https://doi.org/10.3926/hdbr.180

Contribution of Privacy by Design (of the Processes)

Santiago Martín-Romo Romero
PhD in the Business Administration. Certified Information System Auditor from the ISACA Association. Author of several books and papers on the area of information systems with research activities focused in the security and privacy of business processes. Spain.

Carmen De-Pablos-Heredero
PhD in Economics & Business Organization. Director of the Master Degree in Business Organization and Master Degree in Logistic Business Processes SAP at the Rey Juan Carlos University, Madrid, Spain. Author of several books and articles in Business & Education. Spain.

santiago.martinromo@urjc.es, carmen.depablos@urjc.es

Received: October, 2017.
Accepted: December, 2017.
Published: December, 2017.

Title
Contribution of Privacy by Design (of the Processes).

Abstract
Privacy by design (PbD) will soon be a compulsory requirement for firms processing personal data. The GDPR (General Data Protection Regulation), a new Act in the EU establishes compulsory fulfillment for firms located in the European Union from May 2018. By considering that PbD philosophy leads to protect personal data, it is proposed to start the protection from the design of business activities. Privacy from the business process management perspective has barely been studied. In this paper a group of organizational mechanisms oriented to implement protection measures based on privacy by design are provided. Based on the analysis of 18 surveys done to privacy by design and data security experts, some recommendations are offered. They are based in the analysis of strengths, weakness, opportunities and threads envisioned by the different experts.

Keywords
Privacy by design, personal data, process, security, Swot analysis.

1. Privacy by design

Business activities often demand the use of personal data

The performance of business activities requires the use of data coming from persons with whom the firm interact, employees, customers, providers or public organizations in general. These persons are owners of their data and possess a group of rights on them, all around the whole cycle data run at firms, from the collecting of data to their processing and removal (Perera, Ranjan & Wang, 2015), since all may have impact on data privacy.

The EU has promoted changes in the legislation related to privacy in such a way that in 2012, a new regulation was proposed (European Commission, 2012; European Parliament, 2014), currently GDPR. It includes the principle of privacy by design (PbD).

PbD is a concept introduced in the 90s by Ann Cavoukian, ex commissioner of Information and Privacy in Ontario, Canada (Cavoukian, 2012). She proposes preserving the privacy by developing measures that integrate the fundamentals of data protection in the technological system of information processing. This initial focus (Cavoukian, 2012) has been advanced to reach three main areas of application, as technology, business practices (organizations) and physical design (infrastructures).

Since PbD has been included in the GDPR, multiple arguments have arisen supporting this focus. ICO (2017) describes: "The basis of the privacy by design approach is that if a privacy risk with a particular project is identified, this can be an opportunity to find creative technical solutions that can deliver the real benefits of the project while protecting privacy".

Alshammari and Simpson (2017) explain: "Privacy by Design includes a lack of holistic, systematic and integrative methodologies that address the complexity and variability of privacy, and support the translation of its foundational principles into engineering activities. In some ways this is understandable: the approach was developed to take into account a range of sources and standards".

The importance of PbD has been stressed by ICDPPC (2016) PbD: "Not only engineers but also researchers need to start considering privacy engineering principles like privacy by default and privacy by design in new research, products and services". Although as Colesky, Hoepman and Hillen (2016) mention, PbD in itself lacks concrete tools to help software developers design and implement privacy friendly systems and also lacks clear guidelines on how to map specific legal data protection requirements into system requirements.

Some authors, as Bygrave (2017), consider that in the GDPR, PbD suffers from multiple flaws, in particular a lack of clarity over the parameters and methodologies for achieving its goals, a failure to communicate clearly and directly with those engaged in the engineering of information systems, and a failure to provide the necessary incentives to spur the 'hardwiring' of privacy-related interests.

This paper is related to PbD applied from the definition of business processes. It is proposed that firms, from the very first moment they forecast a business activity, they include the required assessments in relation to the personal and processing data that will have to be incorporated in that activity.

As Majdalawieh (2013) points out, privacy from the business management perspective has not been investigated at a great extent and there is a gap in the literature. No studies related to methodologies that integrate privacy in business processes have been found. This same idea is

The EU promoted in 2012 a new legislation that impacts data privacy

revealed in Anderson and Rachamadugu (2008) and in FTC (2010). The PbD "it is also a process, which is intimately tied to the design process" (Kroener & Wright, 2014).

2. The study

The main objective of this paper is to obtain and analyze the opinion of a group of experts in information privacy and security in terms of the advantages and disadvantages that may appear in firms when integrating the protection of privacy from the business processes design.

A survey has been used to collect information and SWOT analysis has been applied to explain the obtained results by means of descriptive statistics. 18 experts have participated in the collecting of data that has taken place from January 2015 to May 2015. Table 1 shows the experts' profiles.

