Privacy Principles: Towards a Common Privacy Audit Methodology

Eleni-Laskarina Makri(✉) and Costas Lambrinoudakis

Department of Digital Systems, University of Piraeus, 18532 Piraeus, Greece
{elmak, clam}@unipi.gr

Abstract. A lot of privacy principles have been proposed in the literature with the aim to preserve users' privacy through the protection of the personal data collected by service providers. Despite the fact that there were remarkable efforts to gather all privacy principles and use them on a common privacy-by-design system, to the best of our knowledge, there is no published methodology that combines in a clear and structured way the existing privacy principles for supporting the design of a Privacy Preserving System. The absence of a widely accepted structured representation of the privacy principles makes their adoption or/and satisfaction difficult and in some cases inconsistent. Considering that privacy protection on its own is not an easy task for an organisation, the "scattered" privacy principles impose significant additional complexity. Consequently, very frequently organizations fail to effectively protect the privacy of their users. In this paper a structured privacy audit methodology that consists of discrete steps that organizations can follow for deciding or/and auditing the privacy protection measures is proposed. Every step is based on the significance of a privacy principle and on the sequence of the audit procedure.

Keywords: Privacy audit methodology · Privacy principles · Privacy protection

1 Introduction

Throughout the last decades the use of Internet has dramatically increased. More and more people use the Internet and its services on a daily basis in order to be informed, educated, entertained, etc. In order to utilize the online services, users reveal their personal information without considering, or just being unaware, of the consequences. As a result, very frequently the privacy of the users is violated since their personal data can be accessed by merely everyone and practically in every way. The meaning of *Internet Privacy* includes the way personal data are used, stored, processed, exploited from third parties etc. It targets to the protection of users against unwanted disclosure of their personal information.

One of the main user concerns is the absence of a privacy audit methodology and thus the uncertainty of whether the service providers protect their personal information adequately or not. On top of that the absence of a privacy audit methodology affects the service providers since they cannot be assured about the completeness and

S. Fischer-Hübner et al. (Eds.): TrustBus 2015, LNCS 9264, pp. 219–234, 2015.
DOI: 10.1007/978-3-319-22906-5_17

effectiveness of the privacy protection measures that they have adopted. In consequence, users' personal data is exposed to many different risks. Having a privacy audit methodology in place, helps users to trust service providers more and consequently use the offered services more.

Even though some steps have been taken towards a common privacy framework, only very few attempts have been made towards a structured privacy audit procedure. Such a procedure is proposed in this paper. To this direction, all privacy principles and requirements have been collected and classified in order to identify: (a) the way each privacy requirement can be satisfied and (b) the priority – sequence with which each privacy requirement should be addressed.

The rest of the paper is organized as follows: Sect. 2 provides an overview of the literature on the privacy principles used by public and private bodies. Based on the literature review, Sect. 3 presents the privacy principles that are the most widely accepted by the scientific community. Section 4 proposes a structured privacy audit procedure that can be followed by an organization to ensure the protection of users' privacy. Section 5 draws the conclusions giving some pointers for future work.

2 Literature Review

A lot of research effort has been invested in developing ways for protecting users' personal data. On one hand, many laws and directives, concerning users' privacy protection, exist in several countries, imposing to organizations that store personal data not to use them without first informing the users and obtaining their consent. On the other hand, there are a lot of public or/and private bodies, which are interested in protecting users' privacy and for that reason have published several privacy principles. At the same time, Privacy Enhancing Technologies (PETs), a variety of ICT measures that protect informational privacy by offering the technical means to protect user's personal data and thus to prevent unnecessary or unwanted processing, are utilised [9, 23]. Yet, both privacy principles and PETs cannot stand alone but are correlated and work on a supplementary basis.

It is many years ago that the protection of users' privacy became a concern and plenty of privacy principles have been established in order to avoid disclosure of personal data. Since 1980 [16], the OECD organization has defined a common privacy framework, which includes the most widely used privacy principles. The eight privacy principles, proposed in the '80 s, are still being utilised on the basis of privacy protection. Eminent scientists, such as Ann Cavoukian and her team [23] have relied on them to conduct their research and many organizations have applied them in order to ensure privacy protection.

