Protecting Personal Data: Can IT Security Management Standards Help?

Giovanni Iachello
College of Computing & GVU Center
Georgia Institute of Technology
giac@cc.gatech.edu

Abstract

Compelled to improve information security by the introduction of personal data protection legislation, organizations worldwide are adopting standardized security management guidelines to inform their internal processes. This paper analyzes whether existing security management standards support process requirements for personal data management, drawing from experience with security policies in private organizations and through an analysis of current European and US legislation. Various aspects of personal data management not commonly addressed by security standards are identified, and a number of generally applicable enhancements are proposed to one common standard, IS17799. The appropriateness of including data protection guidelines in security standards is discussed, showing how these enhancements could simplify the definition of personal data management procedures in organizations.

Key words: *personal data protection, privacy, information security management, IS17799, multilateral security, HIPAA*

1. Introduction

Organizations worldwide have been compelled by law to address the issue of personal information security when personal data protection legislation was introduced starting in the '70s.[1] Previously, the value of personal information was mainly strategic, and high-grade security was domain of large financial and governmental organizations.

European guidelines [6] and related national laws [11, 16, 22] require organizations handling personal data to adopt specific security measures, in order to protect information from misuse, disclosure, loss and corruption. In the United States, new laws like the Health Insurance Portability and Accountability Act (HIPAA) [28] have introduced similar provisions for the private sector, whereas federal agencies have been regulated for a longer time [29, 25, 27]. Many other nations have introduced similar data protection legislation during the '90s.

Concurrently, security risks to information systems have steadily increased: organizations have gradually gone online, introducing new threats; outsourcing and specialization have increased information flows; and, finally, the value and the sheer amount of data have also increased. As a result, security has become an important aspect of information technology and spurred thriving product and service markets.

Seeking cost-effectiveness and simplification, organizations have started to evaluate and certify the security of products and management procedures in a standardized manner. However, these standardization efforts have not, to date, met the needs of organizations dealing with personal data, because comprehensive legislation in the field is fairly recent and generalizations over the specific requirements mandated by regulation are only now starting to be well understood by professionals.

The present paper draws on experience related to the use of one information security standard (IS17799) in private organizations handling personal information. Section 2 reviews current legislation to help identifying areas for improvement for IT security management standards. Section 3 argues that personal data protection should be included in infosec standards. Finally, Section 4 proposes some additions to the IS17799 "Code of Practice", with the aim of helping security managers integrate privacy and security management.

1.1. The management of personal data

Personal information about customers, users and employees represents a valuable asset for any organization, but at the same time requires special care. European regulation grants the *data subject* (the person to whom the information relates) rights, including that of choosing whether or not to allow processing, and, in some cases, even of influencing how the data should be processed (e.g. for what purpose, if they may be disclosed, etc.). In

[1] In the remainder of the text the term "data protection" will be used specifically in connection with personally identifiable data.

the US, similar regulation has recently become effective in connection with the Health Insurance Portability and Accountability Act. Respecting these and other conditions set by legislation can contrast with an otherwise "efficient" use of the data, e.g. for marketing purposes, and requires organizations to shift the focus of security from technology to process design and control.

Although these laws grant the data subject a number of rights, the *data controller* (the organization which manages the data) also has a great deal of freedom in determining how personal information is used, as long as the data subject provides *informed consent* in a more or less explicit manner, depending on the type of data collected, the processing activities and the purpose for collection. Organizations are thus responsible of defining data management policies and of complying with them, which leaves them with the burden of developing suitable internal processes.

While integrity and confidentiality remain core objectives for personal information management, the competing interests of the different stakeholders are difficult to solve simply by increasing "security". First, regulation imposes requirements that actively involve an entity (the user or customer) which is traditionally considered external to the organization, and therefore an explicit source of risk. Second, the organization has limited discretion over the data, and is bound to strict rules regarding their collection, storage and destruction.

Due to their highly centralized nature, traditional security models are not apt to state in a simple manner this kind of partially user-defined policies. For example, while traditional models cope with non-trusted entities (for example a disgruntled employee) at various levels (using need-to-know policies, hierarchical security domains, ACLs, etc.), the organization *itself* is generally assumed to be trusted. But from a *multilateral security* perspective [17], the organization is a source of risk for the data subject, this in fact being the reason for introducing regulation in the first place. In conclusion, addressing data protection requirements only by using security policies based on access control is very difficult, as certain processing activities might be permitted as long as requirements are met, which hardly relate to security in the traditional sense (e.g. having obtained data subject's consent for a particular use).