Table 1
Organisms and experts participating in the study

ORGANIZATION	PROFILE	EXPERT IN
Consultancy firm in data protection	Manager in Data Protection	Information system's (IS) security
iTTi, Innovation & Technology Trends Institute	Manager in IS Security	IS security
Valencia University	Lecturer in legal areas	Legal issues
Big size financial entity	Manager in IS security	IS security
Big size financial entity	Manager in IS security	IS security
Insurance firm	Manager in IS security	IS security
Public firm	Manager in IS security	IS security
Castilla La Mancha University	Full time professor in computing	IS security
Big size financial entity	Manager in IS security	IS security
Murcia University	Lecturer in legal issues	Legal issues
Rey Juan Carlos University	Lecturer in legal issues	Legal issues
Organism responsible in Data Protection	Manager	Legal issues
Insurance firm	Manager of legal issues	Legal issues
Carlos III University	Full time professor in Business Organization	IS security
Carlos III University	Lecturer in IS security	IS security
Freelance in data protection	Expert in legal issues	Legal issues
Polytechnic University of Valencia	Lecturer in IS security	IS security
Consultancy firm in data protection	Manager	Legal issues

As it is shown, all the different profiles that take part in the implementation of the system have been considered.

Statistical processing of data has taken place in a spreadsheet.

This new legislation includes the principle of privacy by design (PbD)

Strengths and weaknesses are related to the internal analysis of the organization (leadership, strategy, people, alliances/resources and processes).

Opportunities and threads are related to the external analysis of the organization (market, industry and competence).

3. The questions and the answers

The survey designed to facilitate the obtaining of information related to weakness, threads, strengths and opportunities derived from the integration of data protection from process design and it is based in 8 questions.

The questions proposed to orient the experts in potential strengths, weakness, opportunities and threads, have been built from the dimensions oriented in the PEST techniques (Johnson & Scholes, 1997), this is to say, political dimension (by including the legal one), economic dimension, social dimension and technological dimension.

Questions related to political and legal issues are shown in table 2.

Table 2
Answers related to political and legal issues

THREADS	OPPORTUNITIES
Offer information to regulation organisms in terms of data protection.	Inclusion of this philosophy in the draft for the European Code for Data Protection 2012.
In case the degree of law fulfillment is not enough, the mix of both with the definition of processes may not be successful.	
The uncertainty on the time where the 2012 European regulation will be finally approved.	
STRENGTHS	**WEAKNESS**
Less effort in attending questions related to the Data Protection Agency (guardianship of affected).	
Improvement in the management of the protection of firm's privacy.	
It enables the detection of cases in which it is recommended developing a PIA (Privacy Impact Assessment).	

Concerning to the proposed answers that belong to the political and legal aspects (DPI, 2013) the situation referring to the new legislation dealing with future legislation concerning to privacy in the EU (European Union, 2016), the level of uncertainty at firms is increasing according to the implementation of GDPR, that contemplates the crisis, the additional charge that can imply the economic and work processes approval as the procedures and documentation and information approval.

In views of the degree of law fulfillment, according to the statistics elaborated, the number of firms that must register their files in Spain is still high (INTECO, 2012; DPI, 2013).

PbD implies integrating data protection in the technological system of information processing

In GDPR, article number 25 explains the future obligation that firms have to elaborate and apply internal policies of data protection that offer guidelines for the principle of "privacy by design" and the "privacy by default" is described (European Union, 2016). For this reason, a potential opportunity to apply this philosophy has been included.

Answers related to the economic aspects are shown in table 3.

Table 3
Answers related to the economic issues

THREADS	OPPORTUNITIES
The risk of not being valued by stakeholders.	Reinforcement of the firm's image.
Delays in the time to market as a consequence of including privacy from design.	Higher levels of stakeholders' trust to the firm.
Use of resources (opportunity costs) in an area that it is not the core of the business in relation to competitors.	Differentiation facing competitors.
The crisis, it does not allow applying resources to these issues.	Use as marketing tool.
STRENGTHS	**WEAKNESS**
Saving in costs in the long run (excluding sanctions).	There will be more costs.
Decrease of the time and effort done in the post implementation of the defined process.	It will slow the definition of processes and therefore the putting into practice of a new business.
	An excessive effort in data security in comparison with expected results.

The proposed answers belong to the economic aspects that are related with the reluctant to the self-adoption of privacy practices by firms. The legislation could oblige them to assure that the principles of privacy are followed. As an example, GDPR establishes the application of sanctions up to the 4% of the results that the firm obtains at a worldwide level. These strong sanctions promote the adoption of the privacy practices required for the fulfillment of legislation (PRIPARE, 2014).

Recent security gaps in information systems have located privacy as a high rated asset at firms. PwC in different reports (PwC, 2013; PwC, 2014) reveals that many firms have decided to shape their business around customer's desires and most CEOs would promote changes to maintain and make their customer's portfolio increased. Customers value each time more the respect for data privacy and confidentiality (PwC, 2015a).

In the European trust barometer (Edelman, 2014) it is confirmed that an 85% of customers believe that whenever an organization exhibits data protection, it has positive effects in its compromise with the firm and with the perceived value of products and services, offering in this second effect the most outstanding impacts. This statement is reinforced by studies as Tsai, Egelman, Cranor and Acquisti (2011) or Jentzsch, Preibusch and Harasser (2012), where it is proofed that users are willing to pay more money to receive a service that respects the privacy more than an invasive alternative of it. Therefore, firms or organizations that respect privacy obtain more competitive advantages (Cavoukian, 2008; Witt 2012; PRIPARE 2014).

A methodology to practice PbD is recommended as firms must fulfill legal requirements by 2018

The respect to privacy on the transaction of products and services will not just produce benefits in the way of increasing returns as a consequence of competitive advantage, but it will also impact in the reduction of risk to potential privacy infringements (Cavoukian, 2008; Watson et al., 2009), and consequently it will avoid non-desired effects in the corporate reputation, demands and costs of fines (Ponemon Institute, 2013). According to the analysis of the study performed in 2015 over 350 firms from 11 countries (Ponemon Institute, 2015), the cost of security breaches produced a 3.8 million of dollars as mean. A 23% of the increase in comparison to 2013 has been produced. For this research a security breach is produced whenever protected or confidential sensitive data are lost or stolen and therefore put on risk.