These privacy principles have inspired a number of privacy legislations. In 1995, the European Commission (EC) introduced the Data Protection Directive (Directive 95/46/EC) [6, 7] in order to reinforce the data protection laws, aiming at the protection of individuals with regard to the processing of personal data and on the free movement of such data [6]. The OECD Privacy Principles (1980) and the Directive 95/46/EC (1995) were among the first serious attempts to protect users' privacy by imposing limitation to the ways that an organization can collect, store and process personal data.

In March 1996 [5], the National Standard of Canada “Model Code for the Protection of Personal Information” was developed based on the OECD Guidelines. Two extra privacy principles (consent and challenging compliance) have appeared for reinforcing the protection of personal information. In addition, the United States Department of Commerce developed Safe Harbor [19], a legal framework that allowed US organizations to comply with the EC Data Protection Directive [16]. Safe Harbor included privacy principles that have been based on the ones defined by OECD (1980).

Along with the privacy laws, directives and standards, there are certain organizations that try to support users’ privacy protection. Based on the OECD Privacy Principles (1980), ISACA published the ISACA/OECD privacy principles, in 2009 [22]. Furthermore, ISACA proposed a list of sample privacy controls to protect and maintain the privacy of users’ personal data. Other organizations such as ENISA [17] or IBM [11] have also taken steps towards privacy protection proposing appropriate mechanisms.

In 2011 [12], the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), provided a privacy framework based on eleven privacy principles that were the existing principles developed by a number of states, countries and international organizations. According to ISO/IEC 29100:2011, privacy principles should be used to guide the design, development, and implementation of privacy policies and privacy controls.

Over the years, the technological environment on which the privacy principles were applied has undergone significant changes, the most important of which were in the volume of personal data being collected, stored and processed. Furthermore, personal data are gradually becoming globally available while at the same time there are many more privacy threats. As such, for the existing more demanding technological environments, new privacy protection measures were necessary. The need to update the European Directive 95/46/EC led the European Commission to propose a major reform of the EU legal framework on the protection of personal data, in 2014 [8]. The new proposals reinforced the users’ rights and at the same time dealt with the challenges of globalization and new technologies [18]. For the same reasons, in 2013 [21] OECD proposed supplementary privacy principles, adding eight more principles.

In parallel, there are several individual efforts from several countries and other public or private bodies. In November 2006, Ann Cavoukian [1], proposed the Global Privacy Standard (GPS), the aim of which was to create a common global privacy framework for the global protection of users’ privacy. The GPS included ten privacy principles, which were derived from collective knowledge and practical wisdom of the international data protection community and was, therefore, the first team work towards a universal privacy framework.

Nowadays, privacy is a serious concern for both users and organizations. For this reason, many researchers support that privacy should be maintained throughout the entire lifecycle of an IT system. In other words, privacy should be considered from the design phase of an IT system until the end of its entire lifecycle. The notion of privacy-by-design as the philosophy for protecting privacy throughout the technological development process, from the conception of a new system up to its implementation, was strongly supported by Ann Cavoukian [4] and Jaap-Henk Hoepman [13, 14].

Despite the fact that there were remarkable efforts [1, 13, 14, 21] to gather all privacy principles and use them on a common privacy-by-design system, to the best of our knowledge there is no published methodology that combines the existing privacy principles for supporting the design of a Privacy Preserving System. One of the basic reasons for that is that the technological environment keeps changing all the time, something that makes it difficult for the organizations to adjust. Another possible reason is that the volume of information is huge and hardly manageable. Furthermore, the current information systems require global availability of personal data in order to operate. In addition, the threats in privacy have increased and organizations cannot catch up with them because of their rapid transformation. All the above are some of the most important reasons why current privacy principles are essential, yet somewhat outdated. Therefore, organizations are still failing to apply effective privacy protection mechanisms.

