the legal framework
- Limitations on the technical side
- Lack of pressure from society
- A variety of misconceptions

Besides the lack of uptake of PbD principles, there is another major gap to be addressed which is related to the poor integration of privacy-related activities in the organization, including not only engineers but also at the management level. The lack of systematic approaches for addressing privacy within organizations during the engineering lifecycle has also been hailed as one of the causes of existing bad privacy (engineering) practices.

Some of these issues can be addressed by recommendations for law and policy makers, researchers and standardization approaches, but given the nature of these gaps the solutions tend to depend on mid/long term results. Meanwhile, there are some recommendations that can be applied in the short term by Industry that can help to avoid the obstacles that currently prevent achieving the desirable higher level of privacy in their services and products. The rest of this section dives into such recommendations.

2.1 Know your PETs

Many organizations like to be at the forefront of new technology and tend to incorporate latest advances such as:

- Using the latest development technology because it increases productivity, improves compatibility or for marketing reasons[1].
- Adopting big data approaches to gain business insight or to provide new services[2].

However, many times security and privacy-related technologies are underestimated as the ROI may be much harder to measure. Privacy and security activities within the Industry should not only be focused on generating revenue but mostly avoiding losses due to privacy and security breaches or failing to comply with the legislation. **Organizations should be aware of technological developments in privacy and security in the same way there are aware of other technologies or methods that may improve their ROI.** Several means can be used to achieve this:

- Follow privacy-related industry-oriented publications such as PDP Journal[3].
- Join privacy or security oriented initiatives such as Cloud Security Alliance or the European Organization for Security.
- Follow data protection news on public media.

[1] http://trends.builtwith.com/docinfo/HTML5-DocType
[2] http://www.idgenterprise.com/report/big-data-2
[3] http://www.pdpjournals.com/overview-privacy-and-data-protection

- Follow latest developments in security conferences both industry-oriented (e.g., RSA Conference[4], Real World Cryptography Workshop[5]), academic-oriented (e.g. USENIX Security Symposium[6], ACM Computer and Communication security[7]), and even hacker-oriented (e.g., BlackHat[8], Chaos Communication Congress[9]).
- Engage with public bodies related to data protection and privacy (e.g. EDPS, ENISA, national DPAs) and leverage their knowledge and their information base (e.g., latest reports from ENISA[10] on Privacy and Data Protection by Design, Securing Personal Data or Cryptographic algorithms).

2.2 Add privacy expertise to your organization

Many organizations are aware of the benefits that managing large sets of data may provide and do not hesitate on planning to invest in big data in the next two years (73% according to a Gartner survey[11]). On the other hand, organizations lack of awareness about the threats that lie behind these data (whenever it includes personal data). **Organizations need to integrate privacy expertise in their structure that will allow them to not only fully understand the risks that are behind the data but also the means and methods, i.e., the available technologies and best practices that should be followed, to mitigate these risks.** Depending on the size of the organization, the domain it belongs to and the type of project it conducts there are several means to incorporate such expertise:

- Include privacy experts/privacy engineers in the employee base to design privacy-preserving products, the same way as big data analysts are hired when big data systems need to be developed.
- Include privacy and privacy-engineering training as part of the organization's training catalogue.
- When the size of the organization is an obstacle for hiring new personnel, hire privacy consultancy services for specific projects or assessments.

2.3 Leverage the open source community

It is hard to find projects or developments in the IT domain that are not integrated with "external" components such as frameworks, APIs or libraries which can be commercial, FOSS (Free and open-source software) or somewhere in between. Organizations must be aware of the hidden privacy costs of using some of these services (e.g. Google Analytics, AdSense). Actually in some cases FOSS initiatives are born to provide the tools to substitute these types of commercial services, which are sometimes linked with ulterior motives. A clear case of this is PIWIK[12] which is an open source analytics platform which was developed trying to avoid the "forced" data sharing practices that are enforced for free-but-commercial services such as

[4] http://www.rsaconference.com/
[5] http://www.realworldcrypto.com/rwc2015
[6] https://www.usenix.org/conferences/byname/108
[7] http://www.sigsac.org/ccs/ccs-history.html
[8] https://www.blackhat.com/
[9] https://events.ccc.de/
[10] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables
[11] http://www.gartner.com/newsroom/id/2848718
[12] http://piwik.org/

Google Analytics. There are different ways in which open source can be used to effectively embed security and privacy in the organization products:

- **There are many open source community initiatives that offer more privacy-friendly alternatives to commonly used software** without necessarily incurring in additional costs, or where costs are worth by the risk minimization stemming from not externalizing data; and also enable organizations to use privacy as a service differentiator. If relying in the open source community is not an option in your organization, **look at open source commercial software, which brings the benefits from both worlds** (open source transparency plus the commercial support).
- **Open source allows to review the source code, minimizing the chances of having intentional or unintentional back doors.**
- **Open source projects allow contributions to improve its quality, which will lead to better data protection software in the organization, and on the market.**

There are many types of open source initiatives that can be leveraged for better data protection, many of them have already been mentioned in (PRIPARE 2014) and (PRIPARE 2015).

2.4 Get closer to the research environment

Research conducted within the academia, besides theoretical work and papers, also includes the development of reference algorithms and prototype implementations to demonstrate the feasibility of research results. This "practical" work is rarely ready to use by the Industry as it is often merely a prototype that is not subject to quality assurance standards or to customers' tests. By fostering the collaboration of the Industry and Academia stakeholders the research conducted are transformed into real innovation. Organizations can get closer to the research environment by:

- Fostering academia-industry associations and collaborations.
- Understand the innovation potential of research results, and being ready to invest effort in bringing research results to an Industrial quality level.
- Investing in research activities.
- Keeping up to date on research activities using industry-research joint privacy conferences.

Privacy is a trending topic at all levels and research results are shaping the future of privacy enhanced technologies and services which are expected to have an increasing demand in the future. Some promising privacy-related domains that must be closely watched are:

- Trusted hardware (e.g. trusted platform modules (TPMs), hardware security modules (HSMs), Intel® Software Guard Extensions…)
- Cryptography for privacy: homomorphic encryption, attribute based credentials, zero knowledge proofs, secure multi-party computation
- Privacy by design methodologies
- Privacy policies and its enforcement
- Anonymisation and pseudonymisation
- Privacy-preserving identity management

2.5 "PRIPARE" for the new Regulation

The forthcoming EU General Data Protection Regulation will unify data protection within the EU and will include changes that will affect Industry practices stemming, on the one hand from the fact that it is a regulation and not a directive, thus directly applicable to all Member States in a uniform way; and on the other hand from the inclusion of new data protection requirements and the establishment of much higher fines (potential fines up to 5% of the organization's annual worldwide turnover of an enterprise or €100m, whichever is greater).

In order to prepare for the advent of the new regulation, expected to be adopted in 2016, and to minimize the regulation's impact**, organizations should start to consider the new principles and key changes**:

- **Accountability**: data controllers will be required to be able to demonstrate compliance with the regulation and the adequate operation of the privacy and security controls.
- **Data protection impact assessment**: whenever processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
- **Data Protection by design**: organizations must implement appropriate technical and organizational measures and procedures to protect data subject rights, taking into account the state of the art and the cost of implementation. These measures must be considered from the onset of the project, during its operation and until it's decommission. Organizations can start analyzing the risks associated to the current processed data to prioritize the measures and procedures to be implemented.
- **Data Protection by default**: organization shall implement mechanisms to ensure that all personal data processed are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum. Organizations can start evaluating their privacy policies, usage of data and choosing adequate mechanisms. An opt-in approach seems a reasonable starting point.

At the same time, the new regulation reinforces and highlights the importance of principles already present in the previous Directive, such as:

- **Transparency**: organizations shall reinforce transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.
- **Data subjects' rights:** organizations shall enhance their procedures and mechanisms to allow data subject's to access, rectify and delete its data.

2.6 Know your users

While currently there is a lack of pressure from society, this status quo is bound to change. The fact that the Snowden revelations multiplied by four the number of encrypted traffic during peak hours in Europe may reveal that this lack of pressure is related to the lack of awareness. Another study already mentioned in (PRIPARE 2015), also provides some proof that there is some kind of relationship among Industry PET's awareness and the level of user concern. A

TRUSTe[13] study revealed that a significant 36% of consumers in France had chosen not to visit a company website due to concerns about their privacy online. In Germany a 34% reported not using a smartphone app due to online privacy concerns.

This reveals that organization must prepare to face the raising of privacy concerns among its users, which are expected to be the result of privacy awareness campaigns (launched privacy and public initiatives) or personal data breaches. **Organizations may prepare not only by putting in place the adequate measures but also by being transparent to its customers and data subjects, and clearly explaining the purposes of their processing of data**. In this sense, organizations should strive **to find how privacy can be turned into an effective differentiating factor and consider the deployment of privacy-preserving mechanisms as an investment**, not just a source of cost (similarly to renewable energy industries, which have successfully converted "green" into their differentiating factor)

2.7 Establish a systematic approach to address privacy issues

Some organizations may have the luck to count with privacy experts and engineers able to "magically" identify privacy risks, design means to address them, and seamlessly integrate these solutions into the overall design and implementation of the system. However, and in the same way as other aspects of system development, an "uncontrolled" or rainless process will lead to unpredictable, unrepeatable and subject-dependent results.

Organizations should define and establish systematic methods to address privacy and security issues not only at the engineering level but along the organization and overall product lifecycle. Although systematizing privacy seems challenging, there are other similar challenging areas where such systematization has been successful (e.g. research (Wilson 1952) or innovation (Knight 1967)) obtaining improved results.

PRIPARE actually proposes a systematic methodology (PRIPARE 2015) with specific processes that can be followed by organizations to embed privacy in their organizations and engineering processes, combining "best-of-breed" existing systematic approaches (e.g. Privacy Impact Assessment (ICO 2014), Risk management processes (CNIL 2012), architecture analysis methods (Nord, et al. 2003) (Nord, et al. 2003), etc.)

There are also other relevant initiatives with the same purpose of systematizing the addressing of privacy aspects within systems and organizations:

- OASIS Privacy Management Reference Model(PMRM)[14]
- OASIS Privacy by Design Documentation for Software Engineers (Pbd-SE)[15]
- ISO/IEC 291XX series (e.g. ISO 29100 Privacy framework[16] or ISO29101 Privacy architecture framework[17])

[13] http://www.truste.com/blog/2012/11/20/behind-the-statistics-%E2%80%93-responding-to-eu-consumers%E2%80%99-online-privacy-concerns-2
[14] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm
[15] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se
[16] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123
[17] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45124

- NISTIR 8062 Draft Framework for Privacy Risk Management for Federal Information systems[18]

2.8 Follow the standards

Organizations should enforce its engineers to follow the security and privacy best practices and guidelines related to the technologies used to develop or being developed, the same way it also enforces other procedures and practices such as code conventions, internal deployment and documentation processes or other guidelines. Following privacy guidelines, standards and best practices helps to transfer community-agreed or provider-approved solutions instead of relying on the organization-limited knowledge. There are several guidelines related to privacy addressing several layers of technology, some of them, that can be relevant to many organizations, are:

- Android best practices for security & privacy[19]
- iOS Security guide[20]
- Red Hat Enterprise Linux 6 Security Guide[21]
- OWASP Secure Coding Practices Quick Reference Guide[22]
- ENISA Smartphone Secure Development Guidelines for App Developers[23]
- Security and Privacy Controls for Federal Information Systems and Organizations[24] (NIST SP800-53)
- Privacy patterns[25]
- Privacy considerations for Internet protocols[26]

[18] http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf
[19] http://developer.android.com/training/best-security.html
[20] https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf
[21] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/
[22] https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf
[23] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines/at_download/fullReport
[24] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[25] https://privacypatterns.eu
[26] https://tools.ietf.org/html/rfc6973

3 Recommendations for policy and law makers

The goal of this section is to formulate recommendations for further development of Privacy/Data Protection by Design in light of limited incentives for compliance with the principle as illustrated in D5.2 (PRIPARE 2015). In D.5.2, we identified that limited incentives for compliance with Privacy/Data Protection stem from: A. uncertainties associated with the content and the scope of the principle in the draft regulation, B. lack of effective enforcement mechanisms (such as sanctions) and C. conflicting legal obligations to retain or share personal data. The proposed recommendations introduce ways through which policy makers could address the above issues.

3.1 Specify the wording and the scope of the principle in the draft regulation

3.1.1 Content of the principle Privacy/Data protection by design

D5.2 identified certain ambiguity on the way the principle of Data Protection by Design has been shaped in the Draft Data Protection Regulation. The inter-institutional debate, as described in D5.2, demonstrated the difficulty to clearly define an obligation to Data Protection by Design. In particular, the Council in its latest report deleted previously proposed definitions of the principle and rather introduced a series of technical measures (Council of the European Union 19 December 2014). Recital 61 reads: 'the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. Such measures could consist inter alia of minimising the processing of personal data, (…) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features'.

At the same time, in Article 23 (1) of the draft Regulation the application of the principle is dependent on a series of criteria. The data controller "having regard to the available technology and the cost of implementation", has to take into account "the nature, the scope, the context and purposes of the processing in order to implement technical and organizational measures appropriate to the processing activity and its objectives [including minimisation and pseudonymisation] in such a way that the processing will meet the requirements of the regulation and protect the rights of the data subject". It thus becomes a quite complex task to assess whether the data controller is subject to the obligation of Article 23 (1) on the basis of the proposed criteria and eventually apply the provision of Article 23(1) in practice.

The issues above demonstrate the need to further specify the content of the principle. To that end, one should look at the initial purpose of the inception of Privacy by Design which is to intervene before a system is built in order to prevent impacts to the fundamental rights to privacy in a timely manner. Then the list of technical measures of Recital 61 should be understood as a guide to help the data controller/processor select amongst available technical measures and fulfil that purpose.