Answers related to social aspects are shown in Table 4.

Table 4
Answers related to social aspects

THREADS	OPPORTUNITIES
STRENGTHS	**WEAKNESS**
Higher data protection of individuals that interact with the firm (degree of accomplishment).	
Less future effort required to attend the right of affected persons (especially in terms of rectification or cancellation).	

The proposed answers belong to the social aspects related to the achievement of higher degrees of transparency for citizens, by protecting one of the most valuable assets in the organization, personal data from customers, employees, etc. (ICO, 2010; DPI, 2013).

As environmental awareness has made firm's ecological practices being increased; privacy awareness has increased the adoption of good practices in this concrete area. A survey performed by London Economics (2010) provides clear evidence that "low levels of information at firms on PET (privacy enhancing technologies) negatively impacts in their perception of benefits". It seems clear that as more information a firm has on PET and privacy practices, an increase on the perception of benefits will take place and its adoption will also increase. Self-regulation practices can therefore increase the level of awareness and the adoption of practices of privacy. Self-regulation has turned into an efficient stimulus that can support and make increase the adoption of practices of privacy, as for example, EU PIA-RFID (2011).

In a recent survey to consumers developed by PwC (PwC, 2015b), a 24% confirmed that their trust in the capability of firms to protect personal data has decreased in the last 12 months. Cybernetic security incidents are today so common that the number increased from 48% in 2013 to 42.8 million of dollars (PwC, 2015a). Last year, almost all the industries have met affected, by incurring in significant costs when managing and mitigating these incidents (PwC, 2015a). So it is not strange that CEOs keep worried for cybernetic security as a potential thread that has increased from 48% to 61% in just one year.

In the report *Achieving Total Retail* (PwC, 2014), that analyzes the perspectives and consumption habits from on line buyers, from 15.000 interviews sent to digital buyers in the whole world on the implications for the companies in the distribution and consuming industries in the next

First step to propose one methodology consists of knowing main opinions coming from experts

years, a 43% of surveyed declared not buying on line because they felt worried for their personal data security.

In the last years espionage programs have been discovered as PRISM (Greenwald & MacAskill, 2013), in which big size companies operating in the information and communication technology industry are involved (Facebook, Yahoo Google, LinkedIn or Microsoft) together with the NSA (Ackerman, 2014). Some initiatives coming from these same companies have arisen so that worldwide companies face practices that regulate the government vigilance and the Acts that regulate their access to information. This is aligned with ancient initiatives as the OECD original principles in this specific issues (OECD, 1980), updated in 2013 (OECD, 2013) or the Madrid Declaration in 2009. This initiative promoted by the industry shows the attempt that big size firms can adopt best practices in terms of security and privacy that obstacle the government espionage programs.

Answers related to technological aspects are shown in table 5.

Table 5
Answers related to technological aspects

THREADS	OPPORTUNITIES
Possibilities of errors in the application of this philosophy produced by professionals that are not trained enough.	Possibility of contracting external services that help in the application of this philosophy.
STRENGTHS	**WEAKNESS**
Higher coordination and collaboration amongst multidisciplinary teams for the definition of processes.	The integration of process privacy analysts will not be welcomed. An excess of will to be independent from other agents.
It turns in an increase of security in general.	Excess of questions related with integrating the definition of processes (privacy, quality, security, labor risks, environment, etc.).
	Lack of methods to put into practice correctly this kind of focus.
	Lack of trained employees (in terms of privacy and in the management of processes) in the Organization to develop this kind of approaches.

In the case of responses derived from the technological aspects, it is worth to stress that when the technology presents an acceptable degree of maturity, in general, it is easier to be understood by everyone, being this time best communicated. Besides, generally speaking, maturity reduces the technological cost. To reduce the cost of privacy practices as better understanding its functioning will decrease adoption barriers (PRIPARE, 2014).

A more efficient way to transfer the research results for the successful exploitation of the market is standardization. The normalization of privacy practices facilitates its adoption, the interoperability and it can offer peaceful to consumer when new technologies are applied (PRIPARE 2014). After the disclosure of PRISM (Greenwald & MacAskill, 2013), one of the action areas to maintain the continuity in the data flows between the EU and USA consists on "promoting privacy rules at an international level" (European Commission, 2012).

Recent reports as Eurobarometers (European Commission, 2017) or reports from independent firms (Rainie, Kiesler, Kang & Madden, 2013) explain how a great majority of users in Internet

Information has been collected from 18 experts in data privacy and security issues

are worried by the use of their data when they are transmitted to providers in the payment process by using a card and Internet mobile phones.

These conclusions match with academic research from Tsai et al. (2011) and Egelman, Felt and Wagner (2013) where it is shown that users that expose their personal data prefer providers that offer them better warranties in terms of privacy, and they are even prepared to pay higher prices for the use of systems that highly protect their privacy.