Furthermore, the literature review has revealed that so far there has been no attempt to provide a roadmap on how the existing privacy principles should be addressed (i.e. are some principles more important than others? is there a specific order that someone should try to satisfy them and in that case what is that order? etc.) for facilitating the design of systems that are indeed consistent with the privacy principles. Although there is extended literature about different privacy principles and their definitions [8, 12, 18, 21], there has been no reference as to which principle should be applied first, which should follow or which could be used as input to others.

The absence of a widely accepted structured representation of the privacy principles makes their adoption/satisfaction difficult and in some cases inconsistent. Considering that privacy protection on its own is not an easy task for an organisation, the “scattered” privacy principles impose significant additional complexity. Consequently, very frequently organizations fail to effectively implement the privacy principles and thus to protect users’ personal information. Now, more than ever before, the need for creating a structured roadmap for the fulfilment of privacy principles is absolutely necessary.

The aforementioned structured roadmap could be also capitalized as the basis of an auditing methodology for the use of PETs by an organization. The need for a common privacy audit methodology is not something new, since in 2004 a team of scientists [15] have highlighted its absence. Nevertheless, until today, no considerable effort has been made towards this direction.

3 Privacy Principles

The protection of users’ personal data and therefore their privacy is a fundamental human right. As mentioned in the previous section, many countries, as well as public and private bodies, have made significant effort to protect this right by defining privacy principles that should be followed by organizations that process personal data. The eight privacy principles, which were first defined in 1980 [16], were adopted by many countries and the public or private bodies. Despite the fact that some bodies have tried to expand them with additional privacy principles, the newly introduced principles have not been adopted yet, due to the lack of time to become widely accepted.

The most common and widely accepted privacy principles [10, 16] will be used in our research work to propose a structured privacy audit methodology.

- ***Purpose Specification Principle***: The personal data should be collected and used only for the specified purposes. The user should be notified for the reason his personal data is collected and used.
- ***Collection Limitation Principle***: The personal data should be collected with lawful and fair means. In this way, only the necessary data will be collected without redundant personal information. Also, the data collection should take place under the user's consent.
- ***Data Quality Principle***: The personal data should be accurate, complete and kept updated. The information quality should be maintained throughout the whole process of collection and use of personal data.
- ***Use, Retention and Disclosure Limitation Principle***: The personal data should be used only with the user's consent or under the authority of law. The use of personal data should be limited without disclosing or making it available for any reason other than the purpose of the collection.
- ***Security Safeguards Principle***: The personal data should be protected by applying security safeguards. In this way, the personal information will be protected from security and privacy threats.
- ***Openness Principle***: The practices, policies, processes and procedures concerning the users' personal data should be easily accessible and transparency should be maintained in every stage of its collection and use.
- ***Individual Participation Principle***: The owner of personal data should participate in the process of its collection and use. The user should have the right to intervene wherever necessary other than in the case where that it is prohibited by the law.
- ***Accountability Principle***: A data controller should be accountable for being in accordance with protection mechanisms which give effect to the above principles.

The above privacy principles are among the most widely adopted ones [10, 16] for the protection of personal information. As it was mentioned in the previous section, there are no better practices or guidelines or no such structured procedure for applying them either from the organization's perspective or from the user's perspective.

Some good practices and advices on how the privacy principles should be accounted during the design of a system can be found in blogs, fora and websites [20]. However, the information remains "scattered" and not yet official. It is therefore really difficult for both an organization and a user, to determine the effectiveness and consistency of the employed privacy protection mechanisms. The existence of a structured procedure can help the organizations apply the privacy principles and, at the same time, help the users to ensure that their personal information is secured. What is more, such a structured procedure can help Privacy Auditors to audit if privacy is effectively applied. Auditing is one of the most important processes in an organization, since it can affect its reputation either positively or negatively. As a consequence, it can either increase users' confidence or users' insecurity.

