Privacy Awareness in the GDPR Implementation Circumstances

Malgorzata Pankowska *pank@ue.katowice.pl*
University of Economics in Katowice
Katowice, Poland

Abstract

Acting in a professional and ethical manner encourages business units to ensure that actions to protect privacy are performed in a reliable, consistent, responsible and effective manner. Some business people say that privacy protection can be considered a source of competitive advantage. General Data Protection Regulation (GDPR) fosters a privacy-positive culture development to provide a positive privacy protection influence on the Internet users' behaviors. GDPR mostly focuses on a framework of activities of business organizations and does not emphasize the role of the Internet users, whose reputation and positive image are exposed. Therefore, the paper aims to discuss hazard tolerance and resilience in the context of privacy by design approach development. The survey on usage of mobile devices and web services is the basis for the discussion. The exemplar survey reveals students' resilience to new media impact on their privacy.

Keywords: GDPR, privacy, mobile devices, web services, business analysis.

1. Introduction

Promoting responsible behavior to protect the privacy of all individuals within a certain community has lately gained a lot of popularity, particularly because of the GDPR implementation in EU countries. Business organizations are involved in discussion and exchange of good practices on how to protect personal data of their customers. Mostly, they consider security as an ongoing process and privacy as a certain status of information protection respecting the appropriate principles. However, taking into account that privacy assurance can be realized by default and by design, there is still an open question on the method of systems development to ensure protection of personal information. In the course of system development as well as business architecture development a lot of work was done, however, it may be necessary to analyze personal attitudes of system users towards their privacy perception, risk and tolerance, as well as their resilience. So far, these issues were out of scope of the discussion on privacy impact assessment (PIA). Therefore, the goals of this paper cover the analysis of risk tolerance and resilience issue in the context of privacy protection and GDPR implementation. The first part of the paper includes discussion on privacy and resilience, good practices and principles of privacy protection. Next, PIA approach is presented and standards on privacy protection are compared. Third part includes the analysis of the survey results on privacy tolerance by students. Finally, recommendations for business analysis for systems development and conclusions are written. The paper is to emphasize that privacy considerations and control should be incorporated into system life cycle development.

2. Definitions of Privacy and Resilience

The GDPR is a comprehensive regulation that unifies data protection laws across all European Union (EU) countries. GDPR defines a set of rights for EU individuals regarding the protection of their personal data and it contains a set of requirements for business organizations on collecting, storage, processing and management of that data. According to Regulation EU

2016/679 of the European Parliament and of the Council of 27 April 2916 on the protection of natural persons with regard to the processing of personal data [21], personal data refers to any information relating to person, who can be identified, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Privacy within an enterprise comprises compliance with legal and regulatory requirements concerning data retention periods, cross-border regulations, and intellectual property. According to Clarke [10], privacy is the interest that individuals have in sustaining a personal space, which is free from interference by other people and organizations. The same opinion was formulated in 1890 by Brandeis and Warren [7]. Kandogan and Haber [19] argue that privacy is an ability of data subject to control the term under which the personal information is collected and used. Torra [28] emphasizes that privacy is a state of limited access to a person. A person has the right to determine the extent to which others have limited access to information about them. Graham [13] analyses physical and information privacy. The first one means an ability to maintain personal own physical space, but the second is the ability of a person to control, manage and delete information about themselves and to decide how and what information is revealed to others. According to GDPR, privacy is considered as a purely legal issue, and the responsibility for it is to be ensured by the business organization and organizational legal counsel. Beyond that, the security is to be ensured and it is perceived as a technical issue. The responsibility for security is placed within the information technology and networking support area.

D'Acquisto et al. [11] specify three categories of privacy:

- respondents' privacy, e.g., the hospital has to implement patients' privacy protection mechanisms;
- holder's privacy, e.g., supermarkets analyze the loyalty of their customers;
- user's privacy, i.e., privacy of the user of a particular system.

Schoeman [22] emphasizes an issue which is important for this paper, arguing that privacy can be seen as a culturally conditioned sensitivity that makes people more vulnerable than they would otherwise be to selective disclosures.

There is always the question of what kind of information can be available to others. Freedom of the Internet usage encourages to ask the question of whether privacy is a desirable state and how valuable it is in relation to other things. For example, a person has diminished their privacy without any infringement any time they reveals something about themselves. Taking into account this paper goals, Schoeman's arguments are valuable, which are as follows [22]:

- privacy relates to the intimate and subtle aspects of a person's life and relations between people;
- privacy involves the acceptance of a person’s discretion to decide when and to what extent inner feelings and attributes are to be explored;
- certain kinds of affronts to a person's sensibilities can be seen as an intrusion into their privacy.