In the industry different viewpoints exist in how increasing privacy in ICT systems. The adoption of privacy practices depend to a great extent on the industry where the firms obtain their benefits. While some industries as financial or health services are more opened to accept privacy practices, since they are accustomed to being evaluated in more strict exam by legal obligations (more sensitive data are processed), other industries that base their business models in the exploitation of personal data (for example, publicity on line or big data) are opposed to any practice of privacy that can endanger their business model. This trend has been confirmed by the ENISA Annual Forum in Privacy report held in 2012: "A number of technical aspects have been considered to solve the problem of privacy, targeting different parts of the privacy architecture. However, the lack of initiatives in the area of private life, where the industry will establish the requirements and initiatives to provide a complete model was once more reinforced" (ENISA 2012).

It is notorious that in this field, a "privacy industry" is being created by developing and deploying trustful frameworks and privacy solutions to enable the accomplishment of the more strict legislation.

In the PRIPARE (2013) project, sponsored by the EU with the main objective to offer a method for privacy protection that can be integrated in the development cycle of systems information, a survey was done to detect PbD practices applied to firms and the problems related with their application. Amongst the main questions, one was focused in finding out the main motivations to apply PbD by providing as potential answers some of the strengths and opportunities included in our questionnaire. Amongst main motivations, it is worth it to remark the following ones:

- Integrate the privacy that offers competitive advantages.
- Economic incentives materialized in the reduction of risks dealing with the collecting of sensitive data.
- Legal compliance.
- Standardization of requirements.
- Self-regulation of the manufacturing industry.
- Maturity and accessibility to technologies that may improve privacy.
- Compromise for the protection of customer's privacy.

4. Participants in the study

Data for the performing of the analysis have been obtained from the survey realized to a group of experts in privacy that belong to the technical environment terms of security and legal aspects derived from the information.

For the selection of experts that take part in the analysis, the following factors have been considered:

- Experience and knowledge in terms of information security and privacy / data protection, and industrial reputation.

Information coming from experts has been analyzed under a SWOT framework

- Diversity of the profiles in the group of organizations: firms, universities, associations, control authorities in the field of personal data protection, legal, consultancy and support service providers related with the protection of personal data.

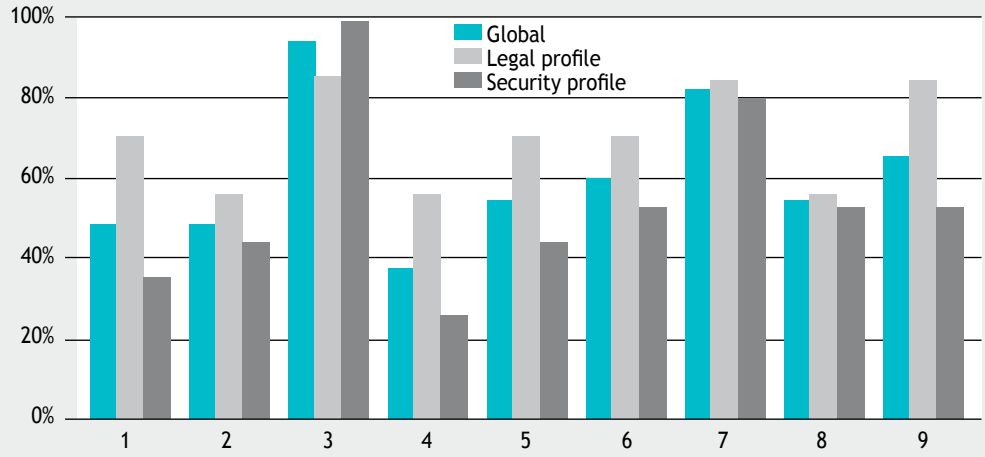
18 complete questionnaires have been received. Experts present two profiles, one of a more legal character and a second one with a more technical one, as shown in table 1. This will help getting the most complete and required information from the different perspectives.

5. Obtained results

Next the different figures showing the opinions of experts on the weakness, threads, strengths and opportunities that are considered when implementing the philosophy for the integration of the protection of data privacy from the process design perspective are provided.

Figure 1 shows that from the proposed strengths, the first chosen by experts has been the obtaining of higher degrees of personal data protection (option 3: 94%), being this option highly valued by the security profiles facing the legal ones. Second option chosen has been the improvement in the management of privacy protection in the firm (option 7: 83%), in this case, with a percentage similar between legal and security profiles. The general increase of security that implies dealing with privacy from process design has also been highly rated (option 9: 67%), in this case much better appreciated by legal than security profiles. Rest of options have been chosen by half of surveyed people, except the option 1 mainly chosen by legal profiles (saving costs in the long term less sanctions) and option

Figure 1
Results in strengths



1 Saving costs in the long run (excluding sanctions).
2 Decrease of the time and effort done in the post implementation of the defined process.
3 Higher data protection of individuals that interact with the firm (degree of accomplishment).
4 Higher coordination and collaboration amongst multidisciplinary teams for the definition of processes.
5 Less future effort to attend the right of affected persons (especially in terms of rectification or cancellation).
6 Less effort in attending questions related to the Data Protection Agency (guardianship of affected).
7 Improvement in the management of the protection of firm's privacy.
8 It enables the detection of cases in which it is recommended developing a PIA (Privacy Impact Assessment).
9 It turns in an increase of security in general.