4 A Privacy Audit Methodology

4.1 From an Organization's Perspective

Towards the definition of a privacy audit methodology, the existing privacy principles have been classified in four levels based on their significance and on the sequence that the audit procedure should take place. Each level is associated with a "*Step*" of the audit procedure. All the steps should be followed in strict order since failure to audit any step automatically means that the remaining steps cannot be audited either, as all steps are interdependent.

The proposed methodology consists of four auditing steps. Each auditing step includes one or more privacy principles and is depicted in hierarchy. The auditing results of each privacy principle can be used as input for the auditing of some other privacy principle in the same or in the next step. The solid arrows between different steps symbolize the input from a privacy principle to another in the next auditing step. At the same time, it has been identified that there is need for certain privacy principles to be maintained throughout the entire auditing procedure.

STEP 1:

- **PRIVACY PRINCIPLE:** Purpose Specification **(PP-S1-1).**
- **PREREQUISITE PRIVACY PRINCIPLE: -**
- **DESCRIPTION:** The first auditing step includes the "Purpose Specification Privacy Principle" (Fig. 1). When an organization wishes to protect the users' privacy, the first step is to clearly define and explain the purpose of collection and use of personal data. To do so, the documents presented in the privacy audit checklist are essential. Therefore, when a privacy auditor wishes to audit if an organization applies the principle, he/she should ask for all the documents, which specify the purpose listed in Table 1.

STEP 2:

- **PRIVACY PRINCIPLE:** Collection Limitation **(PP-S2-1)**.
- **PREREQUISITE PRIVACY PRINCIPLE:** (PP-S1-1).
- **DESCRIPTION:** The first privacy principle that belongs to the second auditing step is the "Collection Limitation Privacy Principle" (Fig. 1). When an organization wishes to protect the users' privacy, it has to limit the data collection and use. Having defined the purpose of data collection and use in the previous step, the organization is obliged to collect and use only the necessary data needed for its services. To do so, the documents presented in the privacy audit checklist (Table 2) are essential. Consequently, if a privacy auditor wishes to audit if an organization applies the principle, he should ask for all documents and means of data collection limitation, as listed below, that are used by the organization. If the "Purpose Specification" principle has not been audited, the auditing of "Collection Limitation" cannot be accomplished.

- **PRIVACY PRINCIPLE:** Data Quality **(PP-S2-2)**.
- **PREREQUISITE PRIVACY PRINCIPLE:** (PP-S1-1).

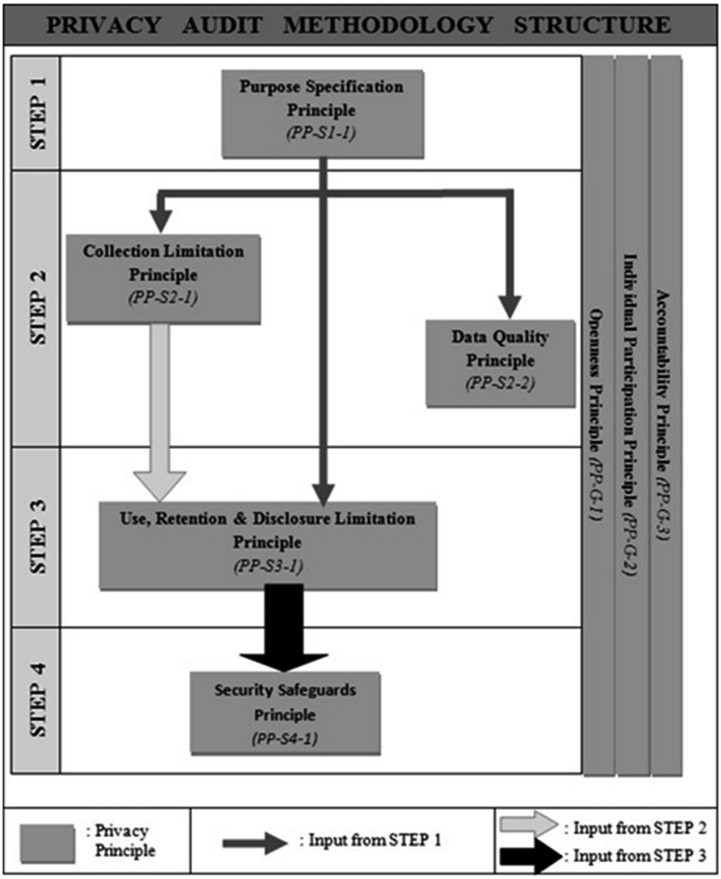
PRIVACY AUDIT METHODOLOGY STRUCTURE
STEP 1
STEP 2
STEP 3
STEP 4
Purpose Specification Principle (PP-S1-1)
Collection Limitation Principle (PP-S2-1)
Data Quality Principle (PP-S2-2)
Use, Retention & Disclosure Limitation Principle (PP-S3-1)
Security Safeguards Principle (PP-S4-1)
Openness Principle (PP-G-1)
Individual Participation Principle (PP-G-2)
Accountability Principle (PP-G-3)
: Privacy Principle
: Input from STEP 1
: Input from STEP 2
: Input from STEP 3