However, mere focus on implementation of such technical measures, embedding as many data protection requirements as possible into the design of systems and strictly automating

compliance with the legal framework may not be sufficient[27]. Technical measures should be combined with organizational measures. It follows from the above that the data controller should rather adopt a more comprehensive policy towards privacy and combine the application of data protection by design measures as listed in Recital 61 with other measures. These may be technical or organizational (e.g., Data Protection Impact assessment - Article 33 of the draft Regulation or appointment of a Data Protection Officer ("DPO") – Article 35 of the Draft Regulation (European Parliament 14 March 2014).

3.1.1.1.1 DPOs: An example of organizational measures

The function of the DPOs will be inherently linked with assisting and evaluating the implementation of Privacy/Data Protection by Design. DPOs may function as a link between different functions of an organization and as such promote the interdisciplinary aspects of the principle Privacy/Data Protection by Design.

In the previous section we analyse the obligation to implement data protection by design with technical means introduced in Recital 61 of the Draft Regulation. However, such technical means may often appear disconnected from markets, user needs and economic contexts (Zibuschka en Rossnagel, Heiko 2011). This is a challenge to be addressed especially taking into account the complex ecosystem of private organisations where different departments function with different assumptions of privacy. Such assumptions may derive from political, economic, business, legal, or technical interests. This is not irrelevant with the nature of the concept of Privacy By Design in itself as it is an interdisciplinary concept which cannot be seen independently from organizational aspects (See (PRIPARE 2014)).

To assist data controllers take into account interdisciplinary aspects of Privacy/Data Protection by Design, the last Council's report on the draft Regulation introduces the obligation to appoint DPOs in Articles 35, 36, 37. DPOs will be assigned to perform internal monitoring of compliance and restore the missing links between the different organizations' departments. In particular, they will provide guidance on how to implement technical and organizational data protection by design measures as required by Article 23 and help the data controller demonstrate compliance (Recital 60) (Council of the European Union 19 December 2014).

DPOs as employees of the data controller have a quite sensitive but pivotal role. They will be the ones to promote the dialogue between different departments and eventually strike the balance between different interests under the common goal to implement privacy/data protection by design. However, the possibility for conflict of interest cannot be neglected (Article 36 para 4). This is why the draft regulation tries to protect DPOs from being penalised of dismissed for reasons other than performing well their data protection compliance tasks (Article 36 para 3, Article 35 para 7). In that regard, D5.2 (PRIPARE 2015) noted that the idea of totally independent Data Protection Officers may be too ambitious, since the latter ones are employed by data controllers.

[27] Leenes, R., & Koops, B.-J. 'Privacy Regulation cannot be hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data Protection Law'. International Review of Law, Computers and Technology. 2013.

Beyond such limitations that may be difficult to overcome, DPOs will be a significant organizational change which together with other means can demonstrate the intention to comply with Privacy/Data Protection by Design and take into account its interdisciplinary aspects. Policy makers should promote their function by encouraging lifelong learning and skills development for DPOs as well as education of industry players on how accommodate the DPOs' function in their companies.

3.1.1.2 Scope of data protection by design

Whereas the Data Protection Directive 46/1995/EC has traditionally tried to regulate the personal data lifecycle, data processing often takes place with products and services provided by actors whose activity has not been until today directly subject to data protection law. However, based on the assumption that negative impacts of technology can often be anticipated very at the stage that such actors operate, we argue that the scope of the principle should be extended to technology providers. The EC Communication which launched the data protection reform, the Albrecht's as well as the Council's report later identified technology providers as actors who have to take into account together with the data controller data protection by design (See (PRIPARE 2015)This is in line with the concept of Responsible Research and Innovation which proposes that all societal actors and innovators should be mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of innovation as a process and of marketable products (Peissl 2011).

This is also the approach taken by the Council's report of December 2014, which points out technology providers should be encouraged take into account data protection by design at the stage of product development (Council of the European Union 19 December 2014).

The reason for this policy option is that often technology providers may not be aware of the impact of their technology on privacy and data protection. For instance, in the case of Remotely Piloted Aircraft Systems ('RPAS'), that are designed to fulfill civil purposes such as photography or environmental protection but can fly over closed gardens and capture video and images, follow individuals on the streets, detect and count how many individuals there are in a building, sometimes without even being noticed (EDPS 2014)). However, technology providers are often familiar with the widely accepted ICT security goals. Confidentiality, integrity, and availability are IT security goals which are employed by system designers in order to identify risks and choose appropriate safeguards (Hansen 2011).

Considering the wide adoption of the IT security triad, privacy and data protection can be developed in a way comparable to the IT security paradigm and focus on protection goals. (Hansen 2011) To that end, to complement security protection goals, three privacy-specific protection goals can be adopted (Danezis, et al. 2014):

- *Unlinkability* ensures that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended and is related to the principles of necessity and data minimisation as well as purpose specification and limitation.

- *Transparency* ensures that all privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed at any time and corresponds to the principles concerning openness and it is a prerequisite for accountability.

- Finally, *intervenability* ensures that intervention is possible concerning all ongoing or planned privacy-relevant data processing, in particular by those persons whose data are processed. Intervenability is related to the principles concerning individuals' rights, e.g. the rights to rectification and erasure of data, the right to withdraw consent or the right to lodge a claim or to raise a dispute to achieve remedy.

Introducing the approach of operating with such privacy/data protection goals can be perceived as a gateway to involve technology providers in implementation of privacy/data protection by design. Privacy/Data Protection Impact Assessments of Article 33 of the Draft Regulation may be used in order to help technology providers identify and mitigate to the most feasible extent privacy and data protection risks stemming from their products. In the case of RPAs, since final use will be subject to the choices of the data controller, mitigation of privacy/data protection risks should be based on the implementation of privacy/data protection by default measures (e.g. adjustable data retention functionalities or different categories of sensors to choose from).

3.2 Foster enforcement

Specification of the content and the scope of the Privacy/Data Protection by Design should be followed by strong enforcement mechanisms.

3.2.1 The role of sanctions

Sanctions represent a hard law measure which is expected to function as an incentive to comply with the principle of Data Protection by Design. As introduced by the draft Regulation in Article 79, sanctions are corrective (deterrence-based) means for compliance since they may occur after a data controller failed to comply with the principle and eventually infringed data protection law. Their effectiveness as enforcement mechanisms that may provide incentives to comply with Data Protection by Design depends on the way DPAs will use their discretion to impose sanctions.

Even though DPA seem significantly empowered to impose sanctions in the draft Regulation[28], D5.2 underlined that efficient involvement according to the law may be too ambitious. Provided that no examples exist for the moment on how to measure compliance with data protection by design, DPAs may face a challenge to use their powers in practice. Lack of resources and/or experience in handling cases of major impact for the political, economic and social life of their state may be relevant factors. To overcome this challenge, policy makers should support their education as well as provide for (financial and human) resources when needed.

[28] Pursuant to Article 79(e) DPAs are entitled examine the degree of responsibility of the controller or processor towards Data protection by Design and impose administrative fines which might reach up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher. Furthermore, DPAs can modulate administrative fines for data protection infringements rewarding in that was data controllers who implemented Data Protection by Design measures (Article 79 (2e).

3.2.2 The role of soft law

Sanctions, as hard law measures, should be combined with soft law enforcement mechanisms. Soft law should be understood as rules of conduct that are laid down in instruments which have not been attributed legally binding force as such, but nevertheless may have certain - indirect - legal effects, and that are aimed at and may produce practical effects (Senden 2004). For efficient implementation of Privacy/Data Protection by Design we examine two soft law alternatives: i. certification as introduced in Article 39 of the draft Regulation and ii. Co-regulation, as a result of mandating Privacy/Data Protection by Design in standards.

3.2.2.1 Certification

Policy makers should promote the development of certification mechanisms introduced in Article 39 of the draft Regulation as a means to demonstrate implementation of Privacy/Data Protection by Design (Council of the European Union 19 December 2014). Certifications shall be issued by the certification bodies referred to in Article 39a, or where applicable, by the competent supervisory authority on the basis of the criteria approved by the competent supervisory authority or, pursuant to Article 57, the European Data Protection Board. The certification body should have an appropriate level of expertise on data protection (Article 39a of the draft Regulation).

Certification can be relevant for several actors in the value chain. Data controllers will have an incentive to certify that they have implemented the principle in their products and services as products and services that have been certified as privacy preserving may enjoy higher popularity amongst in the market. Similarly, technology providers, who might not be data controllers, as in the case of RPAs, described in Section 3.1.1.2 will have the incentive to conform with privacy protection goals and obtain relevant certification in order to make their products more appealing to the data controller/user of the RPAS in case the latter one requests privacy preserving options and more information about privacy-related aspects of the RPAS (domino-effect).

A standardised data protection model that is being acknowledged by the Data Protection Authorities in Germany and proposed for use on the European level is the one proposed by ULD (Danezis, et al. 2014). The model was based on privacy legislation in Schleswig Holstein which offers technology providers the opportunity to achieve a privacy seal for their products (TÜVIT Nord group 2015). Similar initiatives expected to be further developed when the draft Regulation comes into force should be encouraged by policy makers.

3.2.2.2 Co-regulation

In some cases socially harmful practices create the need to mandate Privacy/Data Protection by Design in legislation. That was the case in the US when web tracking became a serious concern for individuals' privacy (for more detailed description see Annex I). The topic was brought to the attention of policy makers by Federal Trade Commission ("FTC") which highlighted that consumers need to have the right not to be tracked by websites and called policy makers to adopt relevant legislation. As a reaction to the call, some states adopted the so called "Do Not Track" ("DNT") legislation to give consumers the choice opt out of third-party online tracking. In

parallel, a standardisation activity was also launched by World Wide Web Consortium. Even though the standardization work has not been concluded, it is expected that the DNT-related initiatives will contribute to restricting web-tracking, nevertheless, their results will be challenged by the fact that the DNT request will not be on 'by default' but left to consumer choice. The reason for this is could be that no specific results had been agreed in advance between the discussing parties and the policy makers.

All in all, the DNT mandate represents an example of co-regulation where different actors, the FTC, the legislator and the industry shared responsibility and address a socially harmful practice (web-tracking). In the European Union, co-regulation is understood as "the mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)" (European Parliament, Council, Commission, 2003).Provided that the Data Protection Directive 46/95/EC encourages member states art. 27(1) to experiment with a co-regulatory approach to the protection of personal data (Article 27 (1), policy makers should explore potential socially-harmful practices where co-regulation could foster Privacy/Data Protection by Design implementation. To ensure its efficiency, policy makers should clearly define the goals and the expected results of related initiatives.

3.3 Lead the way

The EC Communication launching the data protection reform highlighted that the legislator has a responsibility to provide a better space for respecting fundamental rights (European Commission 2010). This responsibility was put into practice by the proposals reforming the framework on data protection law and its principles. The legislator's responsibility to privacy and data protection as fundamental rights should function in a legal environment where policy makers lead the way in privacy/data protection by design implementation in two ways: i. Privacy/Data Protection by Design should be a requirement in public procurement. ii. Policy making should reconcile fundamental rights to privacy and data protection with obligations stemming from other areas of law often imposing obligations to collect, retain or share personal data.

3.3.1 Public procurement tenders

To foster the widespread implementation of Privacy/Data Protection by Design in different economic sectors the LIBE Committee proposed that data protection by design shall be a prerequisite for public procurement tenders in particular for utilities, such as water, energy, transport, postal sector (Article 23 (1a) of the draft proposed by the LIBE Committee (LIBE Committee of the European Parliament 2013). This option was abandoned in later discussion of the Regulation and has not come up ever since. However, in light of limited incentives of the industry to implement the concept, one should observe that data protection by design as a requirement for public procurement tenders would enhance the acceptance of the concept in the private sector. It would further provide incentives to implement it in new products and services involved in public procurement.

3.3.2 Privacy by policy design

Often policy makers are called to develop policies which may pose challenges to fundamental rights to privacy and data protection. An example can be observed in the field of EU regulations on the battle against money laundering and financial crime (For more details see

Annex I).. The proposal for the 4th Anti-Money Laundering Directive contained provisions that entail "a degree of limitation to the right of privacy and data protection" in particular with regards to availability of information on shareholders, requirements for data retention by relevant entities and personal data transfers in third countries (European Commission 2013). That was identified by the impact assessment that the Commission conducted in 2013 and taken into account in subsequent discussions of the Directive. Even though not all potential impacts were addressed, draft proposed by the Council (January 2015) imposes full anonymisation requirements to data shared at cross border level (Recital 15a of the Council's draft).

This example illustrates the value of assessing the impacts of policy making initiatives as they may introduce obligations posing challenges to the fundamental right to privacy. This need has been identified in the EC' Impact Assessment Guidelines of 2009 (European Commission 2009). To continue and strengthen privacy in Impact Assessments, policy makers should define systematic ways to ensure from the beginning that policies take into account privacy at any stage of the policy/law making process (privacy by "policy design").

3.4 Recommendations list

From the analysis above we extract a list of recommendations to be taken into account by policy and law makers in order to further develop the concept of Privacy/Data Protection by Design in policy and legislation.

- Policy makers should specify the content and the scope of the principle.
  -The content of the principle should entail a combination of technical and organizational measures.
  -Policy makers should support the function of DPOs by encouraging education of DPOs and industry players.
  -The scope of Privacy/Data Protection by Design should be extended to technology providers in order to prevent impacts to privacy stemming from their actions.
- Policy makers should foster enforcement of Privacy/Data Protection by Design through hard and soft law measures.
  -Policy makers should support the power of DPAs to impose sanctions by providing for their education as well as financial and human resources.
  -Policy makers should encourage the development of certification mechanisms. Particular attention should be given to certifications proving that technology providers have taken into account data protection law in their products and services.
  -Policy makers should use co-regulation to mandate effective implementation of Privacy/Data Protection by Design in order to restrict socially-harmful practices. It is crucial that policy makers clearly define the goals as well as the expected outcome of such initiatives.
- Policy makers should lead the way in Privacy/Data Protection by Design Implementation.

-Privacy/Data Protection by Design should become a prerequisite for EU public procurement tenders.