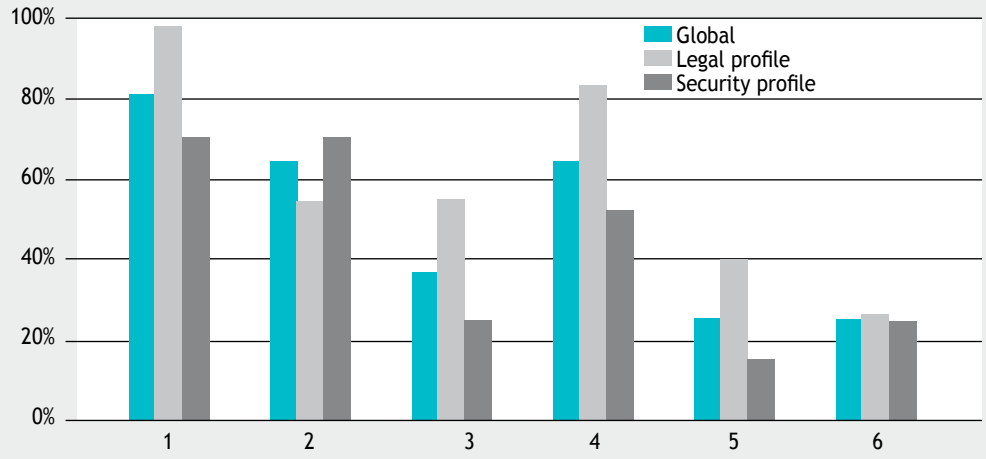
Harvard Deusto Business Research. Volume VI. Issue 3. Pages 176-191. ISSN: 2254-6235

Strengths mainly have to do with providing higher degrees of data protection to data

5 (less effort, future in attending affected rights, specially rectification and cancellation). The least chosen option (option 4: 39%) is the one in counting on with the coordination and collaboration amongst multidisciplinary teams to define processes. This option has been highly rated by legal profiles contrary to security profiles.

Figure 2 shows that the opportunity mostly chosen (option 1: 83%) would proportionate the integration of privacy in the design of processes is the increase in the image of the firm, highly rated by legal profiles. Second place (option 2: 67%) has turned into the highest value in terms of trust by firm's data holders, highly valued by security profiles and in the short term (option 4: 63%) to obtain a differentiation respect to competitors, being in this case highly valued by legal profiles. The alternative that this philosophy can be included in the proposal of the 2012 European regulation in terms of data protection has not been considered (option 5: 28%), although this option has turned into more positive values in legal profiles and option 6 with the possibility of contracting external services that allow the application of this philosophy, showing similar percentages in both profiles. Option 3, the use as marketing, has been highly valued by technical profiles.

Figure 2
Results in opportunities (own elaborated)



1 Reinforcement of the firm's image.
2 Higher levels of stakeholders' trust to the firm.
3 Use as marketing tool.
4 Differentiation facing competitors.
5 Inclusion of this philosophy in the draft for the European Code for Data Protection 2012.
6 Possibility of contracting external services that help in the application of this philosophy.

Figure 3 shows that from weaknesses, the one chosen in the first place (option 6: 83%) has been the existence of lack of prepared workers (in privacy and in process management) in the Organization to deal with this kind of focus – mainly chosen by legal profiles. Second option (option 7: 72%) the lack of methods to put into practice this focus. In this option, legal and security profiles agree. The least chosen weakness (option 4: 6%) has been the excessive effort to reach potential, scarcely chosen by both profiles, legal and security ones. The assessment done by experts in terms of costs

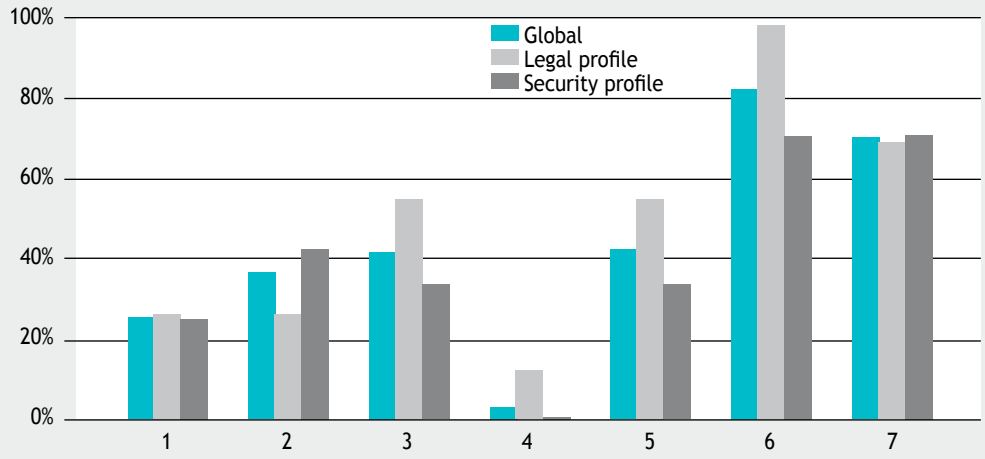
Harvard Deusto Business Research. Volume VI. Issue 3. Pages 176-191. ISSN: 2254-6235

Opportunities come from the improvement in firm's image and trust from different stakeholders

can imply implementing this kind of focus (option 1), since just a 28% of them have considered the option of cost increase, agreeing legal and security profiles.

Options 3 ("The integration of process analysts in privacy would not be welcomed. An excessive desire to be independent amongst the groups") and 5 ("Two much questions to integrate in the definition of processes (privacy, quality, security, labor risks, environment…)" although they are not outstanding globally (close to a 40%), they are quite frequently chosen (almost a 60%) by legal profiles. Contrary to 2 ("It would slow down the definition of processes and the putting into practice of a new business") mostly selected by security profiles (a 43%). It is under 30% in the case of legal profiles.