Revealing their personal behavior, people reveal an acceptance for that. Clarke [10] identifies the following dimensions of privacy:

- privacy of the person, which concerns the integrity of an individual's body and their health;
- privacy of personal behavior, for example in the usage of various media, no monitoring of the individual communication by other persons or organizations;
- privacy of personal data, so when data is collected and processed, the data subject is able to control the data possessed by data processor.

In general, people are interested in controlling the management of data about themselves. Therefore, because of conflicts of interests in a business organization or in a business process, the privacy protection is a process of finding appropriate balances between privacy and multiple interests of organization stakeholders. Data includes symbols, signs and measures, while information is the use of data by humans to extract a meaning and to support decision making. In business, particularly for marketing, data surveillance as the systematic use of personal data system in an investigation or monitoring of the actions or communications of people is extremely useful for staying in the market.

Privacy, with respect to personal data (i.e., personally identifiable information (PII)) is a core value that should be obtained only with appropriate legislation, policies, procedures, and controls to ensure compliance with requirements. In the GDPR circumstances, protecting the privacy of individuals and their PII is a fundamental responsibility of business organizations. According to NIST Special Publication [23], privacy covers each individual's right to decide when and whether to share personal information, how much information to share, and the particular conditions under which that information can be shared. In general, resilience is known as a physical property of a material by which it can return to its original shape or position after a certain deformation that does not exceed its elastic limit [8]. In the context of personal information privacy the resilience concerns staying in business after revealing data. So the business organizations as well as individuals should answer the questions "How resilient am I?" or "Am I resilient enough?" and beyond measuring the current state, the prediction of how it will perform in the future when the risk environment changes is also important. For managing operational resilience, the management activities for security and privacy protection, assurance of business continuity and IT operations are continuous practices. Management of resilience usually concerns business organizations, however also individuals can ask themselves "How am I resilient?" , "What should I do to increase my resilience?" and "What should I reduce to protect my privacy?".

In the context of this paper, the basic question is how resilient you are to Internet applications and social media impact on your privacy. According to Sheffi [25] an investment in resilience and risk management may be considered as conservative and risk-avoidance initiative, but they enable business units to be less risk averse. In this paper, resilience is an internal capability aligned with the people. It can bring competitive advantage, because it helps in competition by increasing the organizational vigilance, responsiveness, and flexibility to detect and respond to unexpected events quickly and effectively. Organizations as well as individuals are more resilient than competitors, when they better predict disruptions, they are more effective at mitigating impacts and faster at achieving post-disruption recovery. The problem is that standards, legal regulations and following them guidelines focus on organizational resilience. According to NIST Special Publication [23], resilience is the system ability to operate under adverse conditions and recover to an effective operational posture. ASIS International Standard [2]defines organizational resilience as the adaptive capacity in a complex and changing environment. In this paper, resilience is not only the ability of an organization to resist being affected by an event, but it is also a capability of individual and that characteristics should be taken into account in the process of information system design, particularly at the business analysis and requirement management stage.

3. Privacy Standards and Principles Wide Spectrum

Compliance and data protection compliance practitioners are nowadays extremely involved in monitoring and harmonizing specific GDPR requirements within different regulations frameworks. Privacy protection is to be included in general business governance planning and risk management activities. Identification of privacy impact, privacy risks and responsibilities is supported by the International Standard ISO/IEC 29134: 2017 [17]. This standard is for the privacy impact analysis process, but controls of the risk treatment are included in ISO/IEC 27002 and ISO/IEC 29151. According to the ISO/IEC 29134:2017 Standard, privacy impact assessment is an overall process of the identification, analysis, evaluation, consultation, communication and planning the treatment of potential privacy impacts on processing personally identifiable information. There are two basic functions of privacy impact assessment (PIA), i.e., informing the stakeholders about identified affected entities, affected environment and privacy risks, and tracking the actions and tasks that improve and resolve the identified privacy risks. According to Tancock et al.[26], PIA is oriented towards meeting legal requirements. It should be prospective, cost effective, trustful, and informing decision makers and stakeholders about information processing. Mapping of personal information flows is emphasized in the approach to PIA in Australia [3] and in Canada [29]. In Australia, PIA covers the description of the project of personal information processing, mapping the information flows, identification and analysis of how the project influences personal information processing, considering alternative processing options, and reporting. In Canada, similarly, there is at first the conceptual analysis of the scope and business rationale of a planned initiative of information processing, registration data flow analysis in form of business process diagrams, review design options, and conducting a privacy and risk analysis of any changes to the proposed initiative, designing to ensure compliance with privacy legislation. Privacy impact assessment as well as privacy protection are based on verified practices and emphasize the respect of certain selected principles. Hoepman [15][16] proposed a privacy-by-design (PbD) approach to protect privacy in the process of technological development. In this approach, privacy protection is to determine the design and implementation of information systems.