-Policy makers should apply “privacy by policy design” and identify systematic ways to take into account privacy at every stage of policy/law making in order to reconcile potentially conflicting obligations between data protection and other areas of law.

4 Recommendations for researchers

The section offers recommendations that aim at addressing limitations and caveats in current solutions as described in (PRIPARE 2015). As in the previous deliverables, we consider recommendations for technologies for personal data management and technologies for data minimization. We further provide recommendations for other aspects related to the engineering of privacy-preserving systems, such as privacy metrics, or risk analysis. Finally, we elaborate on recommendations to strengthen the application of Privacy by Design in ICT research programmes.

4.1 Technologies for personal data management

In this section, we follow the same organization as in Deliverable D5.2 (PRIPARE 2015) and consider successively information tools, tools for the expression of privacy choices and accountability tools.

4.1.1 Recommendations for information tools

Generally speaking, information tools should put subjects in a position in which they can deliver a legally valid, free, specific and well-informed consent. Our recommendations to address the limitations identified in Deliverable D5.2 concern the functionalities of the tools, their user-friendliness and the strengthening of the position of the subject.

4.1.1.1 More comprehensive functionalities

More research is needed to devise information tools that:

- Provide to data subjects a global, faithful and precise (fine-grained) representation of all the personal data that they have disclosed (beyond specific services) including all relevant information flows and all the parties involved.
- Provide insight about the logic of the processing of the data or the algorithms used to track data subjects or to differentiate them. This “algorithmic transparency” will become a key issue with the development of big data and the use of data analytics to support the personalization of a growing number of services.
- Are not under the exclusive control of the operator (or data controller), or can be checked to ensure their comprehensiveness and correctness of the information.

4.1.1.2 Enhanced user-friendliness

More work is needed on Human Computer Interaction (HCI) and this effort has to be conducted in an interdisciplinary way because useful HCI for transparency needs to take into account a wide range of factors (social, psychological, technical, legal, etc.). This is a key issue because information tools without carefully designed interfaces may mislead users and, by providing them a false impression of protection, induce them to disclose even more personal data.

4.1.1.3 Collaborative approach to reduce the imbalance between subjects and data controllers

Regardless of the actual level of information that they can obtain, one could argue that individuals are always in a weak position when they have to take decisions about the disclosure of their personal data because they generally do not have the necessary expertise to fully understand all legal and technical aspects of the situation. In addition to a lack of expertise, considering the number of sites they visit every day, they just do not have enough time to devote to this task.

One solution to redress this imbalance is to take a more collective approach, for example, by developing a form of collaboration between individuals to help them analyse privacy policies and warn their peers about unacceptable terms. ToS;DR[29] (Terms of Service; Didn't Read) is an example of effort in this direction but more work is needed to enhance both the functionalities of these services and their integration in the working environment of the users.

4.1.2 Recommendations for tools for expressing privacy choices

The main challenge with respect to privacy choices is to allow users to express their consent in a precise and unambiguous way. More work is needed both for the definition of general frameworks and for the design of solutions dedicated to specific areas such as social networks and health data management.

4.1.2.1 General frameworks

More research is needed to define general frameworks for expressing privacy policies which meet technical and user-friendliness requirements:

- On the technical side, they must give rise to clear, precise and unambiguous privacy policies, relying on sound mathematical foundations. A formal semantics should make it possible to verify, either a priori or a posteriori, the compliance of a system. Such frameworks and their semantics should go beyond traditional access or usage control and make it possible to express complex privacy policies.
- User-friendliness is also a key requirement to ensure that users can really grasp this kind of tool, really understand the choices that they express and potentially modify them if they change their mind.
- They should be used to define standard policies patterns, which could be instantiated in a clear, principled way, to feed different needs.

4.1.2.2 Domain specific solutions

More research is needed to take into account the specific requirements of complex systems such as:

- Social networks, in which a variety of parameters have to be considered[30] whose consequences can be difficult to understand.
- Health data management systems, in which many different stakeholders are involved, with different access rights.
- Systems collecting or processing location data, which are pervasive and can be used to infer sensitive information.

4.1.3 Recommendations for accountability-related tools

Considering the ever-growing collection and flow of personal data in our digital societies, a

[29] http://tosdr.org/

[30] As an illustration, a Facebook user can define, among many others, the following parameters: members who can see his profile on web searches, members who can see his future posts, members who can post on his timeline, members who can see what others post on his timeline, members are in his restricted list of friends (i.e., who does not see all his information), members who are blocked user (i.e., who cannot be his friend), members who are blocked app invitation senders, etc.

priori controls will be less and less effective for many reasons, and accountability will become more and more necessary to counterbalance this loss of ex ante control by data subjects.
More research work is needed in particular to support accountability of practice[31], through better support for log management and log analysis.

4.1.3.1 Log management

More work is needed on the design of log architectures to ensure that:

- Logs are accurate and secure: it should not be easy for a data controller to create fake logs. In other words, logs should reflect the actual execution of the system, especially in terms of personal data processing (*unforgeability*); once logs are generated, it should not be possible to alter them without detection (*integrity*) and it should be impossible to access logs without proper credentials (*confidentiality*).
- Logs contain enough information: logs should include sufficient information to detect any privacy breach.
- Logs do not contain too much information: the very implementation of accountability measures might introduce further risks of personal data breaches because it may lead to the storage of additional personal data in audit logs. Therefore, log architectures should also be designed with privacy by design in mind, and in particular it should be ensured that they meet the data minimization requirement.

4.1.3.2 Log analysis

One of the key requirements for accountability audits is the development of accurate and reliable techniques for log analysis. More research is needed to develop techniques combining automatic analysis based on a formally defined privacy policy language and complementary manual verifications. This combination is needed since some requirements (e.g. compliance with purpose, contextual rules, justifications for the application of break-glass rules, etc.) may not be checkable automatically and require human intervention. Integration of this aspect within an interactive verification tool is not straightforward and should be subject of future work.

4.2 Privacy-preserving technologies for data minimization

In this section, we follow the same organization as in Deliverable D5.2 (PRIPARE 2015) and consider successively end-to-end encryption, anonymous communication systems, privacy-preserving cryptographic protocols, and obfuscation-based approaches. The recommendations aim at addressing the shortcomings identified in the previous deliverable, which hinder the wide adoption of these technologies in common use online services.

4.2.1 Recommendations for end-to-end encryption developments

End-to-end encryption starts to be used in many services to provide stronger security and protect users' privacy. Yet, the amount of services using this technology is far from what would be desired from a Privacy-by-Design point of view. In order to make end-to-end encryption widely available in online services, several points need to be addressed by research:

[31] Following Colin Bennett classification into accountability of policies, accountability of procedures and accountability of practice.

- When end-to-end encryption is used for storage of data in external services (e.g., Cloud storage), common encryption mechanisms fail short to provide all functionalities needed. The most common examples are the inability to search over encrypted data, or the inability to efficiently share the stored information with other users (this often requires re-encryption and complex key management). Some solutions have appeared that aim at solving this issues, most remarkably Searchable Symmetric Encryption (Kamara, Papamanthou and Roeder 2012) (Chase and Shen 2015) and Format Preserving Encryption (Bellare, et al. 2009) (Luchaup, et al. 2014). While both solutions enable some searching and operations, they are still limited in functionality and performance or only work under certain assumptions that do not always hold in real systems. Moreover, current schemes leak information (e.g., nature of the data, number of elements of every type of data, etc). Therefore:
  - New cryptographic mechanisms are needed in order to enable more functionality, and in more generic scenarios. This will in turn permit all kinds of services to adopt end-to-end encryption.
  - Research is needed to better understand the kind and amount of information leaked in order to be able to evaluate the privacy risk incurred by these schemes.
- End-to-end encryption requires the use of keys, which has two downsides: i) it makes usability cumbersome, since users must manage their keys, and ii) it jeopardizes availability since when keys are lost so is the encrypted data. Novel key management mechanisms are needed to ease the use of end-to-end encryption, and to ease the recovery of keys to improve service availability.
- While free open source encryption libraries exist, its use and integration to obtain end-to-end security requires expertise often not found in standard software development teams. More research is needed to provide developers with easy-to-integrate tools for encryption and key management, if possible for the different type of platforms used nowadays (from mobile to embedded systems).

4.2.2 Recommendations for anonymous communication systems

Anonymous communications systems are becoming increasingly popular, and start to be used by some applications, in particular Tor[32]. However, they are far from being integrated in online services used daily. There are two main challenges to overcome in anonymous communication systems design and deployment:

- The first challenge is the design and development of anonymous communication tools that are effective even when services such as Flash or Javascript are used. These services, that are a cornerstone for current online services both web and app-based, have been shown to create a side channel that allows to de-anonymize users of anonymous communications. More research is needed to find ways to allow these services while preserving the privacy properties offered by anonymous communication systems.

[32] https://www.torproject.org/

- The second challenge is to improve the performance anonymous communication systems such that they offer a good user experience and hence they can be considered a commodity that can be used in all types of online services.

Finally, more research is needed to provide developers with easy-to-integrate anonymous communications features in their products and services.

4.2.3 Recommendations for privacy-preserving cryptographic protocols

The previous deliverable (PRIPARE 2015) acknowledges that there is a wealth of privacy-preserving cryptographic protocols that provide different functionality while preserving privacy. Yet, these technologies have not yet become mainstream tools due to the reasons appearing in (PRIPARE 2015). In order to enable the adoption of these technologies in common online services several steps are needed:

- Research is needed to develop more efficient protocols that can be used in deployed services. Ideally, designers and engineers would need generic efficient protocols to integrate in their applications. However, since this seems very difficult to achieve, research could delve into providing designers with means to derive scenario-specific efficient cryptographic tools from the generic schemes that appear in the academic realm.
- The used of advanced state of the art privacy-preserving protocols requires changes in design of ICT systems with respect to the traditional approach. For instance they may require a third party (whether trusted or not), require changes in the server with respect to a traditional service, require changes in the system to adapt to the adversarial model in which the protocol works. Solving this issue requires work in two directions:
  - First, research is needed to develop systematic ways to support designers and engineers at the time of integrating privacy-preserving cryptography without the need to re-design systems from scratch. (This recommendation complements those in Section 4.3).
  - Second, research is needed to, when possible, adapt privacy-preserving cryptographic protocols to deviate as little as possible from traditional design so that the need for changes when integrating them in deployed systems is kept to the minimum.
- Finally, with respect to deployability, as in the previous cases the main challenge for developers is to find suitable implementations of these protocols to integrate in their products. On the one hand, developers lack the expertise to implement these protocols themselves; and on the other hand there are few implementations available and most of them not ready for deployment (as commented in Section 2.4 and in (PRIPARE 2015)). More work is needed to take academic implementations nearer to the market needs so that privacy-preserving tools can be integrated in deployed services and applications.

4.2.4 Recommendations for obfuscation-based approaches

Security countermeasures can effectively reduce privacy harms related to the sharing of data coming from those who are authorized to access data. However, these means do not allow to selectively control the leakage of certain information which is individual specific, and hence is potentially more harmful than useful to share. Data sanitization, as noted in (PRIPARE 2015) can help with further risk reduction by altering the data itself meanwhile still allowing to learn useful information from it. Current methods have some limitations that need to be addressed:

- All sanitization techniques work along the fundamental trade-off between privacy risks and data benefit and try to maximize the benefit meanwhile sufficiently mitigating the risks. Different solutions provide different trade-offs. For instance, the traditional approach of de-identification by removing direct or indirect identifiers is now known to provide very weak protections and even sometimes low utility. On the other hand, techniques providing stronger privacy guarantee (such as noise injection to guarantee differential privacy), is often criticized for the excessive modification of the dataset rendering them useless for practical use. Fostering research on finding satisfactory trade-off remains a primary concern.
- In addition, very often, clever engineering can significantly boost the performance of existing sanitization methods depending on the data to be shared. There is a need for the implementation and careful documentation of such solutions such that they are ready to be used by developers in the form modules/toolboxes.
- The privacy guarantee of some sanitization techniques are still either unclear or often disregarded. For example, simple random sampling is a powerful tool to boost privacy as it decreases the chance of re-identification, and also allows using less perturbation in order to achieve differential privacy. The privacy guarantee of some intuitive but ad hoc sanitization techniques still remain to be unclear such as data swapping, various perturbation techniques, imputation to create (partially) synthetic data, etc. New (automatized) means to analyse the privacy guarantees of such algorithms need to be developed.
- Last, a main purpose of data anonymization is to allow mining of information. Instead of anonymizing the input data of any machine learning algorithm, the learning algorithm itself can be made privacy-preserving. That is, the (released) output of the computation preserves privacy while the input data is not necessarily anonymized. In certain scenarios, this approach significantly improves utility. Hence, privacy-preserving machine learning is becoming a hot topic of research due to the advent of Big Data. Nevertheless, the formal privacy guarantee of many popular machine learning techniques are still unknown (e.g., different recommender systems), or, if they are privacy-preserving, no alternative solutions exists with practical utility guarantees. Although there are a few theoretical results on differential private machine learning, more practical work is needed to support real-world data, provide empirical utility guarantees, manage privacy loss over time, and develop algorithms with stronger utility guarantees.

4.3 Development methods

4.3.1 Recommendation for research on privacy metrics

There is no a single and universal definition of privacy. The reason is that privacy, in general, includes many distinct concepts or objectives such as unwanted disclosure of personal data, lack of transparency and/or control, or the discrimination caused by the inferences made from personal data. Even more, privacy spans over multiple domains such as health care, transportation, education, internet services, smart infrastructures, financial domain, research data, and so on, each using personal data with different risks (and benefits). It is important to understand and formalize the privacy objectives and requirements in a particular domain.

4.3.1.1 Rigorous and legally acclaimed privacy metrics

It is vital to provide precise definitions of the various privacy objectives in different contexts. These definitions should be harmonized with policy and legal objectives and requirements. Precise definitions would enable designers and engineers to evaluate the privacy-preserving properties of computational mechanisms, which rely on personal data, either empirically or in a more formal, rigorous way.