Figure 3
Results in weakness (own elaborated)



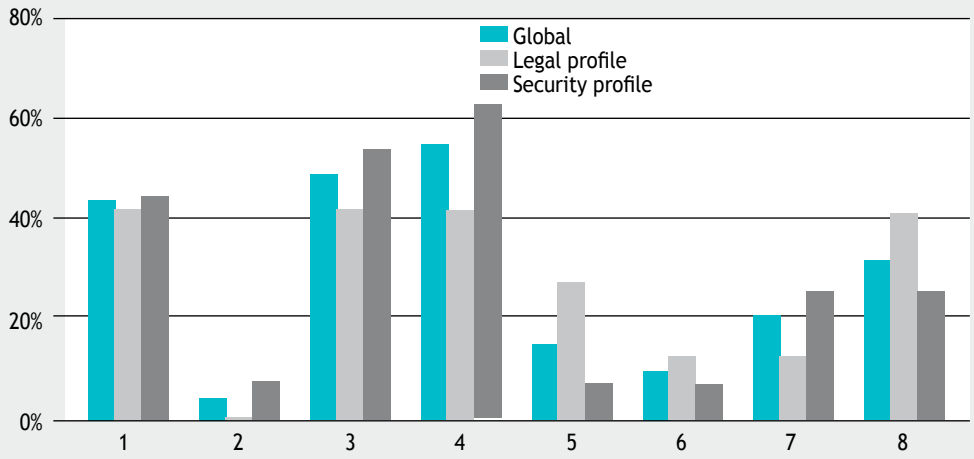
1 There will be more costs.
2 It will slow the definition of processes and therefore the putting into practice of a new business.
3 The integration of process privacy analysts will not be welcomed. An excess of will to be independent from other agents.
4 An excessive effort in data security in comparison with expected results.
5 Excess of questions related with integrating the definition of processes (privacy, quality, security, labor risks, environment, etc.).
6 Lack of trained employees (in terms of privacy and in the management of processes) in the organization to develop this kind of approaches.
7 Lack of methods to put into practice correctly this kind of focus.

In Figure 4 it is shown how threads can imply delays in time to market as a consequence of including privacy by design (option 4: 56%), mostly chosen by security profiles. Second place, as the effort performed by the firm has not been valued (option 3: 50%), it has also been mostly chosen by the security profiles and last, the use of resources (cost of opportunity) in an area that does not belong to the business relating to competitors (option 1: 44%), chosen equally by legal and security profiles. Rests of options have not been chosen often. Although legal profiles have rated more "5" option than security ones. "There is a possibility to contract this option to external professional that are not prepared" and "Possibility to contract the application of this philosophy to external non prepared professionals" and "8". Crisis, today, does not allow dedicating resources to these issues.

Harvard Deusto Business Research. Volume VI. Issue 3. Pages 176-191. ISSN: 2254-6235

Weaknesses are related to the lack of training and prepared profiles in data privacy issues

Figure 4
Result in threads (own elaborated)



1 Use of resources (opportunity costs) in an area that it is not the core of the business in relation to competitors.
2 Offer information to regulation organisms in terms of data protection.
3 The risk of not being valued by stakeholders.
4 Delays in the time to market as a consequence of including privacy from design.
5 Possibilities of errors in the application of this philosophy produced by professionals that are not trained enough.
6 In case the degree of law fulfillment is not enough, the mix of both with the definition of processes may not be successful.
7 The uncertainty on the time where the 2012 European regulation will be finally approved.
8 The crisis, it does not allow applying resources to these issues.

6. Conclusions

The inclusion of requirements to protect people's privacy in their data processing at firms can be done at early stages, when the processes are being designed or later on, once they are implemented.

The integration of privacy data policies from the processes' design leads to the development of a group of strengths, opportunities, weakness and threads that have been judged by a group of recognized experts in data security, from the legal and technical fields.

Experts surveyed consider that strengths in this approach mainly have to do with providing higher degrees of data protection to data from people processed in the firm and opportunities come from the improvement in the image of the firm, the obtaining of higher degrees of trust of data owners towards the firm and the obtaining of a differentiation respect to competitors. Weaknesses come from the lack of training and the lack of prepared profiles (in terms of privacy and process management) in the firm to deal with this kind of focus and the lack of methods to put them into practice. Threads are related to the potential impact on the time to market, and the effort done by the firm by employing its own resources (cost of opportunity) in an area that it is not the core of the business and as a consequence of the low valuation that data owners can offer to this focus.

The most popular three options chosen for each SWOT concept are shown in table 6.

Threads are related to potential impact on time to market and the effort done by firms to practice PbD

Table 6
Options prioritized in the SWOT analysis at a global level

STRENGTHS	WEAKNESS
It provides higher levels of data protection to all the agents the firm interact with.	There is a lack of training and lack of skilled staff (in privacy and process design) to follow this kind of frameworks.
It improves the management of privacy protection.	Lack of methods to put into practice.
A general increase of security that implies managing privacy from the processes design.	Too many issues to integrate the definition of processes (privacy, quality, security, labor risks, environment, etc.).
OPPORTUNITIES	**THREADS**
The image of the firm is improved.	Delays in the time to market.
Higher levels of trust are obtained in the data owners.	Greater business effort employing resources (opportunity cost) in a non-core competence of the firm.
It helps getting a differentiation facing competitors.	Data owners cannot evaluate the focus.