Fig. 1. Privacy audit methodology structure

- **DESCRIPTION:** The final privacy principle of the second auditing step is the "Data Quality Privacy Principle" (Fig. 1). The organization is obliged to keep the personal data of its users accurate, complete and up-to-date to the extent that this is necessary for the purpose of the data collection and use. To do so, the documents presented in the privacy audit checklist (Table 3) are essential. Therefore, if a privacy auditor wishes to audit if an organization applies the principle, he should ask for all documents, means and policies, which the organization uses to maintain the quality of personal data. If the "Purpose Specification" principle has not been audited, the auditing of the "Data Quality" principle cannot be completed.

STEP 3:

- **PRIVACY PRINCIPLE:** Use, Retention and Disclosure Limitation **(PP-S3-1)**.
- **PREREQUISITE PRIVACY PRINCIPLE:** (PP-S1-1), (PP-S2-1).
- **DESCRIPTION:** The third step of auditing includes the "Use, Retention and Disclosure Limitation Privacy Principle" (Fig. 1). This time the organization has to

Table 1. Privacy audit checklist for "Purpose Specification"

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Purpose Specification	The document that refers to the general purpose of the organization.				
	The document that refers to the main and specific aim for personal data collection either before or at the time of data collection.				
	The documents, brochures, videos, advertisements, conference workshop proceedings, notifications via the application, and everything else the organization uses to inform the users about the purpose of data collection.				
	The existence of privacy icons that inform the user about the purpose specification privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

limit the use, retention, and disclosure of personal information so as the individual should have the right to intervene wherever necessary (except if that is prohibited by law). To do so, the documents presented in the privacy audit checklist (Table 4) are essential. Consequently, if a privacy auditor wishes to audit if an organization applies the principle, he should ask for all documents and policies used by the organization to limit the use, retention, and disclosure of personal information. If the "Purpose Specification" principle and the "Collection Limitation" principle have not been audited, the auditing of the "Use, Retention and Disclosure Limitation" principle cannot be accomplished.

STEP 4:

- **PRIVACY PRINCIPLE:** Security Safeguards **(PP-S4-1)**.
- **PREREQUISITE PRIVACY PRINCIPLE:** (PP-S3-1).
- **DESCRIPTION:** The fourth auditing step includes the "Security Safeguards Privacy Principle" (Fig. 1). For the protection of users' privacy the organization has to employ security safeguards against loss or unauthorized access, destruction, use, modification or disclosure of data. To do so, the documents presented in the privacy audit checklist (Table 5) are essential. Therefore, if a privacy auditor wishes to audit if an organization applies the principle, he should ask for all documents and policies used by the organization to apply security safeguards. If the "Use, Retention and Disclosure Limitation" principle has not been audited, the auditing of the "Security Safeguards" principle cannot be achieved.