However, GDPR principles do not emphasize the role of data subjects in privacy protection activities. These principles are as follows [21]:

- Data controllers or processors should describe the personal data collecting choices and they should be available to the data subjects. The data processors/controllers should obtain appropriate consents on personal data processing;
- The legitimate purpose of data use should be specified, as well as limitation of use should be respected;
- Data controllers/ processors should minimize the data collection and process the data only for the specified and documented purposes;
- The personal data should be corrected when necessary, including date, time, and name of who made the change;
- Logs and lists of all corrections to personal data should be documented;
- Data subjects should be able to correct data, when necessary;
- Data controllers/processors are generally required to provide clear, accessible and accurate details about their privacy management program;
- Data subjects are allowed to withdraw consent to use their personal data;
- Data subjects can receive information regarding the purposes, categories, and recipients of their data, retention periods, rights for deletion and making complaints;
- Privacy policies and supportive procedures are necessary to establish the requirements for the data protection officer's responsibilities and the actions for which the data protection officer is responsible;
- Sensitivity policies and supporting procedures are needed to ensure that information has appropriate safeguards;
- Regular privacy and security trainings are ensured to the data processing staff;
- Harm prevention policies and procedures are needed to ensure lawfulness of personal data processing;
- Implemented management policies and procedures ensure that enterprise does not use third party processors unless they provide sufficient guarantees and verified proof that they have implemented appropriate technical measures to support the data subject's rights;
- Breach policies and procedures are needed to include requirements for notifying appropriate supervisory authorities of the breach in a timely manner;
- The security and privacy protection mechanisms should be built into the full life cycle of automated personal data based decision making;
- Risk management policies and procedures are necessary and implemented to ensure business continuity;
- Transfer of data to a third country can be realized only in certain circumstances with respect to data subject's rights and legal remedies.

Taking into account the listed above principles as well as those included in Table 1, the active role of end users, i.e., data subjects has been noticed in the privacy protection activities. The principles do not emphasize the data subjects' personal attitudes and opinions on privacy protection behaviors.

Table 1. Privacy protection principles.

ISACA Privacy	GDPR	ISO 29100:2011	Cobit 5	HIPAA
Legitimate purpose specification and use limitation	Legitimate purpose and automated decision making	Purpose, legitimacy and specification, the use, retention and disclosure limitation	Manage availability and capacity, change acceptance	Procedures for access, disclosure and integrity, ongoing privacy trainings
Personal information and sensitive information life cycle	Privacy by design, PIAs, data subject participation and safeguards	Collection limitation and data minimization	Manage knowledge, assets, and configuration	Inventory of assets, policies, procedures, training and technical control
Accuracy and quality	Data rectification & data quality	Accuracy and quality	Manage quality , manage innovation,	Authorized individuals access rights
Openness, transparency and notice	Transparency and data subject rights	Openness, transparency and access	Ensure stakeholder transparency, manage service agreements,	Controlling of sharing employment, application, utilization, understanding the current use
Individual participation	Data subject access	Individual participation and access	Access and correction	Procedures for policy processing purposes, respecting subject rights
Accountability	Data processing, data protection officers and controllers	Accountability	Accountability, manage operations, service requests and incidents, problems, continuity , manage budget and costs	Identification of disclosures, enforcement sanctions for policy non-compliance
Security safeguards	Security safeguards through data lifecycle	Information security	Manage security services, manage portfolio	Practices for protecting of information, implementing administrative, technical, physical safeguards
Monitoring, measuring, and reporting	Processing, right to be forgotten & data portability records/reports	Privacy compliance	Manage business process controls, monitor, evaluate and assess performance and conformance, monitor	Addressing compliance , security review actions ,
Preventing harm	Lawfulness, data subject access, portability, PIA, risk management	n/a	Ensure risk optimization, risk management, assess compliance	Identification of potential risks, use of security software, i.e., antivirus software
Third party/ vendor management	Processors management	n/a	Manage relationships, manage suppliers,	Identification of third parties and information exchange with them
Security and privacy by design	Controller responsibilities, automated decision-making and data protection by default	n/a	IT management framework, manage knowledge, requirements, projects, and enterprise architecture	Documenting the overall architecture
Free flow of information and legitimate restriction	Data subject rights, lawfulness, data transfers, binding corporate rules	n/a	Ensure governance framework setting and maintenance	Identification of information systems, current procedures of information sharing