Differential privacy is one of the first attempts in this direction. However, such notion of privacy (i.e., controlling information which is specific to a single individual) may be too general and result restrictive in certain scenarios, and at the same time, too loose in others, e.g., when individual's data are strongly correlated, or specific group-level information can also be privacy invasive or unlawful to disclose at all. In particular, it is still unclear whether such inference-based definitions of privacy are the right approach to formalize privacy requirements from legal point of view, and also, if they allow sufficient freedom to adjust the trade-off between privacy and utility.

Therefore, there is a need for much stronger collaboration between privacy researchers, policy and lawmakers, as well as domain experts. Indeed, privacy is a truly interdisciplinary topic involving many disciplines such as computer science, statistics, mathematics, law, philosophy, or economics.

4.3.1.2 Properties of ''good'' privacy metrics

Some desirable properties of good privacy metrics are already known: composability, privacy without obscurity, and transparency to post-processing. Indeed, a "good" privacy definition should be closed with respect composition, i.e., if some data satisfy a certain definition of privacy, then their combination should also satisfy the same privacy definition (perhaps with different parameters). Furthermore, transparency to post-processing requires that any computation done on the sanitized data should not alter its privacy-preserving properties, i.e., the post-processed data always satisfies the same privacy definition as the data itself. This not only simplifies the design of complex privacy-preserving mechanisms, but also allows to precisely quantifying privacy when data coming from multiple different sources are combined in order to compromise some individual's privacy.

4.3.1.3 Privacy metrics "without obscurity"

Many infamous privacy breaches were due to the underestimation of the additional sources available to an adversary. Privacy metrics shall be defined and computed taking into account that the adversary (i.e., the entity trying to perform a privacy breach) may have additional information about the system, such as the sanitization process used to achieve privacy, except for the random bits it may have used. This concept of "Privacy without obscurity" is analogous

to Kerkchoff's principle for security: "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them" and ensures privacy properties shall hold even against adversaries who have additional information on the system.

4.3.2 Recommendation for research on privacy risk analysis

Privacy metrics are only one side of the coin, which is about what privacy-preserving mechanisms aim at limiting. However, there is another side, namely the goal to be achieved by the collection and use of personal data. The balance of these two goals determines what could be done with personal data in general. A suitable level of privacy offered by a system cannot be defined without knowing the risk caused by the collection and use of personal data as well as its potential benefit. However, currently it is difficult to measure the potential harm and benefit stemming from data sharing.

4.3.2.1 Privacy Impact Assessment

In order to quantify the risk either qualitatively or quantitatively, first, the presence of personal data needs to be identified. This requires techniques to measure what exact personal information is revealed by different systems, which use personal data about individuals (e.g., recommender systems). Then, tools and techniques must be developed to enable the assessment of the risk associated with the collection, transfer and use of personal data. This requires elementary and/or empirical research on how information is shared nowadays and also the comprehension of privacy impacts on individuals. Impact assessment is challenging as many seemingly innocuous data can strongly correlate with sensitive information. For example, publishing the high-resolution electricity consumption (even aggregate) data of households can reveal the inhabitant's religion. A similar example has already been shown where muslim taxi drivers were identified based on more frequent stops during prayer times. In addition, the impact assessment of sharing aggregate data also deserves more consideration. Indeed, there are some theoretical evidences that they can expose almost as much risk as micro-data in certain contexts.

Privacy impact assessment is tedious and error prone. Therefore, there is a need for automatized measurement tools, which also support partial transparency in order to preserve proprietary rights of certain entities who may not want to disclose their inventions such as their developed algorithms. Automatized and scalable tools can facilitate the transfer towards a world where human-readable transparency policies can be replaced with these tools that can also be used by the individuals themselves.

Finally, there is also a greater need to formalize the exact motivations of adversaries. It can make sense to consider game-theoretic approaches to model the incentives of the potential adversaries. As in the case of metrics, it is important that newly developed risk analysis methods are designed with strategic adversaries in mind that may use additional knowledge on the system or its users to perform inferences and hence increase the privacy risk stemming from a particular kind of data collection and/or processing.

4.3.2.2 Data Benefit Analysis

Although benefit analysis requires the same principled treatment as risk analysis, it has fallen beyond the scope so far. However, all data sharing, no matter how useful they are, can always negatively impact the privacy of individuals even if they are not involved directly in the collection and use of data (e.g., disclosing correlation between smoking and cancer will potentially entail higher insurance fee for smokers worldwide besides the undisputable social benefit of such information). Therefore, it is also important to assess the benefit of data sharing

to verify whether it outbalances the potential privacy harms. Data sharing can have diverse positive impacts on individuals including better public health, well being, security, etc. Again, fostering stronger collaboration between domain experts as well as policy and lawmakers has vital importance.

4.3.3 Recommendation for research on privacy engineering supporting tools

Most of the recommendations for research on privacy technologies in the previous sections have a point in common: the need for methods that help privacy engineers integrating these technologies in their designs and developments. This indicated that there is need for research in two directions:

- The first direction concerns the need for suitable manners of taking research results to a status in which they are ready to be used by engineers. This includes investigating methods to systematically obtain operational implementations of the research developments, methods to make these solutions platform independent, etc. The goal is to produce technologies and tools that are nearer to be ready-to-use than the research results obtained nowadays.
- The second direction concerns the need to find means to systematically identify and address privacy concerns during the development of ICT systems. The current state of PIAs does not seem to have met that challenge, e.g. there are still gaps from analysis to design that need to be addressed, and design steps are still not well understood (e.g., research on privacy patterns and privacy strategies). More research is needed to both find and bridge these gaps in order to enable privacy-preserving engineering.

4.4 Recommendations for research projects and research programmes

In this section we summarize the recommendations related to the research agenda that were presented at the PRIPARE's briefing on Privacy-by-Design for European Commission staff that took place at the European Commission premises on the 11th June 2015.

4.4.1 Recommendations for research projects

The following recommendations were made for strengthening Privacy by Design in research projects:

- Privacy Impact Assessments (PIAs) should be mandatory and systematic in the execution of ICT projects, in particular those involving ICT development but not only limited to those. PIAs should be carried on from the beginning of the project with a twofold goal: i) tracing the decision making process with respect to privacy, and ii) guide technology developers towards privacy-preserving design and implementation decisions.
- It is desirable to have privacy expertise in project consortiums, with an interdisciplinary point of view. Ideally, there should not only be privacy expertise from a legal point of view, but also knowledge on the technological side to lead the privacy engineering

practices during the execution of the project. During the project, lawyers and engineers should be encouraged to work together, as opposed to next to each other. This includes, for instance, the mapping of technical mitigation measures to legal requirements, the linking of design choices with legal requirements, etc.

- When dealing with privacy, projects should try to focus on anonymization and data minimization, not only on data management. This should be reflected in the architecture of the system and its operation; and, when possible, the use of Privacy Enhancing technologies as the ones mentioned in WP5 deliverables (PRIPARE 2014) (PRIPARE 2015)), should be encouraged.
- The project should explicitly include an evaluation of the effectiveness of the privacy-protecting mechanisms that will be implemented. This should hold for any type of privacy-preserving solutions that have been implemented (e.g., technical, organisational, legal, etc.).

4.4.2 Recommendations for research programmes

- Research programmes should foster the growth of an ecosystem of PETs:
  - On the one hand, programmes should promote the development of operational ready-to-use implementation of PETs (towards TRL9), and foster work towards the study of the composability of PETS, so as to simplify the integration of these technologies in applications and services. This reinforces the recommendations put forward in Sections 4.1 to 4.3, in which the need for implementations of production quality is made patent.
  - On the other hand, the programmes should encourage de development of an ICT community for PETs that would help promoting privacy-preserving practices.
- As mentioned in Section 4.3, the means to measure privacy are not well understood. However, they are needed for the evaluation of privacy-preserving mechanisms (see Section 4.4.1). Research programmes should work towards the establishment of a privacy evaluation framework that allows developers to systematically evaluate the privacy level offered by their designs.
- Research programmes should not only consider Privacy by Design for systems as a whole but also for subsystems, regarding how privacy in these subsystems evolves when they are integrated in larger designs. Programmes should also promote the study of modifiability (i.e., the capacity to change without losing properties) of privacy-preserving systems and subsystems in order to enable easy embedding of privacy practices in ICT developments.
- All recommendations in this report hint that privacy engineering is a complex task, very much complicated by the youth of privacy enhancing technologies that make them difficult to use, and the lack of systematic approaches to integrate them into an engineering process. Programmes should foster the development of a privacy

engineering discipline that trains ICT professionals to integrate risk and design, and to use privacy-preserving tools that currently seem disjoint.

5 Recommendations for Standardization

In this section we outline recommendations for standardization bodies and processes derived from the conversations that took place at the second IPEN Workshop that took place in Leuven (Belgium) on the 5th of June 2015. These recommendations respond to the gaps identified in the PRIPARE project, gaps observed in the conversations at the workshop, or reflect proposals that were done during the standardization session at the workshop.

- Since the right to privacy is a universal human right, it is important that standardization bodies align their efforts when it comes to privacy-related standards. Privacy-related standardization processes should be as independent as possible from businesses interests and should be built with society's needs in mind.
- Standardization bodies working on privacy-related issues would benefit from improving the accessibility to the process and easing the paths to collaboration with the standard. In particular, it would be beneficial to count with open source communities and privacy advocacy communities that have been working on privacy-related issues for long.
- Privacy-related standardization should not only focus on data Personal data/Personally identifiable information, but should foster developers to protect other information beyond these data to better preserve privacy. This goes in the same direction as ENISA's report on Privacy and Data Protection by Design (Danezis, et al. 2014), where the authors highlight the existence of "privacy-relevant data". These data, even though they cannot be strictly considered personal data, may enable linkage of information (and subsequent inference of personal data) or be enough to permit discrimination; and hence should also be protected.
- Standardization bodies need systematic methods to detect and address privacy issues in the new specifications they develop for global infrastructures e.g. communications protocols. While there have been early steps in this direction at some bodies by developing specific techniques e.g. IETF RFC 6973) and tools (W3C PING Privacy Questionnaire) to capture potential privacy concerns in new specifications more guidance on capturing and addressing privacy concerns in standards is required.
- Standards should provide means to tackle the evaluation of privacy-preserving mechanisms. Such means should cover the choice of metrics, and guide developers in the process of computing these metrics for concrete applications in such a way that privacy protection levels can be established.
- Standards should carefully treat the question of data minimization, providing developers with means to identify the minimal set of data that is needed for their product. This is a cumbersome fact, since data minimization is not needed for the actual business process, and since there are no standard metrics it is difficult to evaluate the impact of data collection on privacy.

We also would like to refer standardization bodies interested in privacy-oriented recommendations to the ENISA's report on Privacy and Data Protection by Design (Danezis, et al. 2014) where further recommendations are formulated.

6 Survey and recommendations

In this section, we present the results of a survey[33] on 'Gaps in the application of privacy by design' by industry carried out within WP5. This survey aims at validating the findings of this Work Package: on the one hand what is the state of play with respect to privacy by design in industry (results from task T5.1), and on the other hand which are the gaps that prevent application and deployment of privacy by design (results from task T5.2). The reminder of this section explains first the contents of the survey and then delves into an analysis of the results and its relation to PRIPARE's findings.

6.1 Survey description

The survey contains eight questions aimed at understanding current practices of Privacy by Design in industries. The questions are the following:

1. **Industrial sector?**: segment in the economy where the companies participating in the survey can classify their activities. The categories in the survey are taken from PricewaterhouseCoopers industry sectors classification[34].
2. **ICT oriented company?**: whether the company is mostly focused on ICT related activities.
    - **Possible answers** (one choice only)**:** Yes/No
3. **Does your organization currently apply Privacy by Design in the lifecycle of your products?**: whether the company considers it follows Privacy by Design practices.
    - **Possible answers** (one choice only)**:** Yes/No
4. **If Privacy by design is applied, what is the motivation?**: which is the company's reason to follow Privacy by Design practices.
    - **Possible answers** (one or more)**:**
        i. Embedding privacy provides a competitive advantage
        ii. Economic incentives reflected in reduction of risks associated to collection of sensitive data
        iii. Legal compliance/standardization requirements
        iv. Industrial sector Self-regulation
        v. Maturity and affordability of privacy enhancing technologies
        vi. Commitment to protecting customer privacy

[33] http://goo.gl/forms/AFlv4uBG67
[34] http://www.pwc.com/gx/en/industry-sectors/index.jhtml

5. **If Privacy by Design is applied, when during the lifecycle?**: in which phases of a product's lifecycle does the company consider it follows Privacy by Design practices.
    - **Possible answers** (one or more)**:**
        i. Product analysis phase
        ii. Product design phase
        iii. Product implementation phase
        iv. Product verification phase
        v. Product release phase
        vi. Product mainteinance phase
        vii. Product retirement phase
6. **What Privacy-by-design practices does your company follow?**: what actions does the company take when following Privacy by Design.
    - **Possible answers** (one or more)**:**
        i. Organizational practices (PIA, Privacy Management Program –internal privacy rules and procedures)
        ii. Technical practices to support users' rights enforcements (access control, transparency-e.g. privacy mirrors, privacy policies)
        iii. Technical practices to support minimization of data collection (privacy enhancing technologies: anonymous communications, anonymous payments, etc)
7. **What hinders the application of Privacy-by-Design in your company?**: which reasons prevent the company from taking actions that would be considered Privacy-by-Design practices.
    - **Possible answers** (one or more)**:**
        i. Lack of incentive from the legal framework
        ii. Lack of pressure from society and/or lack of interest from users
        iii. Limitations of existing technologies
        iv. Lack of integration of privacy-preserving technologies within existing development methods
        v. High costs, unavailability or lack of maturity of privacy-enhancing technologies
        vi. Lack of knowledge of how to tackle a privacy-preserving design
8. What is your overall evaluation of your practice of PbD?: whether the company considers the use of Privacy by Design practices satisfactory.
    - **Possible answers** (one choice only)**:** Satisfactory/Not satisfactory.

Optionally, participants could also provide the name and website of their company.