The issue is actually more complex, because the translation of overlapping and vague legal guidelines into specific functional and process requirements is hard, as implementation depends on many other factors (interpretation of laws and regulations, exceptions, industry best practices, etc.). However, the conclusion is that personal data protection can be guaranteed only by adopting, along with traditional security requirements, process requirements which are normally not considered belonging to the security domain, including communication with data subjects, keeping track of their preferences and observing restraint policies.

1.2. Standards in security management

Introduced in the early '80s, evaluation and certification standards for IT security focused at first on software and systems used to process sensitive information, and was employed by governments as a means for streamlining procurement. These standards [4, 12, 13] define products' functional properties and regulate their development process.

Eventually, the increasing complexity of information-intensive processes has led to the development of security standards addressing the organizational aspects of IT security (e.g. responsibilities, communication, crisis management, …) [18, 19, 14]. These standards, which codify industry best practices, are used to drive the design and implementation of processes (Fig. 1). One popular choice for private organizations has been the BS7799 standard and its successor, IS17799. British Standard 7799 was developed in the early '90s as a contractual basis for large (financial and health) organizations, which, needing to share information, required assurance about their respective information management practices. Certification according to the standard grants to the organization (or more often to its IT department) a "secure" status, thus eliminating the need for case-by-case mutual evaluation.

In the past few years, however, security certification standards have been employed in ways which stress their ability to cope with new needs. First, standards are not anymore necessarily used to achieve certification, due to the high cost and lengthy procedures of a formal evaluation, and because neither legislation nor market pressure do (yet) require a formal security certification for most organizations. Instead, many organizations increasingly use standards, or parts thereof, as a codified "best practice", to help IT managers defining effective and complete security policies and processes, or as a basis for informal assessment.

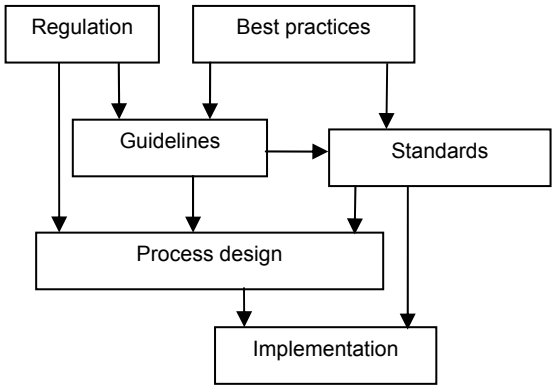

Figure 1. Role of standards in process design

Second, these standards are increasingly used by organizations in connection to data protection issues. Undoubtedly, standardized best practices can be extremely valuable in this domain, because they fill the void of process definition between high-level abstract legislation and low-level technical details. However, new applications question security management standards adequacy for such purposes, or whether they could be enhanced to better support practitioners with their data management needs.

In fact, personal data protection is not specifically covered by the IS17799 "Code of Practice" (the descriptive part of the standard). Privacy issues are cited mainly in relation to legislation compliance, and the standard could even be criticized because it implicitly disregards the privacy of employees (e.g. the "Personnel security" clause contains detailed screening requirements).

While the following discussion centers around IS17799, the conclusions apply to other security management guidelines and standards as well ([18, 19]). IS17799 was chosen as a case study because of the widespread popularity it enjoys, especially in the private sector. Also, thanks to its modular and extensible structure, the standard lends itself well to additions and enhancements, as discussed below.

2. Analysis of data protection requirements

In order to understand what additions would be necessary to the Code to better support personal data management, reference to normative sources is required. To this end, an ample range of legislation and guideline documents have been systematically analyzed, in order to enucleate specific security management requirements. This led in turn to the identification of relevant aspects of personal data management, which form the core of the proposed addition to the Code.

Table 1 summarizes the results of this survey. It lists a number of management requirements present in legislation and codes of conduct and shows to what degree, if at all, these requirements are covered by IS17799. Where applicable, reference to the section of the text is provided. Requirements are grouped in categories, which are further generalized in Section 4.

The survey is based on various sources, not all explicitly included in the table:

- the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 [20],
- the Canadian Model Code (CMC) for the Protection of Personal Information of 1996 [3],
- EU Data Protection Directive of 1995 [6], including some related national legislation [11, 16, 22],
- the Health Insurance Portability and Accountability Act of 1997 (HIPAA) [28],
- the EU Telecommunications Privacy Directives of 1997 and 2002 [8, 10],
- the Electronic Communications Privacy Act of 1986 [26] and
- the EU Telemarketing and E-commerce Directives of 1997 and 2000 [7, 9].