The presented in Table 1 principles have been gathered from different sources, i.e., [1], [5], [14], [18], [21], [23], [28]. A data subject is emphasized to have the right of access to personal data in order to be aware of and verify the lawfulness of the processing. In above documents, data subject profiling means any form of automated processing of personal data to evaluate and predict person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Data subject should have the right to object to processing the data for marketing purposes, particularly for customer profiling. The presented in Table 1 Cobit 5 business framework as well as Health Insurance Portability and

Accountability Act (HIPAA) are supplementary to GDPR regulations. Cobit 5 processes are argued to be helpful for assurance of stakeholder transparency, for management of IT, business strategy, enterprise architecture, suppliers, programs and projects, as well as for management requirements, solutions, capacity, knowledge and changes. As in the EU, where GDPR is to be effective as of 25 May 2018, in USA, the HIPAA, the Patriot Act, and the Homeland Security Act are the most relevant laws [28]. HIPAA aims to protect the rights of consumers by providing them access to their health information. In this way that legal act is to improve quality, efficiency and effectiveness of healthcare in the USA [5].

In this paper it is assumed that to support privacy by design, guiding principles are needed to focus on the user requirements in the system development life cycle, particularly in the concept development stage, as well as during analysis, design and implementation. High level analysis, i.e., business analysis in opposition to system analysis is expected to focus on users. Therefore, the users' attitudes, their behaviors, lifestyles are significant for privacy protection assurance. Many user-centric methods for information system development should be reviewed in the aspect of their applicability for recognition of user profiles and registration of their attitudes towards personal information protection. Reviewing the user-centric methods can be useful not only for information system design and implementation, but also for teaching users how to behave and work with Internet applications, when their personal information is required for accessing a web portal. Unfortunately, presented in Table 1 standards and regulations on privacy protection assume that just business unit is responsible for privacy protection assurance and they do not consider individuals' perception of privacy.

4. Survey on Privacy Awareness

Assuming that according to ISO 29100:2011 [18] privacy protection management requires privacy risk assessment, privacy audit, PIA and privacy self-assessment, in this paper the student opinion survey results are presented and discussed. Although according to the ISO 29100:2011 standard, the self-assessment is oriented towards review of the practices and procedures realized at the enterprise, which is responsible for continuous compliance assurance, the proposed in this paper self-assessment could be adjunctive to proactive privacy management, as well as to appropriate secure information system design, best practices development and continuous training for data subjects. Williams and Nurse [31] have noticed the Privacy Paradox, which according to them means that individuals are assumed to argue about the value of privacy, but they are said to do little to actively protect it. Williams and Nurse argue that people freely disclose their personal information and they are upset when their privacy is infringed. So, the researchers formulated the opinion about a bounded rationality situation and they believe that people reveal their data looking for short-term benefits without considering the long term privacy risks [31]. Williams and Nurse [31] have realized a survey of UK adult population on privacy perception. For the survey they have chosen people in big cities, i.e., London, Birminghan, Cardiff, and Oxford. They collected a total of 112 responses. The gender ratio was rather balanced at 57% female and 43% male. The results of similar investigation done in Poland in 2018 are included in this paper (Table 3). The questionnaires were distributed among university students, age 19-30. Eventually, 160 responses were collected, 39% female and 61% male. In comparison with the research done by Williams and Nurse [31], the question set was extended and some new questions concerning Web services were added. However, before this essential survey, the context for privacy explanation was surveyed. Context consideration seems to be important in domains such as decision making, analysis, design, negotiations or learning. In general, context is argued to have an infinite dimension and cannot be described completely. The adaptation of mobile devices and new media to the university learning processes enriches a context of use of information and knowledge. For evaluation of the privacy controlling and resilience of data subjects, simply the usage of mobile devices is a context for further privacy awareness consideration. The context of work in contemporary learning system includes:

- people, i.e., students, teachers, and the university learning and communication processes;

- platforms used to interact in the learning processes, i.e., Moodle, Blackboard, Google Classroom;
- new media, mobile applications and electronic libraries necessary in learning and communications at universities;
- mobile devices and hardware necessary in the educational processes;
- physical environment, where the interaction takes place.

Table 2. Technologies and mobile devices used by students.