Table 2. Privacy audit checklist for "Collection Limitation"

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Collection Limitation	The document that refers to the purpose of data collection.				
	The documents, brochures, videos, advertisements, conference workshop proceedings, notifications via the application, and everything else the organization uses to inform the users about the purpose of data collection.				
	The document that refers to the policies and procedures, used by the organization to handle and collect the information.				
	The document that refers to the user's consent.				
	The document with the organization policies and procedures, concerning the destruction of personal data, when it is not useful anymore.				
	The appropriate technical means used by the organization's systems to minimize personal data.				
	The lawful and fair means used by an organization in order to collect the data. It includes the physical presence of the auditor during the operation of systems or subsystems. The means can either be technical or not.				
	The organization's privacy policy.				
	The existence of privacy icons that inform the user about the collection limitation privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

Global Principles. The privacy principles that follow have not been classified in any of the four auditing steps since they have been considered to be applicable throughout the entire auditing process (Fig. 1). As a result they have been considered as "Global" privacy principles, applying to all audit steps, and they should be strictly checked during the audit process. In practice, the usability of these global principles is that they add to the audit controls of each distinct audit step (i.e. for the principle "Collection Limitation" of step 2 (PP-S2-1) on top of the audit controls listed in Table 2, the auditor will need to check the global principles as well).

Table 3. Privacy audit checklist for “Data Quality”

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Data Quality	The document that refers to the purpose of data use.				
	The appropriate technical means used by the organization’s systems to audit if the personal data is kept accurate, complete and up-to-date.				
	The document with the organization policies and procedures, concerning the restoration and update of the personal data.				
	The organization’s privacy policy.				
	The existence of privacy icons that inform the user about the data quality privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

Table 4. Privacy audit checklist for “Use, Retention and Disclosure Limitation”

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Use, Retention & Disclosure Limitation	The document that refers to the purpose of the personal data use.				
	The document with the organization’s policies and procedures, concerning the limitation of the use, the retention and the disclosure of user’s personal data.				
	The document that refers to the user’s consent.				
	The organization’s privacy policy.				
	The existence of privacy icons that inform the user about the use, retention and disclosure privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

- **PRIVACY PRINCIPLE:** Openness **(PP-G-1)**.
- **DESCRIPTION:** When an organization wishes to support openness, it has to make available to users all policies, practices and procedures about personal information. To do so, the documents presented in the privacy audit checklist (Table 6) are

Table 5. Privacy audit checklist for "Security Safeguards"

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Security Safeguards	The document that refers to the physical, administrative and technical measures that the organization applies. For all these measures, the privacy auditor should check the premises, the employees and the technical means used by the organization.				
	The employees' training program.				
	The document with the organization's policies and procedures, concerning the employment of security safeguards for the protection of personal data.				
	The organization's privacy policy.				
	The existence of privacy icons that inform the user about the security safeguards privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

essential. Therefore, if a privacy auditor wishes to audit if an organization applies the principle, he should ask for all documents and policies used by the organization to keep its services transparent in and inform its users. If the prerequisite privacy principles are not met, auditing of the "Openness Privacy" principle cannot be accomplished.

– **PRIVACY PRINCIPLE:** Individual Participation **(PP-G-2)**.
– **DESCRIPTION:** The second global principle is the "Individual Participation" (Fig. 1). When an organization wishes to support individual's participation, it should allow users to access and modify their personal information. To do so, the documents presented in the privacy audit checklist (Table 7) are essential. Therefore, if a privacy auditor wishes to audit if an organization applies the principle, he should ask for all policies and procedures used by the organization to help users access their personal data. If the prerequisite privacy principles are not met, auditing of the "Individual Participation" principle cannot be accomplished.

– **PRIVACY PRINCIPLE:** Accountability **(PP-G-3)**.
– **DESCRIPTION:** The final global principle is "Accountability" (Fig. 1). When an organization wishes to be reliable, it should be accountable for complying with measures, which give effect to the privacy principles stated above. To do so, the documents presented in the privacy audit checklist (Table 8) are essential.