The OECD Guidelines provide broadly accepted principles for fair personal data management, including *inter alia*, limitation of use and individual participation. The Guidelines are non included in Table 1 because they do not prescribe specific management requirements. Instead, some management requirements are detailed in the Canadian Model Code, published in 1996 by the Canadian Standards Association, which is largely based on the OECD Guidelines and is included in the table.

The EU Data Protection Directive represents the synthesis of a long experience in different legal contexts, and is considered the most comprehensive law adopted on such a large scale (it has been implemented at the national level by most Member States [5]). National legislation contains specific organizational requirements necessary for regulatory compliance.

HIPAA contains specific provisions for health information protection and is one of the first extensive data protection regulations imposed on the private sector in the US, which makes the comparison with European legislation and management standards particularly interesting. The specific provisions enacted by HIPAA (and indicated in Table 1) are detailed in two recently published Federal Regulations, known as the Privacy Rule [23] and Security Rule [24].

The European [10, 8] Telecommunications Privacy Directives are of interest because they:

1. regulate personal information collected automatically by telecommunication systems,
2. protect individual's rights to confidentiality,
3. affect an increasing portion of trade and everyday life, as ever more services are provided through telecommunications.

The US Electronic Communications Privacy Act [US86] regulates the same sector as the mentioned European Directives, but mainly concentrates on how wiretapping is to be conducted on electronic communications, and provides only a very limited set of rules for service providers to follow to protect consumer privacy.

Finally, the following legislation was included in the survey, but does not appear in the comparative table. The Directives impose privacy-related requirements, indicated in the table with a reference in the first column.

- The European "telemarketing" Directive [7] contains some consumer privacy provisions.
- The European E-commerce Directive [9] is noteworthy because it explicitly links personal data protection and consumer protection in the electronic marketplace.

Table 1. Process/management requirements for personal data security[◊]

Security and process requirements	EU data protection directive 95/46	EU telecom directive 02/58	US HIPAA PL. 104-191[*]	Canadian Model Code	IS17799
Communication with data subject					
Information to the data subject about use of data	yes	yes[‡]	yes	yes	
Public communication about privacy	yes		yes	yes	
Communication of security risks to customers		yes			
Unsolicited communications sender identification		yes			
Unsolicited communications prior consent		yes			
Contact point in the organization for subjects and DPA	yes		yes	yes	partial 12.1.4
Confidential communication with the subject			yes		yes
Information control by data subject					
Request consent for data use	yes	implicit	implicit	yes	
Temporary denial of processing by data subject	yes	yes	partial		partial 12.1.2
Data destruction under request	yes		partial		partial 12.1.2
Access and rectification to data by data subject	yes	partial	yes	yes	partial 9.2
Selectively object to specific data processing	yes	partial	partial		
Organizational processes					
Defined processes to access and amend personal data			partial		
Workforce training and management	yes		yes		yes 6.2
Identification of data processing responsibilities	yes	implicit	yes	yes	yes 4.1.3
Workforce individual access codes to information systems	yes[§]				yes 9.3.1
Review of access rights of data processor workforce	yes[§]				yes 9.2.4
Minimal access to information by processors	yes	yes	yes	yes	partial 9.1
Standard disclosure procedures			yes		
Third parties cascade of correction, amendment, removal	yes		partial	yes	partial 8.7.2
Contractual security obligations for processor	yes		yes	partial	partial 8.7.1
Organization requirements for mergers, acquisitions, etc.	yes[†]		yes		
Definition of an internal privacy policy	implicit		yes		
Security requirements					
Provisions for confidentiality and integrity	yes	yes	yes	yes	yes
Purpose for use of data	yes	yes	yes	yes	
Removal of cached data when original is deleted [9]	yes				
Controlled reuse of media and computing systems	yes[§]				yes 8.6
Destruction of data after a defined time period	implicit	yes		yes	partial 8.4
Provisions for protecting data stored on user equipment		yes			partial 9.8
Anonymization of data for subsequent use	yes	yes		yes	
Anonymous use of services		yes			implicit 8.7.6
Third party management					
Challenge procedures	implicit			yes	
Relationship management with a DPA	yes				
Notification of data processing activities	yes				
Data retention for misuse prevention		yes			partial 12.1.5
Record communication as evidence of transactions		yes			partial 12.1.3
Consultation of opt-out registers [9]					

[◊] Only process requirements directly related to personal data management are included in the table. General security requirements are excluded.

[*] Including application rules [23] and [24].

[‡] For value-added services only.

[†] In implementation guidelines.