Mobile device & technology	**2013 n=114**	**2014 n=127**	**2015 n=114**	**2018 n=160**
stationary phone	2	4	2	29
mobile phone	31	42	45	82
smartphone	26	64	61	144
iPod	3	2	0	6
iPad	5	6	3	8
notebook	67	68	66	93
netbook	20	25	20	22
desktop computer	43	56	55	109
tablet	10	14	22	43
GPS device	1	4	7	68
RFID device	0	1	5	8
automatic personal identification device	2	1	2	27
biometric personal identification device	2	1	1	20

In general, the research on mobile devices usage at an university has been realized for a few last years, i.e., 2013-2018 and it is expected to be continued in future. Successfully, students accepted the survey as important for the evaluation of their competencies to use mobile devices in learning processes as well as in other activities, i.e., professional work, social relationship development, or in healthcare. The questions in survey concerned the issue of what devices and technologies are used by students. The percentages of positive answers are included in Table 2 and in Figure 1. Numbers of students, who provided responses, are included at the top of the Table 2.

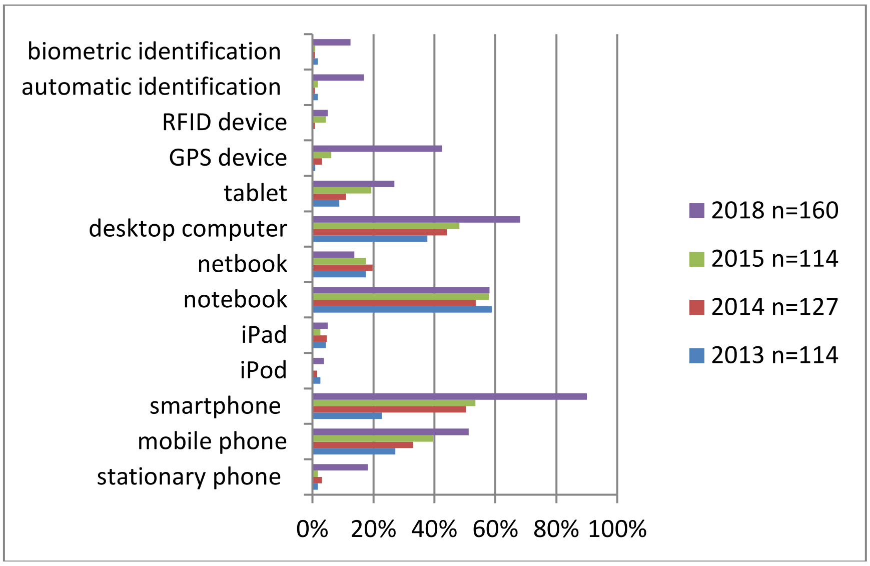

Fig. 1. Technologies and mobile devices used by students.

Table 3. Students opinion on web services.

	Research questions: How often do you :	**several times a day**	**once a day**	**sometimes**	**by chance**	**never**
1	clear your Internet browser's history	4%	4%	**62%**	13%	16%
2	use Internet browser plug-ins/extensions to protect your privacy?	29%	4%	**37%**	8%	23%
3	encrypt data on your computer?	8%	6%	34%	15%	**37%**
4	store unencrypted data (e.g., photos) within a cloud provider such as Dropbox?	3%	6%	28%	11%	**53%**
5	share your photos on Facebook?	4%	0%	**50%**	26%	20%
6	share on Facebook photos interesting for you?	1%	1%	**38%**	26%	34%
7	share on Facebook photos important for you?	0%	1%	32%	23%	**44%**
8	share on Facebook photos of historic/touristic attractions?	1%	0%	37%	21%	**41%**
9	share on Facebook photos of mass events?	0%	2%	**41%**	22%	36%
10	use Tor for your web browsing?	3%	3%	8%	11%	**75%**
11	use PrivBrowse for your web browsing?	4%	1%	11%	4%	**79%**
12	use encryption tools for your emails?	9%	5%	23%	9%	**54%**
13	read the terms and conditions on websites you use?	1%	3%	35%	24%	**37%**
14	share your personal data to register on web portal?	2%	3%	**68%**	21%	6%
15	check permissions before installing smartphone apps?	14%	11%	**44%**	17%	14%
16	remove cookies?	6%	8%	**55%**	18%	14%
17	install software from unknown sources?	4%	2%	**42%**	30%	23%
18	open unknown email address?	2%	3%	11%	19%	**65%**
19	open word attachments sent from unknown email address?	3%	3%	7%	8%	**80%**
20	check if the websites have green padlock?	**24%**	13%	31%	14%	19%
21	use antivirus software?	16%	25%	**44%**	7%	8%
22	leave your devices unmonitored in train, waiting room?	3%	1%	4%	11%	**81%**
23	use mobile phone in open space?	24%	10%	**58%**	6%	3%
24	use open source network in WiFi?	17%	6%	**45%**	13%	19%

Taking into account the answers, a rapid increase of smartphones usage (90% of student population in 2018) is noticed. Beyond that, GPS devices, biometric identification tools, and automatic identification are more and more popular. However, students still use desktop computers for learning, because they are quite comfortable and compatible with mobile devices, i.e., tablets, smartphones.

