An Introduction to the Privacy Impact Assessment Based on ISO 22307

Haris Hamidovic, CIA, is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the NATO-led Stabilization Force (SFOR) in Bosnia and Herzegovina. He is the author of four books and more than 60 articles for business and IT-related publications. Hamidovic is a certified information technology expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

—Article 12, United Nations, Universal Declaration of Human Rights

Rapid advancements in computer technology make it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of data subjects. Furthermore, regulated industries, such as financial services, now place additional conditions on how personal information is collected, stored, shared and used.

New ways of using existing technology and new technologies bring new or unknown risks. It is advisable that corporations handling financial information be proactive in protecting and not abusing the privacy of their consumers and partners.

ISO 22307:2008, Financial services—Privacy impact assessment, recognizes that a privacy impact assessment (PIA) is an important financial services and banking management tool, used within an organization, or by contracted third parties, to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems (IS). This article will focus and comment on the ISO privacy standard and PIA in general. It will present common PIA components for institutions handling financial information that wish to use a PIA as a tool to plan for, and manage, privacy issues within business systems that they consider to be vulnerable.

PRIVACY LEGAL FRAMEWORK

A PIA can be seen as a subsystem of a larger system of privacy protection within the organization. A main element that affects the system of privacy protection, and all its parts, is the requirement of regulators and law.

Citizens, today more than ever, are fearful of what information is being gathered about them and by whom, what information is being shared about them and with whom, how that information is being used, and how long it is being retained. Privacy concerns have sparked debates and provoked legislators to enact laws both protecting and restricting privacy.

The Organization for Economic Co-operation and Development (OECD) has been a frontrunner in the privacy and security arenas and has contributed strongly to the development of the global legal framework. In 1980, the OECD developed its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines). Virtually all privacy legislation and directives find their foundation in this OECD document.

General principles from the OECD Privacy Guidelines include:

• Collection limitation principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

• Data quality principle—Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

• Purpose specification principle—The purposes for which personal data are collected should be specified no later than at the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes, or
such others, as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

• **Use limitation principle**—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.

• **Security safeguards principle**—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

• **Openness principle**—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, the main purposes of their use, and the identity and usual residence of the data controller.

• **Individual participation principle**—Individuals should have the right to:
  - Obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them
  - Have communicated to them data relating to them in an intelligible form, within a reasonable time and manner and at a charge that is not excessive. If such a request is denied, individuals should be able to challenge both the denial and the data relating to them. If the challenge is successful, the data should be erased, rectified, completed or amended within a reasonable time.

• **Accountability principle**—A data controller should be accountable for complying with measures that give effect to these principles.

In 1995, the European Union (EU) raised global awareness of privacy issues with the adoption of the EU Data Protection Directive. In adopting the directive, the EU wanted to ensure that “fundamental” privacy rights were protected when personal information was processed, regardless of the national citizenship of the individual data subjects and without restricting the free flow of personal information within the EU.

Largely because of the EU directive’s prohibition on the transfer of personal information to countries with inadequate legal protection—and the fear in many countries of the potential adverse economic impact that could result from the interruption of data flows from EU countries—a number of other countries have passed essentially identical national data protection legislation, in part, to ensure uninterrupted data flow from the EU. These countries can be roughly divided into two categories:

1. EU trading partners that wish to ensure that data flows will not be interrupted
2. Countries actively harmonizing their national legislation with the EU model in hopes of gaining membership in the EU

The EU Data Protection Directive went into effect in October 1998 and prohibits the transfer of personal data to non-EU countries that do not meet the European privacy standard for data protection. Although the US and the EU share the goal of enhancing privacy protection for their citizens, the US takes an approach to privacy that is different from that taken by the EU. The US uses a sectoral approach that relies on a mix of legislation, regulation and self-regulation. The EU, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies; registration of databases with those agencies; and, in some instances, prior approval before personal data processing may begin.

As a result of these different privacy approaches, the EU directive could have significantly hampered the ability of US companies to engage in many transatlantic transactions. To bridge the different privacy approaches and provide a streamlined means for US organizations to comply with the directive, the US Department of Commerce, in consultation with the European Commission, developed the so-called Safe Harbor Privacy Principles.