[§] In national implementation regulation.

Table 1 shows that different regulations induce a set of partially overlapping requirements on personal data management procedures. In some cases, these requirements are expressed directly in the text of the law; more often, they are defined in implementation specifications (allowing for more expedite revision), or are implied by published best/common practices (this is indicated with the word "implicit"). Considering the scope and detail level of Directive 95/46, it has been used as the benchmark reference. The word "partial" in the remaining columns indicates that the considered law or guideline (EU Telecom directive, HIPAA and CMC) contains a similar requirement, but covering only a subset of the corresponding requirement in Directive 95/46.

Most regulation identifies four main groups of stakeholders (data subject, data controller, data processor and data protection authority) and regulates the interaction between, and the operation of, each of these entities. Requirements are grouped based on the process stage and the stakeholders to which they relate (grouping headers are indicated in boldface), namely:

- communication from controller to subject (first group),
- communication from subject to controller (second group),
- internal processes of the controller/processor (third and fourth groups),
- third party relationship management (last group).

The coexisting presence of both abstract, high-level requirements (e.g. "Workforce training") and very specific requirements (e.g. "Individual access codes to information systems") reflects the actual nature of regulation, which is typically more specific on aspects with standard established practices, and leaves areas where no common practice exists unspecified.

The last column of Table 1 indicates whether IS17799 provides support for the requirement, and the relevant section of the standard. An exact, deterministic assessment of whether IS17799 supports a specific legal requirement is obviously difficult to make; in general, support has been considered sufficient (indicated by a "yes") if, in the author's view, a reasonable and straightforward implementation of the standard would lead to a process which complies with the requirement. In some cases, the guidelines provided by the Code of Practice only partially cover the stated requirement; this is indicated with a "partial" annotation. Although it is an interesting exercise, the discussion of each single assessment is not presented here, due to space constraints.

While the list is not intended to be exhaustive, it can be easily observed that many privacy-relevant requirements mandated by legislation are not covered by IS17799. This result is not unique to that standard: summary analysis of the other management guidelines mentioned above suggests similar results.

3. Does data protection belong to security standards?

In the previous section, five groups of requirements have been identified, implicitly suggesting that they could be included in security management standards with the intent of addressing their shortcomings. At first sight, augmenting these standards with data protection requirements might not seem appropriate: after all, most current standards are already very extensive and further expansion could harm their flexibility and ease of use. Moreover, some requirements listed in Table 1 are not typically considered part of security management.

Nevertheless, there are a number of compelling reasons for introducing multilateral security provisions in traditional security frameworks. First, many organizations (telecoms, financial institutions, health and employment services) face changes to their information security practices directly connected to data protection regulation. Integrating privacy in the discussion of security measures rationale would streamline and simplify process design.

Second, few professionals have a solid grasp of all issues related to data protection, which span legislation, technology and process design. The situation is even more complex for multinational organizations due to subtle differences across national contexts. Moreover, personal data management is still a relatively new topic, and regulation often does not provide sufficient assistance. In fact, even simple regulation can lead to very complex formal requirements on technology and processes, let alone their evaluation and certification (consider for instance the controlled transfer of information to third parties, described below). This emphasizes the need for stronger guidance than that provided by legislation alone, which can be effectively provided by coherent standards.

However, the main argument is that sound personal data management and security cannot be designed disjoint from each other. An example involving a very basic security measure, data backups, will help clarify this point. Regarding backups, IS17799 calls for the following (Code of Practice, section 8.4.1, page 25; ellipses by the author):

"*Back-up copies […] should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. […] The following controls should be considered.*

a) A minimum level of back-up information […] should be stored in a remote location,[…] to escape any damage from a disaster at the main site. […]

b) Back-up information should be given an appropriate level of physical and environmental protection […]

c) Back-up media should be regularly tested, […]

The retention period for essential business information […] should be determined."

Backups of personal data, necessary for guaranteeing integrity and continuity, also cause information replication notwithstanding data minimization principles. The need of selectively deleting data from backups is not considered in the above formulation. However, according to regulation, all copies of personal data under control of the organization should be deleted when fulfilling justified requests of the data subject to terminate processing. Clearly, the organization should be able to treat backups (and other copies like cache) in the same way as data kept in live systems, and dispose of them, or anonymize them, when not anymore needed. This can create considerable practical problems (e.g. if backups are stored on permanent media).

This example shows that even the most basic security requirements need adjustment in order to comply fully with data protection legislation. Experience shows this to be a recurring pattern: security and personal data management need to be systematically reconciled. As a result, if security standards are used for designing or assessing processes where data protection is a concern, they should integrate personal data protection with security.