Devices, i.e., iPods, iPads and netbooks soon will disappear from the usage and from the markets as their functionalities will have been taken over by other devices. Small usage of RFID devices can be explained by lack of knowledge about that solution. People are not aware that they use them often in public, e.g., in supermarkets. The second part of the survey includes questions similar to that presented by Williams and Nurse [31]. Although the results are a little bit similar, the interpretation is distinctive. This survey results on students' attitudes towards privacy are included in Table 3. 62% of students admitted that they clear Internet browser's history (according to Williams and Nurse survey only 26%). It is very positive that 53% students reject the usage of open cloud, e.g., Dropbox (44% in Williams and Nurse survey).

Possibly at universities archived information is not so sensitive as it is in banks or hospitals, however, teachers and students know to avoid open clouds as unsecured. Facebook is still a very popular social network and 50% students admit they use it to share their photos as well as photos from mass events. Tor and PrivBrowse software applications are mostly unknown and for 10th and 11the question the same results were achieved by Williams and Nurse [31]. Taking into account the 3rd and 12th question, students rather do not encrypt data on their computers nor use encryption tools for their emails. 37% students do not read terms and conditions on websites they use and a similar result (i.e., 40%) was noted on Williams and Nurse survey [31]. 68% students admit they share their personal data to register on a web portal. The problem is that they are forced to register, otherwise the services provided by this portal will not be available. Most business portals do not permit to use "opt-out" solution, which would allow access to web services without prior registration.. Students sometimes check permissions before installing smartphone applications, remove cookies and install software from unknown sources. It is a very positive behavior that they never open emails from unknown addresses (due to threats of ransomware) and they check the green padlock (i.e., secure connection protocol) before shopping online. They perceive antivirus software as not very necessary. 87% students admit they never leave their devices unattended, although they fulfill their desire to use the mobile devices in public space. In general, they are conscious with regard to using Internet applications and mobile devices in open space and use them quite reasonably. It can be a result of their personal experiences, peer-to-peer knowledge sharing and self-learning, because university courses do not cover evaluations of open cloud software, nor information about safeguards against ransomware or other Internet threats. Students seem to have their own attitude towards privacy protection. They want to use mobile devices and mass media, but they try to reveal and get the information which is worthwhile for them.

5. Usability of Survey Results

Taking into account the cost of reasonable implementation of privacy protection processes and privacy risk management as well as the rights and freedom of persons posed by personal data processing there is a need to implement appropriate technical and organizational measures, which are designed with respect to data protection principles. Privacy by design can be considered as an approach to IS development that promotes privacy and data protection compliance in the whole system life cycle. Privacy by design can focus on potential problems that are identified at the early stages of business analysis and increased awareness of privacy and data protection across a business organization. Privacy by design as a concept developed by Cavoukian concerns the future of privacy [9]. According to her, privacy should be conformed to the social organization's mode of operation. Privacy by design concerns information systems, accountable business practices and network infrastructure. In this paper, the concept of privacy by design is suggested to be extended and include also social contexts, habits, preferences, resilience and privacy risk tolerance.

Privacy by design can be thought as a certain strategy of including privacy protection in information systems and enterprise architecture development. This approach requires developing sophisticated methods' for its development. The discussion should start at the business analysis stage, which seems to be the first significant stage for information systems design and implementation. Business analysis methodology development is strongly supported by the International Institute of Business Analysis (IIBA) [4]. Therefore, business analysis is understood as the practice of enabling change in an enterprise by defining needs and recommending solutions that deliver value to stakeholders. Babok v.3 Guide [4] proposes to conduct this analysis from different perspectives: agile, business intelligence, information technology, business architecture, and business process management. Babok v.3 Guide emphasizes communication with stakeholders and Requirements Life Cycle Management (RLCM). The business analysis scope should include description of the key stakeholders, including at first profiles of sponsors, the target stakeholders, and the business analysts' roles within the project. Stakeholders are defined in terms of their interest in, impact on, and influence over the change. They are identified and recognized by their needs, changes and solutions, unfortunately their competences, habits and customs are not discussed. These issues are included in the characterization of the project context, which may include attitudes, behaviors, beliefs, culture, demographics, goals, language, computerized infrastructure, processes, products, technology, and even weather. In the aspect of privacy protection, the project stakeholders can be considered as data subjects. Stakeholder analysis involves the identification of stakeholders and their characteristics. This analysis is repeated as other business analysis activities are performed. Techniques used for the recognition of stakeholders' community are as follows:

- brainstorming used to produce the stakeholders' list and to identify their roles and responsibilities;
- business rules' analysis to recognize who is a business rules' developer;
- document analysis to support planning the stakeholders' engagement;
- interviews with stakeholders;
- previous experiences gathered from stakeholders;
- mindmapping to understand relationships between stakeholders;
- organizational modeling to determine the roles and functions of stakeholders;
- process modeling to categorize stakeholders by systems and processes,
- risk analysis and management;
- survey, questionnaires and workshops for interaction with groups of stakeholders.

In the context of privacy protection, the surveys and questionnaires seem to be necessary to reveal the users' attitude towards privacy. Managing the collaboration with stakeholders is an ongoing activity. Their roles, responsibilities, influence, attitudes and authorities should be evaluated and monitored over time. The monitoring could have an impact on better recognition of their needs and better business - information technology alignment (BITA). Otherwise some detrimental and less optimal effects can arrive. The weaknesses include failure to provide quality information or ensure suitable security, resistance to change and needless expenditures on information systems.

The most easily understood tasks in any system design is to define the system functional requirements. Secondary are nonfunctional requirements, e.g., safety, security, privacy. The software tools and languages support functional requirement engineering (e.g., UML language), however, SysML language includes also the possibilities for nonfunctional requirements modeling. In SysML language, you can specify functional, interface an performance requirements to be included in Requirement Diagram. In general, nonfunctional requirements are subjective and relative [20]. They are subject-oriented, so they are specified, interpreted and evaluated differently by different stakeholders. Nonfunctional requirements are relative, so they depend not only on users, but also on the systems where they are implemented [20]. Stakeholders, particularly end users are assumed to present a need or a solution for information systems development, therefore their engagement is to be planned. Lately developed user-directed information system methodologies, i.e., Participatory Design [27], User Experience Design [30], User Centered Development Process [12], Persona Development [6], User Centric Management [24] aim at fulfilling individual users' needs quickly and efficiently. Their strategy is to actively co-create values in collaboration with system providers.

6. Conclusion

Recognition of stakeholders' characteristics in the process of usage of mass media, mobile devices, and Web services could be useful for information system modeling and as such could be realized at the first stage of the system life cycle. Business analysis itself should allow to recognize the system target market and avoid redundant expenditures in system design. The business analysis should concentrate not only on functional requirements management, but also on nonfunctional requirements. The applied methods can cover interviews, questionnaires, collecting user experiences and realization of workshops, just to learn the user community by the system analysts. Taking into account the presented above standards and regulations, it should be noticed that in different countries and business units their interpretation can be different, however, beyond them in information system development process, also personal attitude of individuals should be considered. In the future, further survey will be distributed in other countries, just to evaluate culture impact on privacy perception. Beyond that, there is still hypothetical question that people are more and more tolerant of privacy protection.

References

1. Adopting GDPR Using COBIT 5 (2017), ISACA, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Adopting-GDPR-Using-COBIT-5.aspx. Accessed March 15, 2018
2. ASIS International, ASIS SPC.1-2009, American National Standards Institute, Inc. "Organizational Resilience: Security, Preparedness, and Continuity Management Systems - Requirements with Guidance for Use." (2009), https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf. Accessed June 22, 2018
3. Australian Government: Office of the Privacy Commissioner. “Privacy Impact Assessment Guide.” (2006), http://www.privacy.gov.au/ materials/types/download/ 9349/6590. Accessed October 30, 2009
4. Babok v.3. A Guide to the Business Analysis Body of Knowledge, IIBA, International Institute of Business Analysis, Toronto, Ontario, Canada (2015), http://www.innovativeprojectguide.com/documents/BABOK_Guide_v3_Member.pdf. Accessed March 31, 2018
5. Beaver, K., Harold R.: The Practical Guide to HIPAA Privacy and Security Compliance. Auerbach Publications, Washington (2004)
6. Bill, A., Tullis T., Tedesco, D.: Beyond the usability Lab, Conducting Large-scale Online User Experience Studies. Morgan Kaufmann Publishers Elsevier, Amsterdam (2010)
7. Brandeis, L.D., Warren, S.D.: The Right to Privacy, Harvard Law Review, Vol.4., No.5. (1890), pp. 193-220, http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Accessed March 30, 2018
8. Caralli, R.A., Allen, J.H., White, D.A.: A Maturity Model for Managing Operational Resilience. Addison-Wesley, Upper Saddle River, NJ (2010)
9. Cavoukian, A.: Privacy by design. The 7 foundational principles in Privacy by Design.Strong privacy protection—now, and well into the future (2011). https://www.ipc.on.ca/wp-ontent/uploads/Resources/7foundationalprinciples.pdf. Accessed March 17, 2018
10. Clarke, R.: Introduction to Dataveillance and Information Privacy, and Definitions of terms (2006), http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html. Accessed March 20, 2018
11. D’Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.-A., Bourka, A.: Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics, ENISA Report (2015) https://arxiv.org/ftp/arxiv/papers/1512/1512.06000.pdf. Accessed March 30, 2018
12. Goncalves, J., Santos, C.: POLVO- Software for Prototyping of Low-Fidelity Interfaces in Agile Development. In: Jacko, J.A. (ed.) Human-Computer Interaction, Design and Development Approaches, pp.63-71. Springer-Verlag, Berlin, Heildeberg, (2011)
13. Graham, Ch.: Conducting privacy impact assessments, code of practice, Information Commissioner's Office (2014), https://ico.org.uk/media/for-organisations/documents /1595/pia-code-of-practice.pdf. Accessed March 15, 2018
14. Harold, R.: Using ISACA's Privacy Principles to Create an Effective Privacy Program, Data Privacy Asia, Singapore (2013), https://www.cpomagazine.com/wp-