Generally, countries fall into one of three categories:

1. They have an omnibus data protection law.
2. They follow a sectoral approach and often let the private sector resolve these issues.
3. They have no privacy laws at all.

Most developing countries fall into the last category. The US falls into the middle category, and the EU has the more regulatory approach of the first category.

Privacy impact assessments are not used in all jurisdictions with data or privacy protection regulation. Many exercises, which are called privacy impact assessments, are, however, little more than legal compliance checks.
PRIVACY COMPLIANCE

Good privacy is good business. Good privacy practices are a key part of corporate governance and accountability. One of today’s key business imperatives is maintaining the privacy of personal information.9

Becoming privacy-compliant is a process. It requires adherence to a well-defined methodology, documentation of information, systems, data uses and requirements. The first step is to identify where the enterprise is, then determine where it should be and, finally, identify the path to get there. In between, numerous activities are required.

An adequate privacy compliance program can create or improve consumer trust and, thereby, impact sales and revenue. In addition, such a program can assist in mitigating law suits; surviving the court of public opinion; enhancing corporate branding; and improving the quality of corporate information on consumers, suppliers and employees through better management of personal information.10

A privacy compliance audit differs from a privacy impact assessment in that the compliance audit determines an institution’s current level of compliance with the law and identifies steps to avoid future noncompliance with the law. While there are similarities between PIAs and privacy compliance audits in that they use some of the same skills and are tools used to avoid breaches of privacy, the primary concern of a compliance audit is to meet the requirements of the law, whereas a PIA is intended to investigate further to identify ways to safeguard privacy optimally.11

PRIVACY IMPACT ASSESSMENT

A PIA is a tool that, when used effectively, can identify risks associated with privacy and help organizations plan to mitigate those risks. Recognizing that the framework for privacy protection in each country is different, the internationalization of privacy impact assessments is critical for global banking, in particular for cross-border financial transactions.12

ISO 22307:2008 states that objectives of a PIA should include:

• Ensuring that privacy protection is a core consideration in the initial considerations of a proposed financial system and in all subsequent activities during the system development life cycle

• Ensuring that accountability for privacy issues is clearly incorporated into the responsibilities of respective system developers, administrators and any other participants, including those from other institutions, jurisdictions and sectors

• Providing decision makers with the information necessary to make fully informed policy, system design and procurement decisions for proposed financial systems, based on an understanding of the privacy implications and risks and the options available for avoiding and/or mitigating those risks

• Reducing the risk of having to terminate or substantially modify a financial service after its implementation, to comply with privacy requirements

• Providing documentation on the business processes and flow of personal information for use and review by departmental and agency staff and to serve as the basis for consultations with clients, the privacy officers and other stakeholders

To meet these objectives, PIAs have common process elements that should be followed to be effective. The following are the six common elements that are required of any PIA process:13

• PIA plan
• Assessment
• PIA report
• Competent expertise
• Degree of independence and public aspects
• Use in the proposed financial system decision making

The following sections analyze each of these basic PIA elements.

PIA Plan

The PIA process requires a plan with a scope. This scope shall guide the PIA process for a specific proposed financial system (PFS). A PFS involves:

• A new financial system consisting of new or changed customer services and business processes
• New use of existing technology or technologies and infrastructure support systems, particularly those technologies and infrastructure systems that support the business processes involving collection, storage or access to personal information.

The PIA plan shall systematically establish the steps to be followed, questions to be answered and options to be examined for the PFS being assessed.

The identification of known and relevant risks to personal information is required. There may be risks to personal information other than those addressed by privacy laws and regulations. These include identity theft and pretexting. Identifying all known and relevant risks to personal information should precede any study or research, examination of alternatives to the proposed financial system, and the rendering of conclusions and recommendations.

The PIA plan should include a detailed description of the PFS, as defined by the scope. The business process and data flow diagrams need to identify how information flows through the organization as a result of a particular business activity or activities. At a minimum, the diagrams should identify, on a general level, the major components of the business processes and how personal information is collected, used, disclosed and retained through this process.

Assessment
Assessment should be performed within the scope defined by the PIA plan, using competent expertise. Business process and data flow analysis of the personal information used by the system(s) need to be performed.

ISO 22307:2008 requires that gap analyses be performed on privacy policy compliance and impact analyses be performed on infrastructure support and the security program.

Findings and recommendations should be determined for the PIA report.