6.2 Survey results

6.2.1 Currently applying Privacy by Design

Out of the 35 entities that answered the survey 19 (54%) consider to be currently applying Privacy by Design practices in their product lifecycle (see Figure 1). This is a rather high percentage given the relative youth of the Privacy by Design concept, but it must be taken into account that many of the survey respondents are clients or collaborators of PRIPARE partners and hence have a particular bias to consider privacy as an important matter.

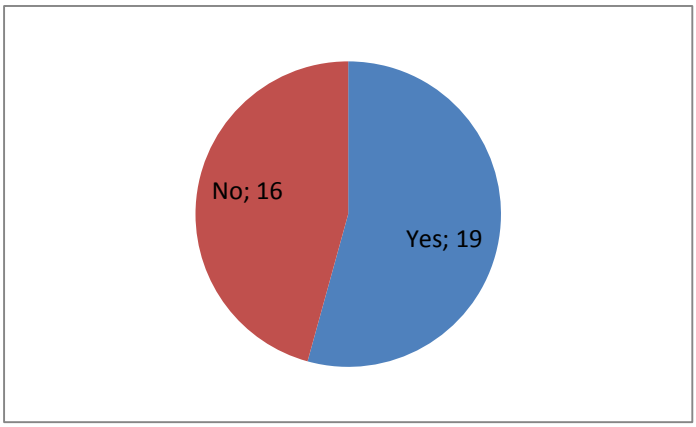


Figure 1 Application of Privacy by Design among the respondents

The following sections will explore the extent to which the practices declared by these companies reflect privacy-preserving practices or there is a misconception in what it means to apply Privacy by Design.

We note that both the entities that are applying Privacy by Design, as well as the ones that are not, have answered all the questions in the survey. The answers of the former describe their actual practices, the answer of the latter describe which practices they would like to follow if they were applying Privacy by Design

6.2.2 Participants' Industrial sector

Figure 3 Industrial sectors of survey participants shows the industrial sectors in which the entities participating in the survey offer services or develop ICT products.

We observe that, although the number of participants is not that high, there is representation of several sectors. As expected, the largest representation (42%) in the survey is of Technology-oriented organizations. The second most popular are R&D organizations, both companies and EU projects (14%). The rest of sectors have few representatives, being the Healthcare or Financial services sectors the best represented. We note that these two sectors are very relevant for our survey on Privacy by Design since they process and store highly sensitive data.

Figure 2 ICT-orientation of the participants in the surveyshows whether the entities participating in the survey consider their products and/or services as ICT-oriented. Of the 32 entities that declare themselves ICT-oriented, a majority (56%) consider to be applying Privacy by Design. On the contrary, not applying Privacy by Design seems to be the most popular option, though we only have 3 samples in the survey.

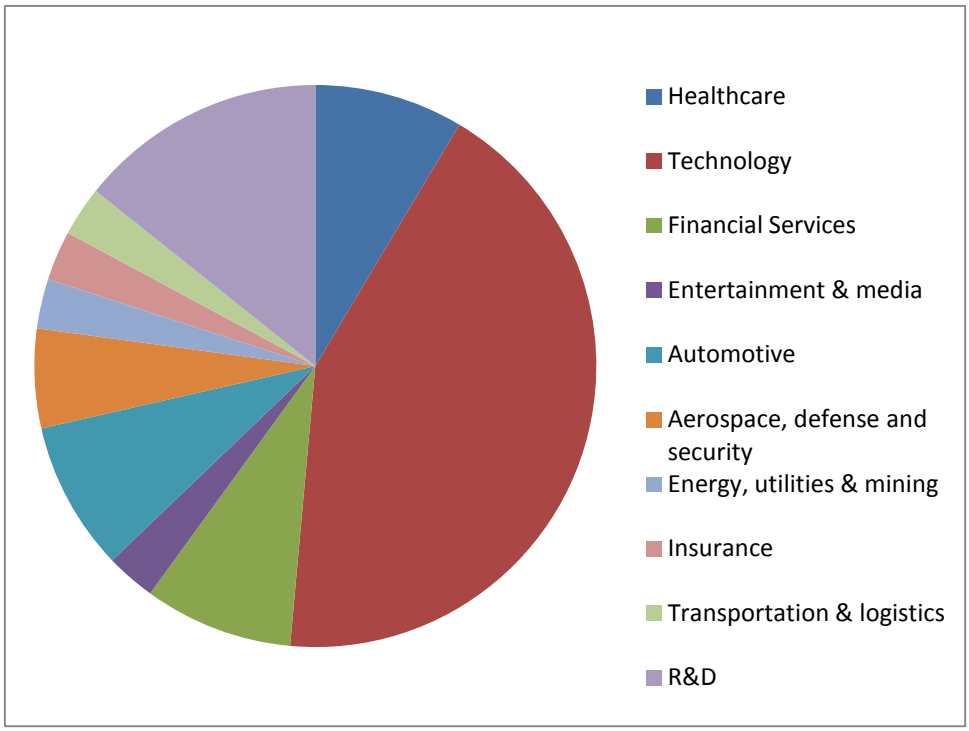


Figure 3 Industrial sectors of survey participants

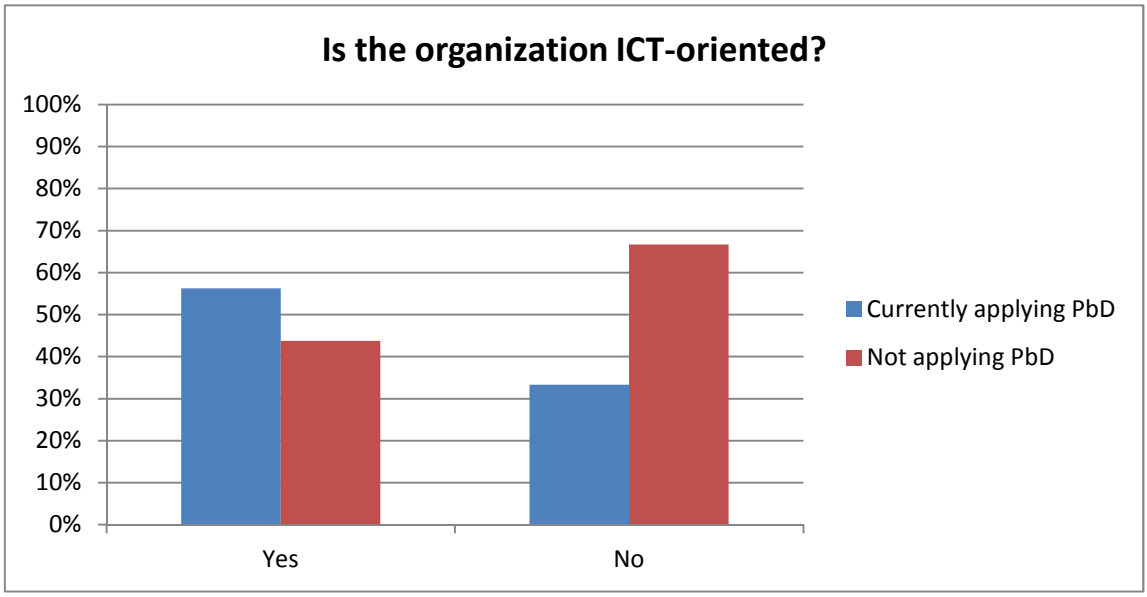


Figure 2 ICT-orientation of the participants in the survey

In Figure 4, we study the application of Privacy by Design depending on the industry sector. For the most representative sample, the Technology sector, we see that a 70% of the companies consider to be applying Privacy by Design. Again, this value is surprisingly high, and we will delve into this fact in the next sections. We would like to note that, in other sectors where privacy is a fundamental requirement, such as eHealth or the Financial services sectors, it is surprising that few organizations consider to be applying Privacy by Design.

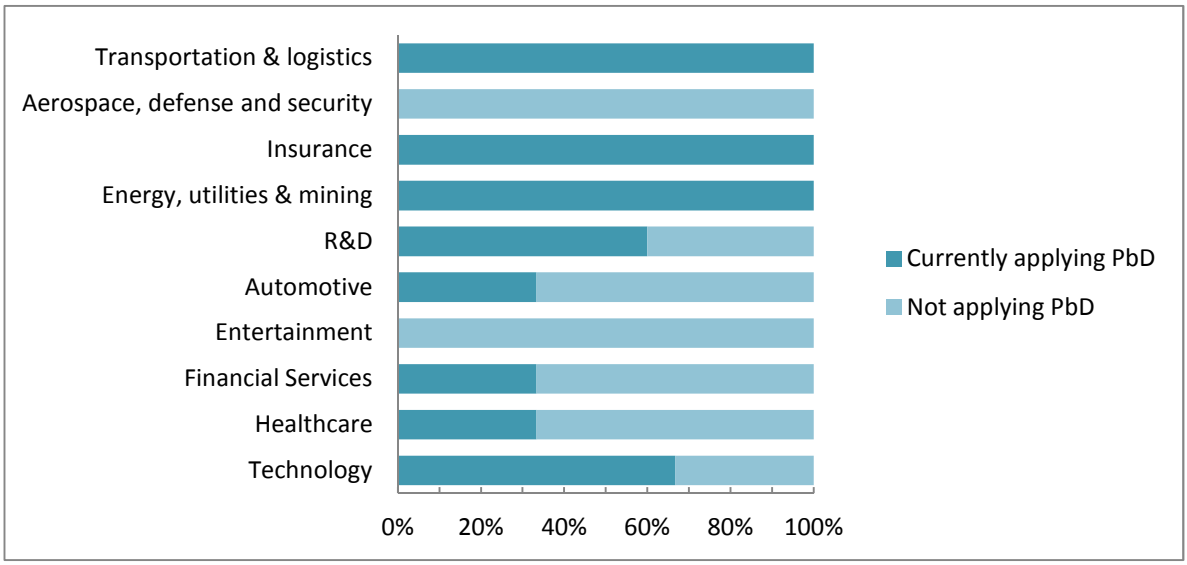


Figure 4 Privacy by Design application per industrial sector

6.2.3 Motivation to apply Privacy by Design

In this section we analyze the motivation put forward by each of the survey participants in order to apply Privacy by Design. The first part of the section studies the answers of entities that declare to be currently applying Privacy by Design practices; and the second part deals with entities that are not currently applying Privacy by Design and declare what would be their motivation to start doing it.

6.2.3.1 Currently applying Privacy by Design

Among the entities that consider being currently following Privacy by Design practices, the most popular motivation is to be compliant with regulation and standardization frameworks, with an almost 80% of participants declaring it is important for them, see Figure 5 Motivation for applying Privacy by design in organizations that already follow such practices (recall that in this question participants could choose multiple options). This coincides with the general belief that the incentives to perform Privacy by Design mostly stem from legal obligations and fear to sanctions.

The second most chosen reason is the commitment to protect customers' privacy. It is worthy to note that among these entities, an 80% claim to be using technologies to minimize the disclosure of user data, and more than 60% apply Privacy by Design from analysis to implementation phases. However, as we discuss in Section 6.2.5.1, it is unclear that these entities actually use technical means to minimize the collection of personal data.

The third reason, with more than 50% of entities considering as a motivation, is the competitive advantage provided by offering customers privacy-preserving products as opposed to not doing so. Other reasons such as industry self-regulation or the reduction of risk derived from not collecting data are not perceived as good motivations for introducing Privacy by Design in industrial practices.

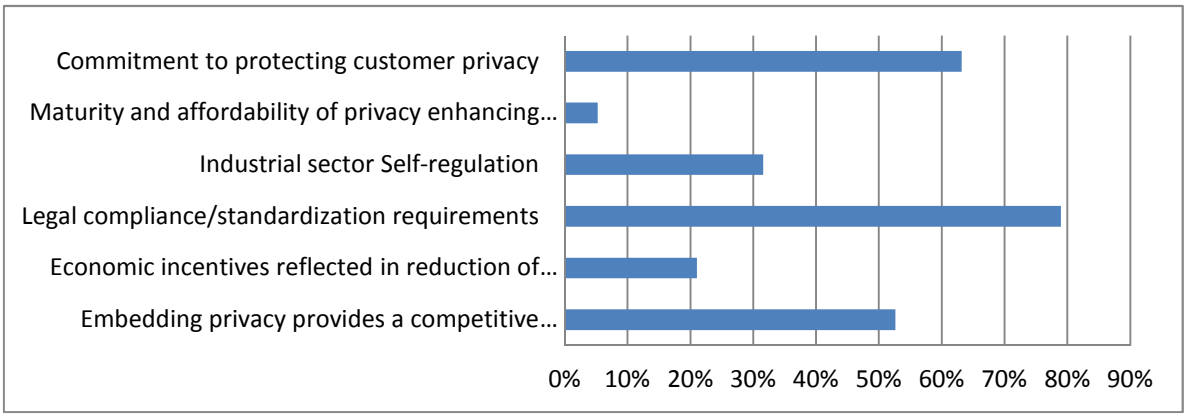


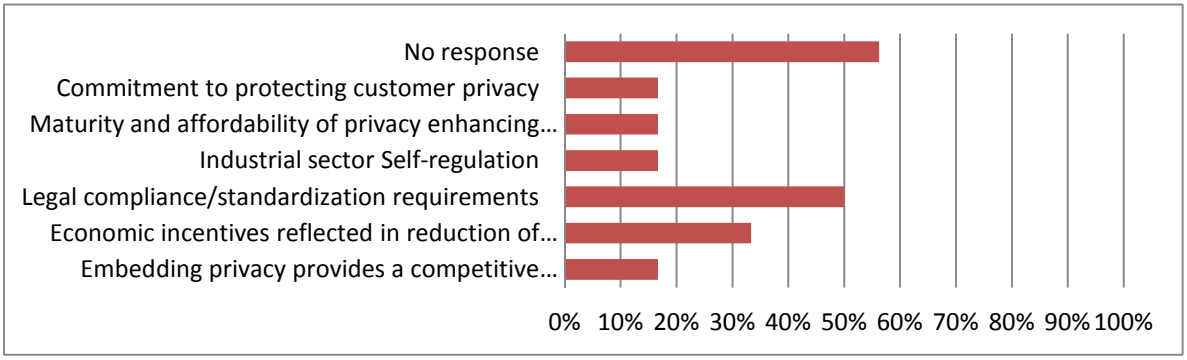
Figure 5 Motivation for applying Privacy by design in organizations that already follow such practices

Finally, the maturity and or affordability of using privacy enhancing technologies is not an incentive. This supports our findings in PRIPARE deliverable D5.2 (PRIPARE 2015), where we highlight the little maturity of many of these technologies and the high difficulty of integrating them into deployed systems.