Supervision tasks would also benefit from standardization. Data protection authorities (DPA) in charge of overseeing personal data management are often overburdened and understaffed, and are unable of assisting and assessing organizations on an individual basis. Often the clarification of the details of regulation is left to industry-wide guidelines, and conformance to the single organization. A standard framework could aid in defining "privacy protection profiles", using a common language and structure, for use by industry, similarly to Common Criteria's Protection Profiles [13].

Independent certification has been used successfully in the past (e.g. IT security evaluation criteria) to provide increased assurance of the security qualities of information systems. A data protection quality standard, along the lines of ISO 9000, could provide consumers as well as corporations with increased assurance for trusting data controllers, especially in sectors such as health care, financial services and employment services. The success of BS7799 and initiatives such as the Generally Accepted Information Security Practices (GAISP) show that private organizations are indeed pushing towards tighter integration and standardization in security management, not last with the aim of increasing information flows among them.

3.1. Extending IS17799

In light of the above discussion, augmenting IS17799 would leverage its vast deployment by the private sector, reducing implementation costs. Moreover, the standard's modular structure simplifies the task of developing additions: new requirements could be implemented by adding a new clause (chapter) to the Code of Practice. Alternatively, existing clauses could be modified. The former option was favored here, in order to retain the standard's modular structure, and for better maintainability.

The choice of exactly which new requirements to include, and their detail level, should maintain a level of abstraction consistent with the existing standard. The new requirements should provide guidance to process designers and fill the gap between legislation and the actual process. Moreover, a common set of modular requirements should be usable by practitioners and supervision authorities alike. In general, additions to the standard should meet the following basic properties suitable to any good requirement set.

- Verifiability: requirement implementation must be verifiable during audit; e.g. a binary determination of compliance should be possible for each statement.
- Simplicity: multiple assertions should be divided into different statements; this helps verification tasks, and supports coding cross-requirements.
- Generality: requirements should not refer to specific organizational settings.
- Applicability: it should be clear whether a requirement is mandatory or not in a given setting; this is most important in case of certification.
- Consistency: the requirements should be internally as well as externally consistent.

The additional privacy clause should be considered optional and would not be used, at least initially, for certification, because not all organizations need to manage personal information. To this effect, the Specification section (i.e. the normative part) of the standard [2], which lists the requirements which must be met in order to be certified, would not be amended.

In the next section, an overview is provided of the possible structure and contents of such additions.

4. Proposed management requirements

The proposed additional requirements to IS17799 are grouped in five broad areas, as indicated in Table 2 below. This grouping is different from that of Table 1, being based on five requirements areas which mimic the current organization of IS17799; this organization was preferred on consistency grounds. For each category in Table 2, some sample requirements taken from Table 1 are listed, to show how requirements coded in legislation could fit in the top-down structure induced by the standard.

In the following sections, each requirement area is explained, and appropriate enhancements to the standard are proposed to support the requirements in Table 1, which are not covered by the Code. It should be noted that the following discussion is meant to be just a starting point for developing comprehensive and coherent requirements which could make their way into a future version of the standard.

Table 2 Data protection requirements organized according to IS17799 conventions

Requirement Areas	Sample Requirement(s)
Privacy Policy	Definition of an internal privacy policy Organization requirements for mergers, acquisitions, etc.
Responsibility	Identification of data processing responsibilities
Product / Process Specification	Anonymization of data for subsequent use Standard disclosure procedures Defined process to access and amend data
Communication	Communication of security risks to customers Relationship management with a DPA Notification of data processing activities
Challenge Compliance	Data retention for misuse prevention Data destruction upon request Challenge procedures

4.1. Privacy policy

A policy document provides basic guidelines and principles for all requirements and procedures related to some specific area of activity. Security policies are essential for sound security management: similarly, organizations should also develop and maintain an internal privacy policy.

Note that this internal privacy policy is fundamentally different from the public privacy policy written for the data subject according to the Openness principle [20]. The latter is a statement, required by most regulation, that organizations collecting personal data provide to the data subject before requesting informed consent. The former is used within the organization as a basis for defining specific rules and to verify their implementation. It is aimed at employees and third parties, such as business associates and the DPA and its scope includes aspects which normally would not be included in the public policy (staffing, budgeting, internal roles, etc.).