content/uploads/2017/04/Using-ISACAs-Privacy-Principles-to-Create-and-Effective-Privacy-Program.pdf. Accessed March 30, 2018

15. Hoepman, J-H.: Privacy Design Strategies (2012), https://www.cs.ru.nl/~jhh/publications/pdp.pdf. Accessed March 29, 2018
16. Hoepman, J.-H.: Privacy design strategies. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds.) ICT Systems Security and Privacy Protection, pp.446-459. Springer, Heidelberg (2014)
17. International Standard ISO/IEC 29134: 2017, Information Technology - Security techniques - Guidelines for privacy impact assessment (2017), ISO, Geneva
18. International Standard ISO/IEC 29100: 2011, Information technology- Security techniques - Privacy framework (2011), ISO, Geneva, http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. Accessed March 15, 2018
19. Kandogan, E., Haber, E.M.: Security Administration Tools and Practices. In: Cranor, L.F., Garfinkel, S. (eds.) Security and Usability, Designing Secure Systems That People Can Use, pp. 357-379, O'Reilly, Beijing (2005)
20. MacG Adams, K.: Nonfunctional Requirements in System Analysis and Design. Springer, Cham (2015)
21. Regulation (EU) 2016 of the European Parliament and of the Council of 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 (2016), European Parliament and the Council of the European Union, http://data.consilium.europa.eu/doc/ document/ST-5419-2016-INIT/en/pdf. Accessed March 30, 2018
22. Schoeman, F.: Privacy Philosophical dimensions of the literature. In: Schoeman, F.D. (ed) Philosophical Dimensions of Privacy: An Anthology, pp.1-34. Cambridge University Press, Cambridge (1984)
23. Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53A, Revision 4, December 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf. Accessed March 30, 2018
24. Shapiro, A.: Users not Customers. Penquin Books Ltd. London (2011)
25. Sheffi, Y.: The power of resilience, How the Best Companies Manage the Unexpected. The MIT Press, Cambridge (2015)
26. Tancock, D., Pearson S., Charlesworth A.: The Emergence of Privacy Impact Assessments (2010), http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf. Accessed March 10, 2018
27. Torpel, B., Voss, A., Hartswood, M., Procter, R.: Participatory Design: Issues and Approaches in Dynamic Constallations of Use, Design and Research. In: Voss, A., Hartswood, M., Procter, R., Rouncefield, M., Slack, R.S., Buscher, M. (eds.), Configuring User-Designer Relations, pp.13-30. Springer Verlag, London (2009)
28. Torra, V.: Data Privacy: Foundations, New Developments and the Big Data Challenge. Springer, Cham (2017)
29. Treasury Board of Canada Secretariat. “Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks.” (2009), http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipgpefrld1-eng.asp. Accessed November 19, 2009
30. Unger, R., Chandler, C.: A Project Guide to UX Design For User Experience designers in the field or in the making. Peachpit Press, Berkeley (2009)
31. Williams, M., Nurse, J.R.C.: Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective. In: Tryfonas, T. (ed.) Human Aspects of Information Security, Privacy, and Trust, pp. 186-197. Springer, Cham Switzerland (2016)