Table 6. Privacy audit checklist for "Openness"

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Openness	The document that refers to the purpose of data collection.				
	The document that clearly expresses the policies, practices and procedures for the management of personal information.				
	The technical or other means that the organization uses to inform the users about the management of personal data. The privacy auditor should check the means in practice.				
	The document stating the way in which policies, practices and procedures for the management of personal information are made public. The privacy auditor should control the ways of publication in practice.				
	The document with the steps that inform a user about all policies, practices and procedures for the management of personal information (on user's request).				
	The organization's privacy policy.				
	The existence of privacy icons that inform the user about the openness privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

Therefore, if a privacy auditor wishes to audit if an organization applies the principle, he should ask for all policies and procedures used by the organization so as to be reliable towards users. If the prerequisite privacy principles are not met, auditing of the "Accountability Principle" principle cannot be accomplished.

4.2 From a User's Perspective

Protecting user's personal data should always be of interest to the organization. The user should always have the right to be informed about the protection mechanisms in place, as well as about the personal data and the documents the organization uses.

To be more specific, in order for the user to trust the organization and the services offered, it is essential that he will be given the right to get any information he needs in

Table 7. Privacy audit checklist for “Individual Participation”

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Accountability	The Privacy Officer and the employees who are responsible for the management of personal information.				
	The training program of Privacy Officer and employees.				
	The policy about the responsibilities of the Privacy Officer.				
	The supplementary policies and procedures that the Privacy Officer has created.				
	The organization’s privacy policy.				
	The existence of privacy icons that inform the user about the accountability privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

regard with the collection, processing and storage of his personal data, as well as the way the organization complies with the main privacy principles. Indicatively, from the user’s perspective the following cases should be supported by the organization: (Fig. 2)

- The first case is when the user wishes to be informed about the audit procedure followed by the organization. In this case the organization should allow the user to get information about all the documents, means and policies or practices that are used in order to collect and process his personal data. The user should have access to all or to selected documents with the audit information of privacy principles. These documents should be offered in a user-friendly way, so users can easily access them at anytime.
- The second case is when the user wishes to contact the organization in order to get further information. The organization should provide an appropriate user-friendly way to receive user requests and provide them with the necessary clarifications. The idea behind that interaction, between the organization and the user, is to support the necessary transparency that the user needs in order to decide if he will proceed utilizing the services offered by the organization or not.
- The third case is when the user is not interested in the details of the auditing procedure but he simply needs some assurance that his personal data are secure. To achieve that the organization could employ the following privacy audit icons that will visually inform him that the organization has been audited by an appropriate auditing body.

Table 8. Privacy audit checklist for "Accountability"

PRIVACY PRINCIPLE	EVIDENCE	ASSESSMENT			ACTIONS
		M	NM	PM	
Individual Participation	The document that refers to the policy which informs the users on the personal data that the organization collects.				
	The document that refers to the user's consent.				
	The policy that refers to the period of time in which the organization should respond to the users' requests concerning the access to the corresponding personal information.				
	The policy that refers to the way third parties manage the users' personal data and how the users can have access to them.				
	The policy that refers to all exceptions of denying access to users' personal data.				
	The complaint procedures.				
	The identification procedures.				
	The organization's privacy policy.				
	The existence of privacy icons that inform the user about the individual participation privacy principle and obligate the organization to follow it.				

M: Met, NM: Not Met, PM: Partially Met

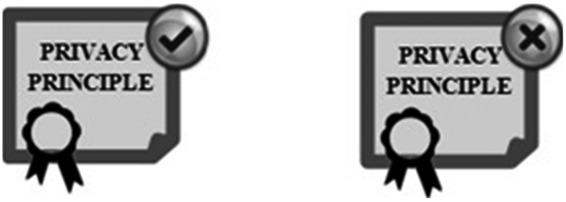

Fig. 2. Privacy principle icons

5 Conclusions and Further Work

Driven by the most widely used privacy principles, which have been either introduced by countries or by public/private bodies, this paper presents a structured privacy audit methodology that consists of discrete steps that organizations can follow for protecting or/and auditing the privacy of their users. Every step is based on the significance of the privacy principle and on the sequence of the audit procedure.