6.2.3.2 Not applying Privacy by Design

From the 16 entities that are not currently applying Privacy by Design practices, 10 of them did not answer any further question, while 6 did provide us with insights on what reasons would motivate them to start applying Privacy by Design (see Figure 11 Reasons that hinder the application of Privacy by Design for survey participants that do not currently apply such practices).

Similarly to the entities that already follow Privacy by Design, legal obligations seem to be the most popular motivation. On the contrary, the second reason is the economic incentive provided by the risk reduction when personal data is not collected. Other reasons received very little attention.



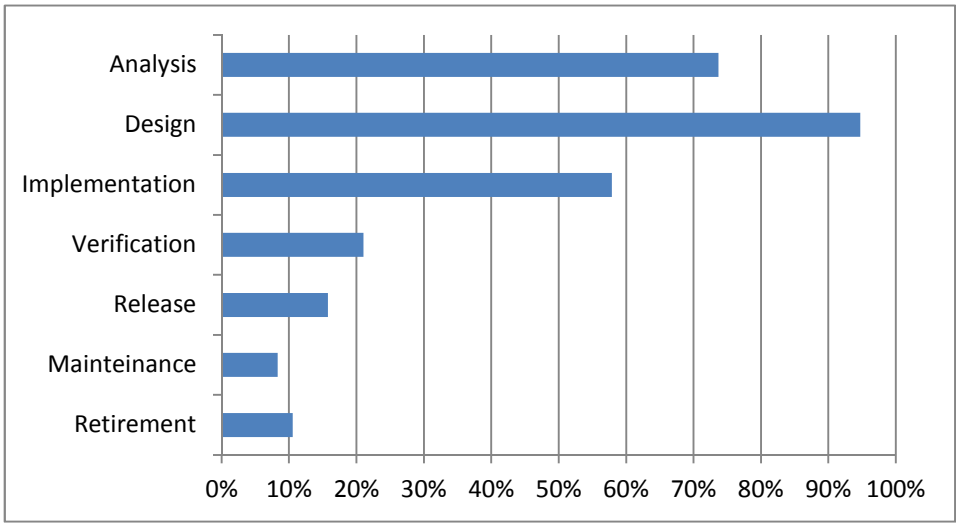
6.2.4 Privacy by Design in the products' lifecycle

The next question in the survey dealt with the products' lifecycle phases in which the participants perform Privacy by Design activities. As in the previous section, we distinguish participants that currently practice Privacy by Design from those that do not yet apply such practices.

6.2.4.1 Currently applying Privacy by Design

Figure 6 Motivation for applying Privacy by design in organizations that do not follow such practices

First we look at the lifecycle phases individually. As expected, see Figure 7 (multiple answers could be chosen), companies already practicing Privacy by Design mostly carry out such activities in the Design (94%) and Analysis phases (74%). This percentage is significantly reduced when it comes to the implementation of the system (58%), probably stemming from the lack of mature technologies to support the design as well as the difficult integration of the existing tools. The other phases (verification, maintenance and retirement) receive very little attention



(20% or less) when it comes to preserve privacy.

If we look at the lifecycle as a whole, seeFigure 8, participants have different approaches to (or understanding about) where to consider Privacy by Design. As expected, Analysis-Design-Implementation is the most popular combination. It is interesting that only one participant declares to apply Privacy by Design throughout the full lifecycle; and that some have chosen very surprising combinations such as Analysis-Design-Retirement without considering privacy at intermediate steps.

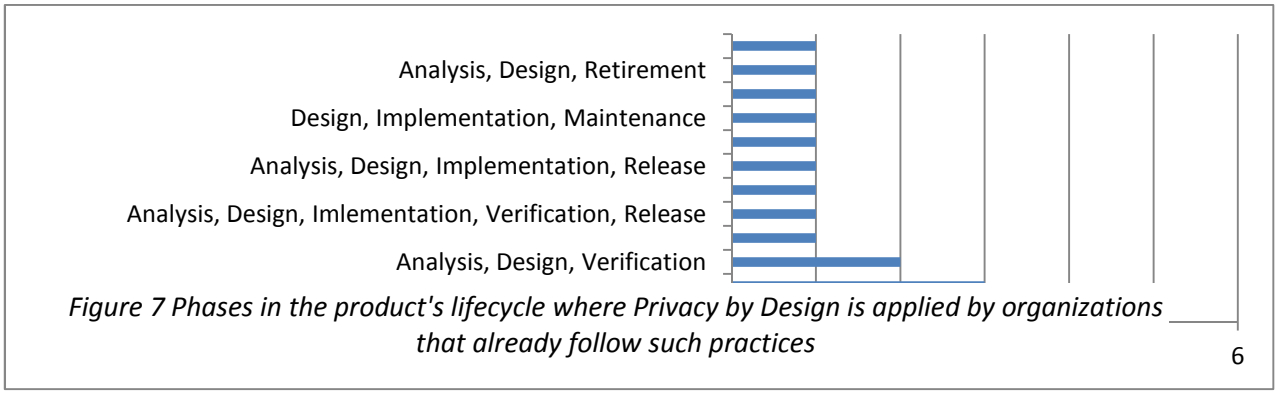


Figure 7 Phases in the product's lifecycle where Privacy by Design is applied by organizations that already follow such practices

Figure 8 Number of organizations applying Privacy by Design in different sub-lifecycles (organizations that currently follow Privacy by Design)

6.2.4.2 Not applying Privacy by Design

Only four of the participants that do not currently apply Privacy by Design provided an idea of which would be the lifecycle steps in which they would apply privacy by design (12 participants that do not apply Privacy by Design left this question without response). Among these 4, two would only consider Privacy by Design in the analysis, design and implementation phases, while the other two declare they would actually consider throughout the full lifecycle.

6.2.5 Privacy by Design practices

We next analyse the nature of the privacy by design practices followed by the participants both currently, and declared intentions of those participants that currently do not include Privacy by Design in their activities.

6.2.5.1 Currently applying Privacy by Design

Participants currently practicing Privacy by Design apply different privacy-preserving measures, as shown in Figure 9. The most popular choice is to be applying organizational measures, as well as using technical means to enforce users' rights preservation and technical means to minimize data collection (30% of participants). The second most chosen combinations are only techniques for rights enforcement, or a combination of rights enforcement and data minimization (both chosen by 15% of participants). The rest of the options are only declared by a minority of survey respondents.

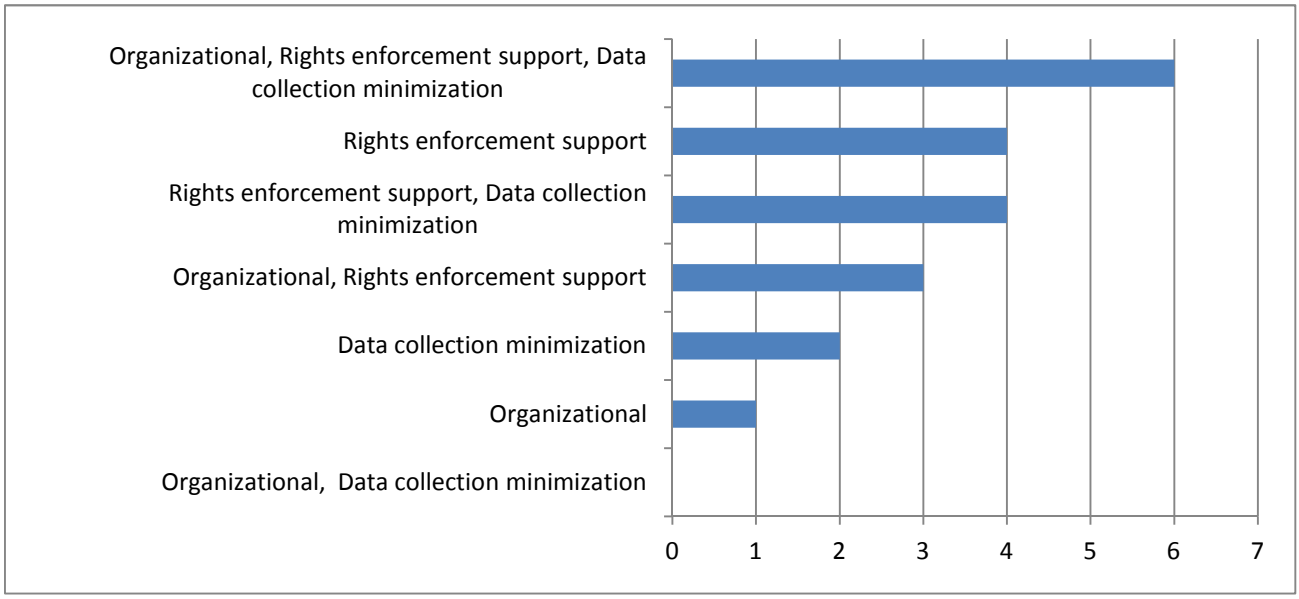


Figure 9 Types of Privacy by Design practices currently followed by organizations

It is surprising that 11 participants declare to be using "Technical practices to support minimization of data collection (privacy enhancing technologies: anonymous communications, anonymous payments, etc)", since our findings say that these are rarely mature, bring great penalties in terms of performance, and are not easy to integrate (PRIPARE 2015). Therefore, we investigated (to the extent possible) whether this is true. For this purpose we have browsed the websites provided by six of these companies (the other five did not provide us with this data, since it was optional). These are the results:

1. Participant 1, developing services and technologies oriented to efficient use of energy and sustainability. The products in their website do not seem to contain personal data, and hence it is difficult to assess whether there is minimization or collection or just there is no need.
2. Participant 2, offering insurance services. The specialized insurance products in their website (e.g., vehicle fleet management, or telemarketing) seem to require the collection of a great deal of personal data, and there is no hint in the website as to the minimization of this collection. It is worthy to say that the company offers professional services in the assessment of Data Protection compliance.
3. Participant 3, consultancy specialized in electronic transactions. The website contains references to expertise in the deployment and use of cryptocurrency in the company's solution. We believe that this validates the claim that the company uses technical means to minimize disclosure.
4. Participant 4, providers of context-aware personalization technology. Their product is based on the collection of mobile sensor data for personalized services (from marketing to mobility management). The website contains comprehensive discussions on why privacy is important for users' acceptance of personalization. Yet, the technical means expressed are mostly oriented towards compliance with data protection and help users to enforce their rights (e.g., informed consent, transparency tools, etc). Also, privacy is always approached from the point of view of not disclosing data towards third parties, not the company itself.
5. Participant 5, providers of biometric solutions. Their products do include privacy-preserving techniques to protect biometric templates in such a way that they cannot be re-identified, nor linkable in different databases.
6. Participant 6, EU project. This project has the design of privacy-preserving solutions among its goals, and hence the project results implement technical measures to minimize the disclosure of personal data, e.g., location.

This small study, although very limited, shows that there is a variety of understandings of what is minimizing the collection and disclosure of personal information. These differences mislead companies into believing that they are applying Privacy by Design and protecting customers' privacy while this is not always the case. For instance, companies using HTTPS may consider that this is enough privacy protection. While this technology indeed minimizes the disclosure f data towards third parties, it does not minimize the amount of data shared with the service provider as opposed to the technologies considered in the option "Technical practices to support minimization of data collection (privacy enhancing technologies: anonymous communications, anonymous payments, etc)".

Further details on privacy practices

The survey allowed respondents to elaborate on the privacy practices used by their organization. These are the responses we got:

Table 1: Details on current Privacy by Design practices

Declared practices	Company comments in survey	PRIPARE Comments
Technical practices to support	We aim to incorporate privacy-by-	The details do not allow

users' rights enforcements Technical practices to support minimization of data collection	design where applicable in providing technology services to clients.	assessing whether the respondent actually applies Privacy by Design or not.
Organizational practices Technical practices to support users' rights enforcement Technical practices to support minimization of data collection	Technical means for minimization Local processing and aggregation Avoidance of logs to hinder reidentification	Clear practices to support Privacy by Design
Organizational practices Technical practices to support users' rights enforcement	Encryption of sensitive information, disk and memory Full system roles, managed by two-factor authentication	Only practices to protect data from third parties.
Technical practices to support users' rights enforcement	They depend on the project. Typically customer driven.	The details do not allow assessing whether the respondent actually applies Privacy by Design or not
Organizational practices Technical practices to support users' rights enforcements Technical practices to support minimization of data collection	Legal disclaimer associated to data protection included in all support contracts with external stakeholders (providers, partners, etc...) Legal disclaimer associated to data protection included in labour contract with employee. In addition, specific learning contents are mandatory	Though the company declares the use of technical means to support Privacy by Design, the described countermeasures are organizational or legal practices.
Organizational practices	1. gather the security requirements. 2.- Develop a PIAs assessments 3.- Develop a Security Risk Assesments 4.- Develop a Security Control Design 5.- Develop the Security Controls	The described practices are mostly oriented to security, not privacy.
Organizational practices Technical practices to support users' rights enforcements	Dedicated people to set policy on data privacy compliant with data regulation. Project management including the evaluation and implementation of standard solutions to protect availability, confidentiality, integrity, and traceability of the data...	The described practices are mostly oriented to compliance with data protection and ensuring security, but not specific to privacy protection.

Similarly to the previous study, the detailed responses about privacy make it patent that survey participants have very different ideas of what is Privacy by Design, with many times get confused with Security, establishment of legal contracts, or application of Data Protection. Only one of the organizations seems to be protecting data from themselves.