The level of detail of the policy depends on the specific case; policy documents, because of their general nature, should not include items which need to be amended in case of small changes to the processes and management structure within the organization. As any policy document, the privacy policy should be actively maintained and endorsed within the organization by senior management. It should also define how infringements to the policy are handled. To this effect, the privacy policy should be *written*, in order to verify and assess processes and practices against a stable reference.

Finally, the policy can be also used as a communication and education tool within the organization, to spread knowledge about data protection among staff and employees, and awareness of individual responsibility.

4.2. Responsibility

One fundamental aspect of personal data management is the assignment of responsibilities: accountability is a prerequisite to enforcement and therefore for credible asset management, especially in the case conflicting interests exist. Legislation is generally very vague in this area, and typically only calls for the institution of an "privacy officer" within the organization: more guidance is needed in order to define sound processes.

Enhancements to the standard would include requirements for the definition of responsibilities and the identification of responsible subjects (or roles) within the organization, and for the written assignment to these subjects of data management duties.

In general, responsibilities for using the data should be distinct from that of maintaining their privacy properties. An independent "privacy officer" might be better suited to identify misuse or infringement, being less pressured to use the data for mission goals competing with data protection, as opposed to the user of a dataset. In small organizations, where dedicated staff is unavailable, this role is typically assigned to the CIO or equivalent.

Any management guideline should acknowledge that different subjects in the organization play different roles related to personal data. Operators (e.g. bank clerks, medical staff, etc.) working day to day with personal data should be made aware of handling procedures and regulations, and should be able to access the data according to need-to-know policies. Their responsibilities include:

- keeping the data up-to-date and correct,
- avoiding disclosure and misuse,
- informing and collecting consent from the data subjects according to the privacy policy,
- cooperating with need-to-know principles and other policies,
- reporting incidents and threats to the personal data.

Management roles in the organization should verify that policy and regulations are applied and that infringement is prevented and corrected.

Other specific roles within the organization, in some cases required by legislation, should be defined and responsibilities should be allocated. These include a "contact point" for inquiries and requests by data subjects and authorities. Responsibility should also be assigned for amending and deleting data and terminating any processing activity as mandated by law.

Finally, responsibility assignments should be periodically reviewed.

4.3. Product and process specification

While legislation does not mandate any specific process implementation, process definition has a fundamental impact on the effectiveness of personal data protection.

Consider as an example the cost/benefit tradeoff present in most surveyed legislation, whereby some requirements (e.g. informing the data subject or obtaining consent for use) can be waived when the effort required to comply would be "unreasonable" related to the kind of data collected and the processing activities involved. Just how "reasonable" such effort is, clearly is influenced by process design.

Detailing the impact of regulation on process design would entail a discussion too lengthy for the present paper. However, since medium and large organizations typically custom-develop their workflow systems, data protection should be addressed from the start by process design. This is well illustrated the "backup policy" example reported above. Once the backup policy and techniques are defined, it becomes very difficult to introduce privacy-enhancing provisions at a later stage. Ideally, specific provisions taken during the development of products, systems and processes should ensure that all relevant regulations and policies are complied to.

There are numerous aspects of process design which impact data protection; three, particularly well suited for addition to the standard, are briefly described below.

Data minimization. Data protection can be achieved at the process level by reducing the amount of managed information (information economy) and by defining need-to-know policies. Simply changing where information is stored, or how individuals are identified, can greatly reduce the need of storing or transferring information. For this reason standards should require to develop and assess processes according to information reduction principles, and to evaluate and document a compromise between process complexity, efficiency, and data protection. This would encourage the organization to analyze its internal processes throughout, and to provide evidence that the process design strikes the optimal balance between the protection of personal data, performance, and the allowed use of the data. Process documentation is especially important for complex workflow systems and large organizations, which are often independently analyzed as a "white box" (e.g. by external audit).

Sound process design based on the data minimization principle also allows to effectively reduce the cost of regulation compliance. For example, converting data to anonymous form prior to processing, when possible, can greatly simplify processes because data protection laws waive many requirements on anonymous data.

Information labeling. The consent expressed by the data subject to processing may be as simple as a yes/no alternative (to the defined policy), but in most cases, it involves multiple decisions about different activities, by permitting certain operations (e.g. processing for carrying out a contract) and disallowing others (e.g. transfer to third parties, marketing activities, …). Keeping track of these preferences requires the organization to associate policies and user preferences to the collected data, and to handle the data so that these preferences are preserved and complied to when the data moves within or out of the organization. One way to meet such requirement is that of labeling information with "privacy attributes" [1].