Table 7 presents by profiles (legal or security) the highly chosen options. The existence of low differences in the options selected by both profiles can be stressed.

Table 7
Options mostly selected in the SWOT analysis according to the profiles

	LEGAL PROFILE	SECURITY PROFILE
Strengths	3. Higher data protection of individuals that interact with the firm (degree of accomplishment). 7. Improvement in the management of the protection of firm's privacy. 9. It turns in an increase of security in general.	3. Higher data protection of individuals that interact with the firm (degree of accomplishment). 7. Improvement in the management of the protection of firm's privacy. 9. It turns in an increase of security in general. 6. Less effort in attending questions related to the Data Protection Agency (guardianship of affected). 8. It enables the detection of cases in which it is recommended developing a PIA (Privacy Impact Assessment).
Weakness	6. Lack of trained employees (in terms of privacy and in the management of processes) in the organization to develop this kind of approaches. 7. Lack of methods to put into practice correctly this kind of focus. 3. The integration of process privacy analysts will not be welcomed. An excess of will to be independent from other agents.	7. Lack of methods to put into practice correctly this kind of focus. 2. It will slow the definition of processes and therefore the putting into practice of a new business.
Opportunities	1. Reinforcement of the firm's image. 4. Differentiation facing competitors. 3. Use as marketing tool.	1. Reinforcement of the firm's image. 2. Higher levels of stakeholders' trust to the firm. 4. Differentiation facing competitors.
Threads	1. Use of resources (opportunity costs) in an area that it is not the core of the business in relation to competitors. 3. The risk of not being valued by stakeholders. 4. Delays in the time to market as a consequence of including privacy from design. 8. The crisis, it does not allow applying resources to these issues.	4. Delays in the time to market as a consequence of including privacy from design. 3. The risk of not being valued by stakeholders. 1. Use of resources (opportunity costs) in an area that it is not the core of the business in relation to competitors.

Harvard Deusto Business Research. Volume VI. Issue 3. Pages 176-191. ISSN: 2254-6235

As a consequence of this diagnosis, 4 different strategies are recommended so that firms can perform PbD

This group of strengths, opportunities, weakness and threads orient in the elaboration of action guides or recommendations that are going to be offered to firms and they can be considered when developing a framework of privacy by design from the process perspective to reinforce the strengths, offer solutions for weaknesses avoid threads and exploit opportunities.

According to the results, the following actions are suggested. They imply strategies and options to be put in practice so that firms can implement privacy by process design:

- Offensive strategy (strengths + opportunities):
  - Formalize the practice of privacy by process design from inside the firm, by creating procedures and organizational routines that help in its application.
  - Include as another part in the firm practices, the improvement of processes in the processing they develop from privacy.
  - Obtain whenever is possible, certifications in privacy and quality standards that proof the fulfillment with privacy.
- Defensive strategy (strengths + threads):
  - Communicate to data owners on the privacy by design focus adopted by the firm and the advantages that it implies.
  - Perform marketing actions oriented to communicate the data processing that the firms perform in terms of privacy protection.
  - Standardize tasks that help managing privacy from the process definition and that impact as less as possible in times and costs of managerial resources at firms.
- Re-orientation of strategy (weaknesses + opportunities):
  - Raise managers' awareness to consider privacy as part of all the decisions involved in the collecting and sharing of personal data.
  - Integrate the processing of privacy in all disciplines that support the process cycle in the firm, by including it in business cases, procurement processes, and project management.
  - Develop a culture of privacy awareness in employees.
  - Perform campaigns and training programs for employees in the phases of process definition to sensitize on the need to integrate the privacy in the process design.
- Survival strategy (weaknesses + threads):
  - Promote and collaborate with consultancy firms in the use of methods for integrating privacy in the definition of processes.
  - Create at organizational levels of working profiles oriented to support the culture of privacy and that can respond to the firm's employees any doubt that may arise from this specific area.
  - Incorporate privacy risks in the analysis and management of risks performed in the firm.

7. References

Ackerman, S. (2014). US tech giants knew of NSA data collection, agency's top lawyer insists. *The Guardian,* 19/03/2014. Retrieved August 8, 2015, from http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew- nsa-data-collection-rajesh-de

Alshammari, M., & Simpson, A. (2017). Towards a Principled Approach for Engineering Privacy by Design. In E. Schweighofer, H. Leitold, A. Mitrakas & K. Rannenberg (eds.), *Privacy Technologies and Policy.* APF 2017. Lecture Notes in Computer Science, vol. 10518. Springer, Cham. https://doi.org/10.1007/978-3-319-67280-9_9

Anderson, J. & Rachamadugu, V. (2008). Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure. *2008 IEEE International Conference on Services Computing,* 2, 351-358.

Bygrave, L. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review,* 4(2), 105-120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

Cavoukian, A. (2008). *Minimize Risk – Maximize Protection and Gain a Competitive Advantage: Privacy is Good for Business.* Report.