6.2.5.2 Not applying Privacy by Design

Only three of the participants that do not apply Privacy by Design provide an idea of what would be their practices. The trend is to use technical means to enforce users' rights, though also organizational measures and disclosure minimization techniques are mentioned.

6.2.6 Reasons that hinder the application of Privacy by Design practices

We also questioned participants about reasons that hinder the (full) application of Privacy by Design practices in their organization. We analyze the responses in this section, whose findings validate the gap analysis described in Deliverable 5.2 (PRIPARE 2015).

6.2.6.1 Currently applying Privacy by Design

The most popular reason that hinders the further application of Privacy by Design for the participants that already perform some practices is the high cost, unavailability or lack of maturity of privacy-enhancing technologies (chosen by almost 60% of the participants), see Figure 10. This is complemented by the poor integration of privacy-preserving technologies and privacy engineering in general in existing development methodologies (chosen by almost 40% of the participants). Both claims reinforce PRIPARE's gap analysis on privacy technologies result, and also the idea that further research and more importantly development is needed in order to provide a set of tools that actually promote the wide adoption of Privacy by Design practices.

Surprisingly, the third most claimed reason is the lack of pressure from society and users. While this statement validates PRIPARE's findings, it contradicts the general belief that users do care about privacy and shows that indeed, from a business perspective providing privacy-preserving products is not a must.

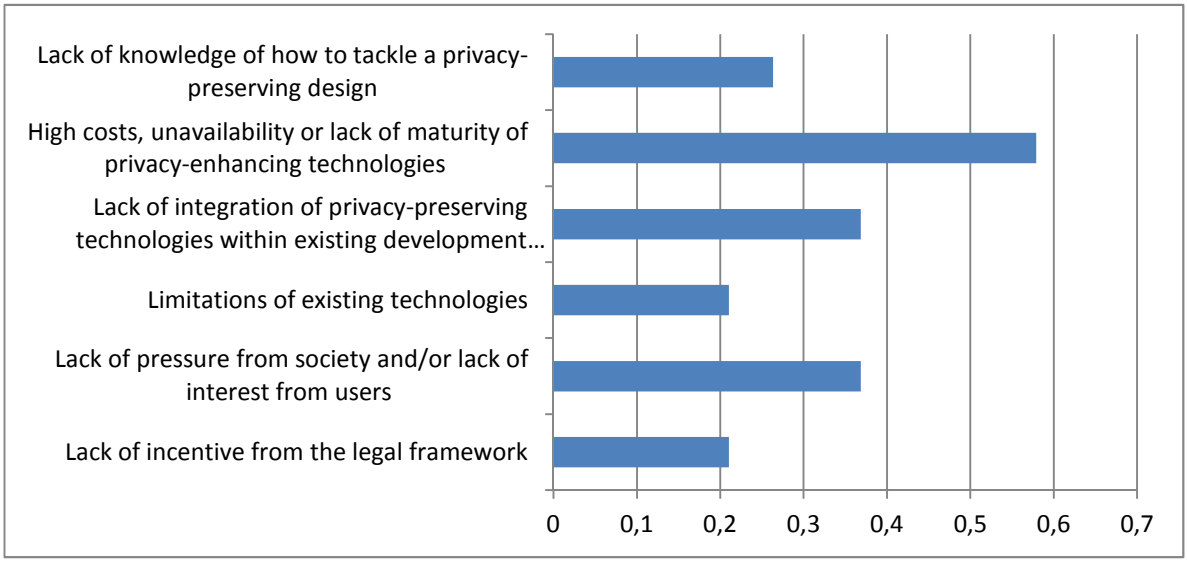


Figure 10 Reasons that hinder further application of Privacy by Design in organizations that already follow such practices

The other reasons offered as options in the survey: lack of incentives stemming from the legal framework, lack of knowledge, or limitations of available technologies, seem not to be significant.

Further details on reasons that hinder the application of Privacy by Design

Again, we provided participants with space to elaborate on the reasons perceived to not follow Privacy by Design. These are the responses we collected:

Table 2: Further details that hinder the application of Privacy by Design in industry currently following these practices

Declared reasons	Details	PRIPARE Comments
Lack of incentive from the legal framework Lack of pressure from society and/or lack of interest from users Limitations of existing technologies Lack of integration of privacy-preserving technologies within existing development methods High costs, unavailability or lack of maturity of privacy-enhancing technologies	Privacy-conscious consumers, governments, management Effective PETs and clear deployment guidelines Lack of means to convey privacy problems to users, how to obtain really informed consent?	Both declared reasons and details confirm PRIPARE's findings with respect to the gaps.
Lack of integration of privacy-preserving technologies within existing development methods High costs, unavailability or lack of maturity of privacy-enhancing technologies Lack of knowledge of how to tackle a privacy-preserving design	Even though we have the knowledge and tools to design and implement secure and privacy-preserving solutions, we fall short when trying to measure, evaluate and improve them.	Missing tools for evaluating the performance of privacy-preserving solutions is another gap identified within PRIPARE
Lack of incentive from the legal framework Lack of pressure from society and/or lack of interest from users High costs, unavailability or lack of maturity of privacy-enhancing technologies Lack of knowledge of how to tackle a privacy-preserving design	Easy to use technology: commodity.	-
Limitations of existing technologies Lack of integration of privacy-preserving technologies within existing development methods High costs, unavailability or lack of maturity of privacy-enhancing technologies	Contingency plan to Privacy by Design incidents Deployment of new control process associated to new business model (final user access, external customer sites, .etc..)	These two missing elements will be incorporated to PRIPARE's gaps list.
Lack of pressure from society and/or lack of interest from users	1. Guidelines 2. Legal requirements assessment 3. Security software frameworks to help within the development	These two companies miss even very basic guidelines to start introducing Privacy by Design practices. This is an even greater gap than that identified by PRIPARE.
Lack of incentive from the legal framework High costs, unavailability or lack of maturity of privacy-enhancing technologies Lack of knowledge of how to tackle a privacy-preserving design	Have a tool giving the minimum legal requirements by country, the authorized technologies we can use to allow to protect data, like the algorithms the ciphers the key length...	
Lack of pressure from society and/or lack of interest from users Lack of integration of privacy-preserving technologies within existing development methods	Security and privacy are not part of current educational programs. I can get an MIT masters in Computer Science without going to one lecture on security and privacy. Other universities /	The lack in education on privacy (and even security) is already discussed in WP4.

	institutes do not do a better job. There are dedicated security programs, but the integration in other programs is vital.	

6.2.6.2 Not applying Privacy by Design

Among the participants that do not apply Privacy by Design, 11 out of 16 provided reasons for this fact. A summary of results is shown in Figure 11, representing the percentage of respondents choosing each of the reasons (recall that this was a multiple choice question).

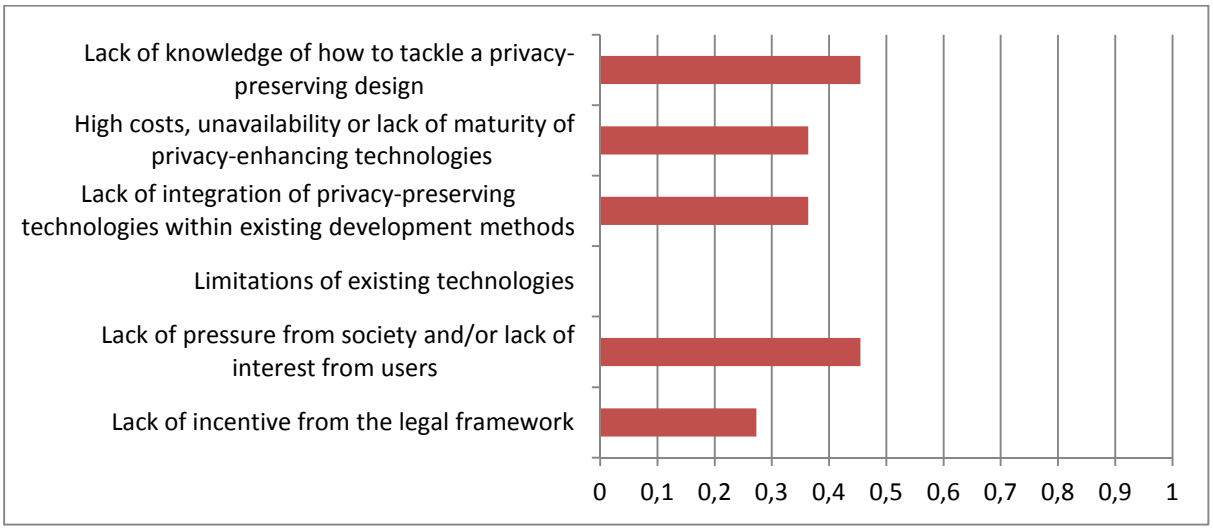


Figure 11 Reasons that hinder the application of Privacy by Design for survey participants that do not currently apply such practices

All reasons provided seem to be equally important for these companies, being the lack of knowledge and lack of pressure from customers the most popular choices.

Surprisingly, none of the participants mentioned the limitations of existing technologies as a reason for not using them which makes us believe that their information on these technologies is scarce or inexistent.

Further details on reasons that hinder the application of Privacy by Design

These are the details provided by participants that do not currently apply Privacy by Design on what they miss in order to start integrating Privacy by Design practices in their organizations.

Table 3 Further details that hinder the application of Privacy by Design in industry currently not following these practices

Declared reasons	Details	PRIPARE Comments
Lack of knowledge of how to tackle a privacy-preserving design **Our products don't need it**	We don't know much about it. Additionally, since our products are most of the time used on workstations not connected to the Internet, it's not a big issue for us.	All comments reflect a clear lack of awareness of what Privacy by Design is and how to follow its practices.
Lack of pressure from society and/or lack of interest from users Lack of integration of privacy-preserving technologies within existing development methods Lack of knowledge of how to tackle a privacy-preserving design	The main reason for not tackling PbD is the lack of knowledge of the advantages and implications of doing it.	A second conclusion to derive is that these participants do not have any incentives to start learning about it.

Lack of incentive from the legal framework Lack of pressure from society and/or lack of interest from users High costs, unavailability or lack of maturity of privacy-enhancing technologies	I believe mostly it is missing regulations (for stricter privacy controls, privacy enhancing technologies) and missing interest from public/customer side	
We don't know about it	We don't have any information about privacy by design	

6.2.7 Satisfaction with respect to Privacy by Design Practices

The last question in the survey referred to the degree of satisfaction of organizations with respect to the application of Privacy by Design. Figure 12 summarizes the result.

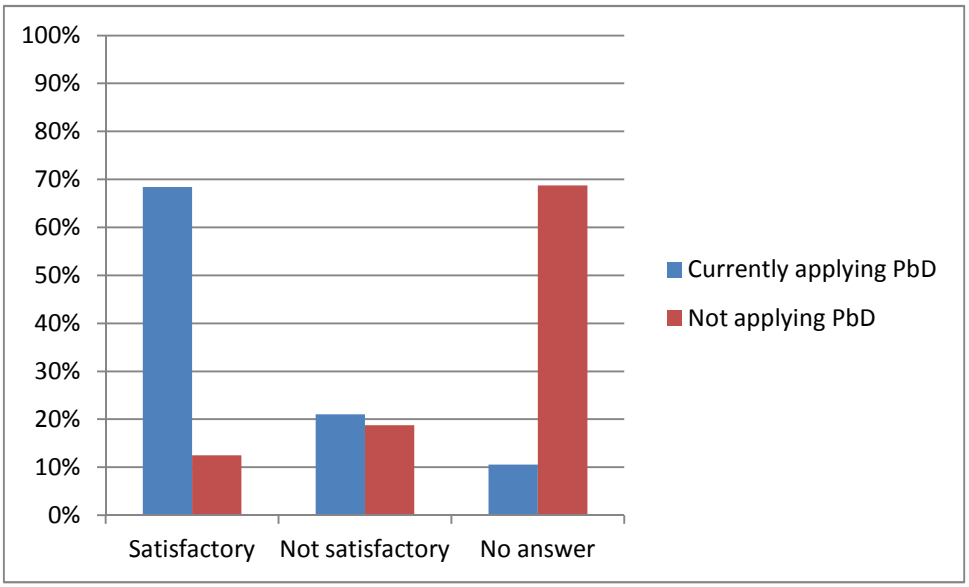


Figure 12 Organizations satifaction with respect to Privacy by Design practices

We observe that a majority of companies currently applying Privacy by Design (in blue) are satisfied with their current practices. This, given the findings in Sections 6.2.4 and 6.2.5, where survey participant's practices are found to not completely follow all Privacy by Design steps, or not without sufficient depth, or actually not following it, indicates that more education and awareness about these types of practices is needed.

7 Summary and Conclusions

This deliverable has put forward a series of recommendations for industry, policy makers, researchers, and standardization bodies, aimed at improving the state of play with respect to the application of Privacy by Design in ICT design and development.

The recommendations formulated in this deliverable address the main issues identified in Deliverable 5.2 (PRIPARE 2015): lack of incentive from the legal framework; limitations on the technical side; lack of pressure from society; and, the variety of misconceptions existing in industry with respect to privacy, Privacy by Design, and privacy-preserving technologies.

We approach the recommendations at different levels to solve these problems. Our advice to industry is to follow closely advances in research on privacy-preserving technologies, and to not underestimate the need to count with privacy expertise at the technical level within the organization similarly to other fields such as for instance Big Data or embedded systems. These recommendations are complemented by advice to policy makers on reducing ambiguity of the law and on embedding "privacy by default" also in law-making; and by advice to researchers in order to produce technologies that are nearer to the needs of the market and easy to integrate in commercial products. Furthermore, we also provided recommendations to standardization bodies to ensure that new standards provide good support to the application of Privacy by Design.

The last section of the deliverable contains a summary of the results of the survey 'Gaps in the application of privacy by design' carried out within WP5. The answers to this survey confirm the findings made in the first tasks of WP5 in terms of the current state of play in industry with respect to privacy, and the obstacles companies find when trying to follow Privacy by Design in their developments.