Labels are widely used as a form of security meta-information attached to data: IT security evaluation criteria provide for them with specific requirements [13]. In the privacy domain, such attributes identify what operations are allowed on the data: this kind of labels are already used in many systems which gather information about users (e.g. preferences on mailing lists, communication of data to third parties, etc.), but are often handled inconsistently. Privacy attributes may be lost or ignored when the data is transferred to other information systems, and during non-regular activities such as backups and crisis management.

Process and information systems should thus be designed to store attributes and make them always accessible along with the data to which they relate, throughout their entire lifecycle in the organization, and even when the data are transferred to third parties. Third parties should not ignore or remove such attributes. Moreover, the data subject should be able to access the privacy attributes along with the data in order to query and update his or her preferences.

Third party management. Data subject preferences are tightly coupled with third party relationship management, i.e. the management of the external entities that handle personal information for or with the data controller (e.g. CRM and marketing outsourcing, ICT services).

Third party management involves not only ensuring data confidentiality and integrity, and tracking what information may be disclosed to external entities and what not, but also verifying third party operating procedures, in order to assess whether sufficient assurance is provided that a third party will not violate, even accidentally, the policy accepted by the data subject. From this standpoint, standardizing personal data management and its related documentation could be extremely helpful, just like IS17799 currently helps standardize the format and content of security management documentation (and indirectly the processes themselves).

When designing third party data transfer, the organization should also plan for procedures to support the transmission of changes to data subjects' preferences (in the form of privacy attributes) or to the data itself (e.g. consent revocation) to all interested third parties. Since data might be further disclosed to others in a chain-like fashion, it is necessary to keep track of all third parties to which the data was disclosed. In case of consent revocation, the organization which originally collected the data from the user should be able to enforce and verify that all third parties have actually deleted the data.

Third party management, as briefly described above, entails complex procedures and costs for the organization. Data protection regulations acknowledge this by limiting requirements on third party relationship management: effort should be reasonable and commensurate to the value and sensitivity of the data. Again, just how "reasonable" this cost is depends to a great extent on how the process is designed, i.e. on how seriously the organization actually intends to protect the personal data it manages.

4.4. Communication

Most legislation requires organizations to be able to communicate with the data subject and the DPA, for a variety of reasons (see Table 1). External communication can benefit from standardization: many requirements are common to most regulation, and include the disclosure of policies, the collection of user consent, the management of inquiries, challenges, and information requests. Most of these transactions involve access control, confidential communication and the collection of privacy preferences essential to the data management process.

Management guidelines should include the definition of methods and constraints for accessing personal data by the data subject, for example the adoption of a "same media" policy (i.e. allowing access over the Internet for data gathered on a web site). This does not necessarily need to be an extra cost: communication with the data subject can be integrated with customer relationship and public relations efforts.

Somewhat complementary to this is the communication with the supervising body (e.g. the DPA in Europe and the Department of Health and Human Services for HIPAA). The supervising body usually acts under notification of potential infringement to verify the normative compliance of a data controller. The relationship between DPA and controller is well-defined in most regulation and shares common requirements, which again makes it a prime candidate for standardized guidelines.

Provisions should be adopted at least for notifying the DPA of the establishment and termination of data processing activities, for responding to queries and investigations originating with the DPA, for adapting to changes in regulation, and for signaling organizational changes (e.g. caused by mergers or acquisitions).

4.5. Challenge compliance

As consumers are learning to use the options provided by legislation for controlling the use of information about them, the number of challenges to data controllers is increasing (e.g. in Italy, after a slow start, the number of appeals to the data protection authority is now doubling yearly [15]). Challenges to data handling practices can be anything from a request of information from a data subject to full legal action. Ignoring these requests is not an option for any organization, as sanctions are foreseen for non-complying organizations.

Complying with challenge procedures requires organizations to define standard methods for handling these requests, both from legal and procedural standpoints. Predefined requirements to cover such a great variety of cases may be too complex to develop; however, some generic parameters can be set, including general standard procedures, responsibility assignment and response time and modalities.

For example, data management processes should support requirements imposed by data protection regulation in the area of data processing termination (i.e. when the data subject requests the termination of a certain processing activity); among other, internal processes should be implemented in such a way that it is possible to:

- identify data referring to a specific subject,
- delete or render anonymous any copies of such data, and
- generate sufficient evidence that all copies of the data have been actually disposed of or made anonymous.

For the sake of effectiveness, the responsibility of handling challenge requests should be assigned within the organization to a role with the authority to block or terminate data processing activities related to a specific individual, and to recommend changes in operational practices.