Currently, we are in the stage of applying the proposed privacy audit methodology to a real environment in order to validate its correctness and effectiveness, as well as its importance for both organizations and users. Furthermore, we are in the process of integrating this work with a privacy requirements elicitation methodology, in order to develop a uniform environment that system developers can utilize for both identifying privacy requirements and then audit their correct implementation.

Acknowledgements. This work has been partially supported by the Research Center of the University of Piraeus.

References

1. Cavoukian, A.: Creation of a Global Privacy Standard, November (2006). http://www.ipc.on.ca/images/Resources/gps.pdf
2. Cavoukian, A., Taylor, S., Abrams, M.E.: Privacy by Design: essential for organizational accountability and strong business practices, Identity in the Information Society, Springer (2010). http://link.springer.com/article/10.1007/s12394-010-0053-z
3. Cavoukian, A.: The privacy payoff: how building privacy into your communications will give you a sustainable competitive advantage. In: International Association of Business Communicators International Conference 2008, New York, June 24, 2008. http://www.ipc.on.ca/images/Resources/2008-06-24-IABC-NYC.pdf
4. Cavoukian, A.: Privacy by design – the 7 foundational principles, Technical report, Information and Privacy Commissioner of Ontario, January 2011. (revised version)
5. Canadian Standards Association, Model Code for the Protection of Personal Information, A National Standard of Canada, Canadian Standards Association, March 1996. http://www.rogerclarke.com/DV/CanModel.html
6. Le Métayer, D.: Chapter 20 - Privacy by Design: A Matter of Choice, Data protection in a profiled world, Springer, (2010). http://link.springer.com/chapter/10.1007/978-90-481-8865-9_20
7. Directive 95/46/EC of the European Parliament and of the Council, The European Parliament and the Council of the European Union, October 24, 1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
8. Directive of the European Parliament and of the Council, European Commission, Brussels, March 12, 2014. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN
9. van Blarkom, G.W., Borking, J.J., Olk, J.G.E.: PET, Handbook of Privacy and Privacy-Enhancing Technologies, The Case of Intelligent Software Agents, 2003, ISBN 90-74087-33-7. http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

10. Generally Accepted Privacy Principles (GAPP) (2010). www.aicpa.org/privacy, https://www.cippguide.org/2010/07/01/generally-accepted-privacy-principles-gapp/
11. Karjoth, G., Schunter, M., Waidner, M.: Privacy-enabled Services for Enterprises, IBM Research, Zurich Research Laboratory (2002). http://www.semper.org/sirene/publ/KaSW3_02.TrustBus-final-2002-05-01.pdf
12. Information technology — Security techniques — Privacy framework, International Standard, ISO/IEC 29100:2011(E) (2011)
13. Hoepman, J.-H.: Privacy Design Strategies, May 7, 2013
14. Hoepman, J.-H.: Privacy Design Strategies, October 25, 2012
15. Konstantina, K., Stefanos, G., Konstantinos, M.: Towards a Privacy Audit Programmes Comparison Framework. Springer-Verlag, Heidelberg (2004)
16. OECD Privacy Principles, OECDprivacy.org (1980). http://oecdprivacy.org/
17. Privacy, Accountability and Trust – Challenges and Opportunities, ENISA, February 2, 2011. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study
18. Reform of data protection legislation, European Commission, (2012). http://ec.europa.eu/justice/data-protection/
19. Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce, July 21, 2000. http://www.export.gov/safeharbor/eu/eg_main_018475.asp
20. The 10 Privacy Principles of PIPEDA, PrivacySense.net. http://www.privacysense.net/10-privacy-principles-of-pipeda/
21. The OECD Privacy Framework, OECD (2013)
22. Tommie, W.: Singleton, IT and Privacy Audits. ISACA J. **5**, 2009
23. Wang, Y., Kobsa, A.: Privacy-Enhancing Technologies (2008). http://www.cs.cmu.edu/afs/cs/Web/People/yangwan1/papers/2008-Handbook-LiabSec-AuthorCopy.pdf