Finally, we refer the interested reader to ENISA's report "Privacy and Data Protection by Design – from policy to engineering" (Danezis, et al. 2014) for further insights on privacy engineering and recommendations to embed privacy-protection mechanisms in the development of applications and services.

8 References

Antignac, Thibaud, and Daniel Le Metayer. "Privacy by Design: From Technologies to Architectures." *Annual Privacy Forum 2014 8450 (2014) 1-17*, 2014: 1-17.

Bellare, Mihir, Thomas Ristenpart, Phillip Rogaway, and Till Stegers. "Format-preserving encryption." *Selected Areas in Cryptography.* 2009. 295-312.

Cavoukian, Ann. "Resolution on PbD, 32nd International Conference of Data Protection and Privacy Commissioners." 2010.

Center for Democracy and Technology. *Recommendations for a Comprehensive Privacy Protection Framework.* February 4, 2011. https://cdt.org/insight/recommendations-for-a-comprehensive-privacy-protection-framework/ (accessed May 20, 2015).

Chase, Melissa, and Emily Shen. "Substring-Searchable Symmetric Encryption." *Privacy Enhancing Technologies.* 2015. 263-281.

CNIL. *Methodology for privacy risk management.* Commission nationale de l'informatique et des libertés, 2012.

Congress. *Senator Jackie Speier Do Not Track Me Online Act of 2011.* H.R. 654, 2011.

Council. "Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering Official Journal L 166 , 28/06/1991 P. 0077 - 0083." 1991.

Council of the European Union. "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) 15395/14 2012/0011 (COD) ." Brussels, 19 December 2014.

Council of the European Union. "Proposal for a Regulationon information accompanying transfers of funds and Proposal for a directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing - Political agreement." COM (2013) 44 final COM (2013) 45 final, 30 January 2015.

Danezis, George, et al. *Privacy and Data Protection by Design – from policy to engineering.* ENISA, 2014.

Do Not Track. *Overview.* http://donottrack.us/ (accessed May 20, 2015).

EDPS. *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation – Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe.* EDPS, 2014.

EPTA. *European Parliamentrary Technology Assessment.* 2015. http://eptanetwork.org/about.php (accessed May 18, 2015).

European Commission. *2014 impact assessment (IA) reports / IAB opinions.* http://ec.europa.eu/smart-regulation/impact/ia_carried_out/cia_2014_en.htm#markt (accessed May 10, 2015).

European Commission. "European Commission. „Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union 4.11.2010 COM." 2010.

European Commission. "Impact Assessement - Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the

financial system for the purpose of money laundering, incl. terrorist financing SWD(2013) 21." Commission Staff Working Document, Strassbourg, 2013.

—. *Impact Assessment.* last updated 24/04/2015. http://ec.europa.eu/smart-regulation/impact/background/background_en.htm (accessed May 18, 2015).

European Commission. "Impact Assessment Guidelines SEC(2009) 92." 2009.

European Commission. *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing /* COM/2013/045 final - 2013/0025 .* Brussels: European Commission, 2013.

European Parliament. "European Parliament legislative resolution on the 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 COM(2012)0011 - 07 0025/2012, Brussels, 14 March 2014.

European Parliament, Council, Commission,. *Interinstitutional Agreement on better law-making.* Brussels: OJ 2003 C321/01, 2003.

European Union. "Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration OJ L 344 , 28/12/2001." 2001.

Federal Trade Commission. "Prepared Statement of the Federal Trade Commission on Do Not Track Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on the Energy and Commerce, United States House of Representatives." Washington, 2010.

FP7 PACITA project. *General Info.* 2012. http://pacita.strast.cz/en/conference/general-info (accessed May 18, 2015).

Hansen, Marit. "Top 10 Mistakes in System Design from a Privacy Perspective." In *Privacy and Identity Management for Life - 7th IFIP Summer School - Revised Selected Papers*, by Jan Camenisch, Bruno Crispo, Simone Fischer - Hubner, Ronald Leenes and Giovanni Russelo. Trento, Italy: Springer, 2011.

ICO. *Conducting Privacy Impact Assessments - Code of Practice.* Information Commissioner's Office, 2014.

Jaakkola, Hannu, and Bernhard Thalheim. "Architecture-driven modelling methodologies." In *Proceedings of the 2011 conference on Information Modelling and Knowledge Bases XXII*, by Anneli Heimbürger et al, 98. IOS Press, 2011.

john. *stuff.*

Kamara, Seny, Charalampos Papamanthou, and Tom Roeder. "Dynamic searchable symmetric encryption." *ACM conference on Computer and communications security.* ACM, 2012. 965-976.

Kint, Jason. *Advertising Age: Debunked: Five Excuses for Dismissing Do Not Track.* April 10, 2015. http://adage.com/article/digitalnext/5-excuses-dismissing-track-debunked/297992 (accessed August 22, 2015).

Knight, Kenneth E. "A Descriptive Model of the Intra-Firm Innovation Process." *The Journal of Business* 40, no. 4 (1967): 478-496.

LIBE Committee of the European Parliament. "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 (GDPR), unofficial consolidated version after LIBE vote provided by the Rapport." 2013.

Luchaup, Daniel, Kevin P. Dyer, Somesh Jha, Thomas Ristenpart, and Thomas Shrimpton. “LibFTE: a toolkit for constructing practical, format-abiding encryption schemes.” *USENIX Security Symposium.* 2014. 115.

Microsoft Corporate Blogs. *Microsoft on the Issues.* 3 April 2015. http://blogs.microsoft.com/on-the-issues/2015/04/03/an-update-on-microsofts-approach-to-do-not-track/ (accessed August 22, 2015).

Nord, Robert L., et al. *Integrating the Architecture Tradeoff Analysis Method (ATAM) with the Cost Benefit Analysis Method (CBAM).* Carnegie Mellon University, 2003.

Office, Information Commissioner's. "Conducting privacy impact assessments code of practice." 2014.

Organisation for Economic Co-operation and Development (OECD). *OECD Guidelines Gov-erning the Protection of Privacy and Transborder Flows of Personal Data.* OECD, 2013.

Peissl, Walter. "Responsible Research and Innovation: The Case of Privacy." In *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, by European Commission. Luxembourg: Publications Office of the European Union, 2011.

PRIPARE. "D1.2 Privacy and Security-by-Design Methodology." 2015.

PRIPARE. "D5.1 State-of-play: current practices and solutions." 2014.

PRIPARE. "D5.2 Multilateral gap analysis: identification of research gaps." 2015.

Senden, Linda. *Soft Law in European Community.* Oxford: Hart Publishing, 2004.

The British Institute of International and Comparative Law. *Comparative implementation of EU Directives (II) on Money Laundering.* London: City of London, 2006.

TÜVIT Nord group. *ULD Privacy Seals.* 2015. https://www.tuvit.de/en/privacy/uld-privacy-seal-1075.htm (accessed May 20, 2015).

W3C. *Tracking Preference Expression (DNT) W3C Editor's Draft 17 June 2015.* Specification, W3C, 2015.

Wilson, E. Bright. *An Introduction to Scientific Research.* McGraw-Hill, 1952.

Zibuschka, Jan, and Rossnagel, Heiko. *Designing Viable Security Solutions .* AMCIS 2011 Proceedings - All Submissions. Paper 284, 2011.

Annex I: Case studies

The case of Anti-Money Laundering Directive

To combat money laundering and financial terrorism the EU has adopted legislation since a while ago. The first **Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering** was already adopted on the **10 of June 1991** (Council 1991) **and amended by the second one** (Directive 2001/97/EC) ten years later (European Union 2001). The Directive was adopted under the co-decision procedure with overarching goal the fight against financial crime.

In 2002 in order to help the European legislative bodies perform such assessments, the European Commission launched 'impact assessments' (IA) as a systematic way to assess potential impacts stemming from a piece of legislation (European Commission last updated 24/04/2015). This new impact assessment system was an action of the Better Regulation Action Plan and of the European Strategy for Sustainable Development, and later the Lisbon Strategy for growth and jobs of 2005 (European Commission last updated 24/04/2015).The first IA were performed in 2003 (only 20 of them in 2003) and gradually increased to around 70 or more per year (European Commission n.d.). Since no IA took place for the Second Anti-Money Laundering Directive, it is unclear to what extent and in what way the legislator assessed potential impacts to fundamental rights and freedoms of individuals of this Directive at the time of its adoption.

A key element in the Directive was the requirement on banks and other financial institutions to report suspicious transactions to the relevant competent authorities and the prohibition on "tipping off", which meant prohibition to alert customers about the fact that a suspicious transactions report has been made. Even though customers may have been made aware at their initial interactions with the bank that their personal data may be used to comply with anti-money laundering requirements, the fact that they had no access to the information that a suspicious transactions report has been made 'against them' was essentially in conflict with the right of the data subject to obtain access to information under Article 12 of the Data Protection Directive 95/46/EC. A comparative report on the implementation of the Directive in 6 Member States illustrated that data protection constituted a concern in some member states. However the majority of the member states took the view that the battle against money laundering takes precedence over data protection and privacy. (The British Institute of International and Comparative Law 2006) Even though the Second Anti-Money Laundering Directive triggered to some extend privacy and data protection concerns, no impact assessment seems available for the third anti money laundering directive 2005/60/EC.

In order to strengthen the Internal Market by reducing complexity across borders, to safeguard the interests of society from criminality and terrorist acts and to streamline with the international approach, the Commission proposed a draft for the Fourth Anti-Money Laundering Directive (European Commission 2013). The proposal for the Directive was drafted after an IA, which, amongst others, analysed the potential consequences of the proposed legal framework with respect to the current EU rules. With regards to data protection, the IA illustrated the need to clarify the interaction between anti-money laundering/combating terrorist financing and data protection requirements in the text of the Directive. (European Commission 2013)

In particular, the IA analysed the impact of the legislative proposal on fundamental rights and highlighted that some of the proposed measures may involve a degree of limitation to the right

of privacy and data protection and thus the proposed measures should be balanced in an appropriate way against those limitations. Some examples concerned the provisions of the draft Directive on the availability of information on shareholders, requirements for data retention by relevant entities as well as personal data transfers in third countries. (European Commission 2013) After the IA and the inter-institutional debate, the latest draft proposed by the Council in January 2015 took a privacy preserving approach by imposing full anonymisation requirements to data shared at cross border level (Recital 15a) (Council of the European Union 30 January 2015).

The example of the Anti-money Laundering legislation illustrates the need to implement privacy/data protection by design in policy and law making. Currently impact assessment guidelines guide the Commission on the way to balance different economic, societal, political interests of the union. Privacy is a possible societal impact which may affect individuals, private and family life, personal data (European Commission 2009). Departing from this already existing practice, there is a need to investigate how privacy can be considered systematically in policy making. Privacy risk assessment methodologies should be combined with other methods, as proposed by the FP7 PACITA project, such as cross-disciplinary expert studies, stakeholder involvement, citizen consultation and parliamentary discourse (FP7 PACITA project 2012). Existing approaches, such as Privacy Impact Assessment (ICO 2014) or Technology Assessments, such as the ones undertaken by the EPTA network (European Parliamentary Technology Assessments) (EPTA 2015) should be considered to foster interaction and communication in formulating privacy-preserving policy and law.

The case of the Do Not Track mandate for legislation in the US

This section introduces an example where the need to mandate Privacy/Data Protection by Design was mandated in legislation. Such an example is the case of Do Not Track legislation in the US which aims at regulating behavioral advertising. Previously existing practices of websites performing online behavioral advertising revealed policy and legal gaps in the US. The FTC published a testimony illustrating such gaps by pointing out that consumers have the right to choose not to be tracked by websites and to prevent them from tracking their online behaviors. Eventually, the Congress adopted legislation which provided for the obligation to adopt mechanisms implementing data protection by design and by default features.

Do Not Track is a technology that enables users to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms (Do Not Track sd). It is also a policy framework which has been developed in the US since a while ago. In 2009 the FTC published a testimony pointing out the risks of behavioral advertising and highlighted the need to create a mechanism providing users the choice to opt out of tracking (Federal Trade Commission 2010). The proposed policy framework was intended to inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy, and guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines (Federal Trade Commission 2010).

The policy framework idea of the FTC was further followed up by the Congress. In February 2011, Senator Speier introduced the “Do Not Track Me Online Act of 2011”, which would authorize the FTC to promulgate regulations requiring online advertisers and websites to allow users to opt out of having their online activities tracked through the creation of a Do Not Track mechanism (Congress 2011). The act provided users the ability to in principle block personal data collection for online behavioral advertising purposes. This legislative intervention as a part

of the whole policy framework of Do Not Track initiated by FTC support to the policy of Do Not Track produced remarkable results in a few short months, as both Microsoft and Mozilla announced their intent to develop browser features that would allow consumers to prevent third-party tracking (Center for Democracy and Technology 2011).

In parallel with the above regulatory activity, the World Wide Web Consortium ('W3C') has been developing a DNT standard. In July 2015 the W3C Tracking Protection Working Group has published its work in progress which introduces a specification for the Tracking Preference Expression (W3C 2015). As W3C mentions, '*the specification defines the DNT request header field as an HTTP mechanism for expressing the user's preference regarding tracking, an HTML DOM property to make that expression readable by scripts and APIs that allow scripts to register site-specific exceptions granted by the user. It also defines mechanism for sites to communicate whether and how they honour a received preference through the use of the Tk response header field and well-known resources that provide a machine readable tracking statues*'.

Whereas the conclusions of this standardisation activity will help specify the actual content of the DNT, its efficiency may be questioned as the DNT request is expected to be left on consumer choice (Kint 2015). Companies will be able to remain compliant with the standard, even if they do not turn the DNT setting on by default. In such cases the task of managing emerging privacy risks will be externalised to the users. Addressing this issue, Microsoft explicitly mentioned in April 2015 that DNT will not be the default state in Windows, however, first time or users that have upgraded their software "will be provided with clear information on how to turn this feature on in the browser settings should they wish to do so" (Microsoft Corporate Blogs 2015).