5. Conclusion and future work

As data flows grow and information fluidity increases, many organizations today face the challenge of effectively and systematically managing personal data. One way to tackle this problem is to provide common guidelines in the form of best practices for personal data management. The present paper contributes to this goal by providing a throughout analysis of a number of different regulatory regimes, and by identifying five main areas of security management requirements which need to be addressed by organizations engaged in personal data processing.

The case for integrating personal data management guidelines in security guidelines is discussed, and an example is provided of how security and data protection requirements are intertwined, and need to be jointly designed in order to be effective. The proposed enhancements could form the basis of an actual addition to IS17799 when the next ISO review occurs.

Further work should include developing draft guidelines and applying such enhancements in a real-world setting in order to evaluate their usefulness and effectiveness.

6. Acknowledgements

I would like to thank Kai Rannenberg, the members of IFIP Working Group 9.6/11.7 "IT Misuse and the Law" and André dos Santos for their support, valuable comments and for reading through early drafts of the paper. This work was partially funded by the National Science Foundation through the Graduate Research Fellowship Program and by the Sam Nunn School of International Affairs at Georgia Institute of Technology.

7. References

[1] P. Ashley, M. Schunter, C. Powers, "From Privacy Promises to Privacy Management – A New Approach for Enforcing Privacy Throughout an Enterprise", *ACM New Security Paradigms Workshop (NSPW)*, Virginia Beach VA, 2002.

[2] British Standards Institute, *BS7799-2:2000 Information security management. Specification for information security management systems*, 2000.

[3] Canadian Standards Association, *Standard CAN/CSA-Q830, Model Code for the Protection of Personal Information*, 1996, www.csa.ca/standards/privacy/code/.

[4] Department of Defense, *Trusted Computer System Evaluation Criteria (TCSEC)*, DoD standard 5200.28-STD, 1985, www.radium.ncsc.mil/tpep/library/tcsec/.

[5] European Commission, *Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data*, 2002, www.europa.eu.int /comm/internal_market/privacy/law/implementation_en.htm.

[6] European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, www.europa.eu.int.

[7] European Union, *Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts*.

[8] European Union, *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*.

[9] European Union, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*.

[10] European Union, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*.

[11] *German Federal Data Protection Act*, December 20, 1990, amended English translation, www.datenschutz-berlin.de /recht/de/bdsg/bdsg01_eng.htm.

[12] *Information Technology Security Evaluation Criteria (ITSEC)*, Technical Report, Version 1.2, 1991 www.cesg.gov.uk/assurance/iacs/itsec/index.htm.

[13] ISO, *ISO/IEC 15408:1999 (Parts 1-3) Information technology – Security techniques – Evaluation criteria for IT security*, 1999, www.commoncriteria.org.

[14] ISO, *ISO/IEC 17799:2000 Information technology – Code of practice for information security management*, 2000.

[15] Italian Data Protection Authority, *Relazione 2002*, May 20, 2003, www.garanteprivacy.it.

[16] Italian Law n. 675 of Dec. 31 1996, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, 1996, www.interlex.it/testi/l675_96.htm.

[17] Müller, G. and K. Rannenberg, Eds., *Multilateral Security in Communications, Volume 3: Technology, Infrastructure, Economy*, Addison Wesley, ISBN 3-8273-1426-7, 1999.

[18] National Computer Security Center, *A Guide to Understanding Trusted Facility Management*, 1989 NCSC-TG-015, www.fas.org/irp/nsa/rainbow.htm.

[19] NIST, *Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook*, http://csrc.nist.gov /publications/nistpubs/index.html.

[20] Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, www.oecd.org.

[21] K. Rannenberg, "Multilateral Security: A Concept and Examples for Balanced Security", *ACM New Security Paradigms Workshop (NSPW)*, Ballycotton, Ireland, 2001.

[22] United Kingdom, *Data Protection Act*, 1998, www.dataprotection.gov.uk/.

[23] US Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information; Final Rule*, 45 CFR Parts 160 and 164, Aug 2002.

[24] US Department of Health and Human Services, *Health Insurance Reform: Security Standards; Final Rule*, 45 CFR Parts 160, 162, and 164, Feb 2003.

[25] United States Senate, *Computer Security Act of 1987* http://security.isu.edu/publications.htm.

[26] United States Senate, *Electronic Communications Privacy Act of 1986*, www.law.cornell.edu/uscode/.

[27] United States Senate, *Federal Information Security Management Act of 2002*, http://csrc.nist.gov/policies/FISMA-final.pdf.

[28] United States Senate, *Health Insurance Portability and Accountability Act of 1997*.

[29] United States Senate, *Privacy Act of 1974*.