Cavoukian, A. (2012). Privacy by Design. *IEEE Technology and Society Magazine,* 31(4), 18-19. https://doi.org/10.1109/MTS.2012.2225459

Colesky, M., Hoepman, J., & Hillen, C. (2016). A Critical Analysis of Privacy Design Strategies. *IEEE Symposium on Security and Privacy Workshops,* 33-40. https://doi.org/10.1109/SPW.2016.23

DPI (Data Privacy Institute) (2013). *Reflexiones sobre el futuro de la Privacidad en Europa. II Edición del Estudio de la propuesta de Reglamento de Protección de Datos de la UE.* ISMS Forum Spain.

Edelman (2014). *2014 Edelman Trust Barometer.* Retrieved August 23, 2015, from http://www.edelman.com/2014-edelman-trust-barometer/

Egelman, S., Felt, A., & Wagner, D. (2013). Choice Architecture and Smartphone Privacy: There's a Price for That. In R. Böhme (ed.), *The Economics of Information Security and Privacy,* 211-236, Springer. https://doi.org/10.1007/978-3-642-39498-0_10

ENISA (European Union Agency for Network and Information Security) (2012). *Report on Annual Privacy Forum 2012.* Retrieved August 20, 2015, from https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/report-on-annual-privacy-forum-2012

EU PIA-RFID (2011). *Privacy and Data Protection Impact Assessment Framework for RFID Applications.* Annex to the Opinion 9/2011 on the revised Industry Proposal. Brussels: Article 29 Data Protection Working Party. Retrieved August 18, 2015, from http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework- final.pdf

European Commission (2012). *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) 11 final. 2012/0011 (COD). Retrieved August 23, 2015, from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1419003505129&uri=CELEX:52012PC0011

European Parliament (2014). *European Parliament legislative resolution of 12 March 2014 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 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading). Retrieved August 13, 2016, from http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402

European Commission (2017). *Europeans' attitudes towards cyber security.* Special Eurobarometer 464a. TNS Opinion & Social. Retrieved December 1, 2017, from http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union,* L119, 59, 1-88. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

FTC (Federal Trade Commission) (2010). *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.* Retrieved September 23, 2015, from http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian,* 7/6/2013. Retrieved August 8, 2015, from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

ICDPPC (2016). *Artificial Intelligence, Robotics, Privacy and Data Protection.* International Conference of Data Protection and Privacy Commissioners.

ICO (Information Commissioner's Office) (2010). *The Business Case for Investing in Proactive Privacy Protection.* https://ico.org.uk/media/about-the-ico/documents/1042345/privacy-dividend.pdf

ICO (Information Commissioner's Office) (2017). *Big data, artificial intelligence, machine learning and data protection.* Version: 2.2.

INTECO (2012). *Estudio sobre la protección de datos en las empresas españolas.* Instituto Nacional de Tecnologías de la Comunicación. León: INTECO.

Jentzsch, N., Preibusch, S., & Harasser, A. (2012). *Study on monetising privacy. An economic model for pricing personal information.* ENISA.

Johnson, G., & Scholes, K. (1997). *Dirección estratégica. Análisis de la estrategia de las organizaciones.* Madrid: Prentice-Hall.

Kroener, I., & Wright, D. (2014). A Strategy for Operationalizing Privacy by Design. *The Information Society,* 30(5), 355-365. https://doi.org/10.1080/01972243.2014.944730

London Economics (2010). *Study on the economic benefits of privacy enhancing technologies (PETs).* Final Report to the European Commission. Retrieved August 26, 2015, from http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

Majdalawieh, M. (2013). Building a Privacy Model in the Business Processes of the Enterprise: An Information Systems Design Science Research. *Eurasian Journal of Business and Management,* 1(1), 15-31.

OECD (Organization for Economic Co-operation and Development) (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Retrieved July 23, 2017, from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD (Organisation for Economic Co-operation and Development) (2013). *2013 OECD Privacy Guidelines.* Retrieved August 26, 2015, from http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

Perera, C., Ranjan, R., & Wang, L. (2015). End-to-End Privacy for Open Big Data Markets. *IEEE Cloud Computing,* 2(4), 44-53. https://doi.org/10.1109/MCC.2015.78

Ponemon Institute (2013). *2013 Cost of Data Breach Study: Global Analysis.* Retrieved July 3, 2017, from http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf

Ponemon Institute (2015). *2015 Cost of Data Breach Study: Global Analysis.* Retrieved July 7, 2017, from https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.pdf

PRIPARE (2013). *PReparing Industry to Privacy-by-design by supporting its Application in REsearch.* FP7-ICT-2013-1.5. European Project Report.

PRIPARE (2014). *State-of-play: Current Practices and Solutions.* European Commission. Seventh Framework Programme for Research, Technological Development and Demonstration Web prepare. European Project Report.

PwC (2013). *10Minutes on building a customer-centered organization.* Report.

PwC (2014). *17th Annual Global CEO Survey.* Report.

PwC (2014). *Achieving Total Retail.* Report.

PwC (2015a). *18th Annual Global CEO Survey.* Report.

PwC (2015b). *Analyse this: Are CEOs embracing the boom in personal data?* Report.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, Privacy, and Security Online.* Pew Internet Report. Retrieved June 19, 2016, from http://pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research,* 22(2), 254-268. https://doi.org/10.1287/isre.1090.0260

Witt, S. (2012). Integrated Privacy Modeling and Validation for Business Process Models. *Proceedings of the 2012 Joint EDBT/ICDT Workshops.* EDBT-ICDT 2012. ACM. https://doi.org/10.1145/2320765.2320821