PIA Report
The PIA report is a policy-level discussion of a PFS that summarizes the specific privacy implications and risks together with mitigation measures, as appropriate.

Competent Expertise
The PIA process for a PFS and its services should require competent expertise as directed by the financial institution. Competent expertise should be required throughout the PIA process, including the development of the PIA plan, the performance of the PIA assessment and the development of recommendations in the PIA report.

Competent expertise includes the following:
• Knowledge of the specific PFS and its business objectives, the PFS design and the system development life cycle methodologies applied by the financial services institution
• Knowledge of the privacy policies and compliance requirements relevant to the PFS, including legal expertise to provide advice and recommendations with respect to privacy and financial service authorities, institutional supervisory mechanisms, and potential conflicts in which multiple statutes or jurisdictions are involved
• Operational program and business design skills to examine proposals in terms of business flow and context, stakeholder analysis, public/private partnerships, governance structures, and feasibility in terms of mitigation strategies
• Knowledge of technologies and alternatives to be applied by the PFS, including technology and systems expertise to provide technical and systems advice on mainframe and legacy systems, Internet tools and system interfaces, information, security, technical architecture, and data flows
• Information and record-keeping skills, to provide advice on how records are kept and the retention of information

Degree of Independence and Public Aspects
The degree of independence should be balanced against corporate needs to protect trade secrets, and it could include:
• Access by a public supervisory body (e.g., government regulators)
• Public availability of edited versions
• Inclusion of the public

Use in the Proposed Financial System Decision Making
A PIA could be used in the following ways:
• The report needs to include present recommendations including alternatives.
• Decisions should be documented and attached to the report.

In a case of “privacy crisis,” PIA can help in the following ways:
• By providing an authoritative document of system privacy compliance and actions planned to mitigate compliance risks
• By providing a record that management exercised due diligence
POSSIBLE PROBLEMS
The following are examples of problems that may be identified by performing the PIA process:
- Unintended instances of personal information used in a manner that creates privacy policy compliance risks
- Misunderstandings of privacy compliance requirements
- Misunderstandings of strategic business plans and technology directions that are, or have the potential to become, privacy policy compliance risks

CONCLUSION
Privacy impact assessments are only valuable if they have, and are perceived to have, the potential to alter proposed initiatives in order to mitigate privacy risks. Where PIAs are conducted in a mechanical fashion for the purposes of satisfying a legislative or bureaucratic requirement, risk assessment, as a key element of PIA, is often omitted.

Privacy is an issue that cannot be presented without proper context. The natural connection between privacy and security is quite simple: Without security there is no privacy.

In many countries, because there is no legislative mandate to conduct privacy impact assessments and because the privacy commissioner can only recommend their completion, provision of assistance and guidance to those conducting PIAs is critical to having the PIA adopted.

PIAs and privacy compliance represent the subsystems of the wider system of privacy protection. Good privacy protection systems must include both elements.

While there are similarities between PIAs and privacy compliance audits, in that they use some of the same skills and seek to avoid privacy breaches, compliance audits are primarily directed toward existing systems to validate their compliance with required policies, standards and law. By contrast, a PIA is used at an early stage in the development of a PFS and is useful in identifying optimum privacy options and solutions. If a PFS introduces a change to an existing system, the most recent privacy compliance audit provides very useful information for assessing the impact of the PFS.

The PIA is a tool for addressing privacy issues in a system under development. To be effective, a PIA needs to be conducted as part of a formalized process. The PIA provides a way to ensure that a proposed new system under development complies with applicable laws and regulations governing customer and consumer privacy.

One way of proactively addressing privacy principles and practices is to follow a standardized privacy impact assessment process for a proposed financial system, such as the one recommended in ISO 22307:2008.

ENDNOTES
1 United Nations, Universal Declaration of Human Rights, General Assembly, 1948
3 ISO 22307 can be used to define the basic characteristics of PIA as a functional whole, in terms of the system’s theory, i.e., its elements, structure and purpose.
4 Westby, Jody R. (editor); International Guide to Privacy, American Bar Association, USA, 2004
7 Op cit, Westby
8 Ibid.
9 American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants, Generally Accepted Privacy Principles, CPA and CA Practitioner Version, 2009
11 Op cit, ISO 22307-2008
12 Ibid.
13 Ibid.