ISO 29100

HOW CAN ORGANIZATIONS SECURE ITS PRIVACY NETWORK?

www.pecb.com
Introduction

About ISO/IEC 29100

Why should PII be protected?

Consequences of not protecting PII

What are the Benefits of having a Privacy Framework?

Why is PECB a Worthy Choice?

Steps for Obtaining a PECB Certification

PRINCIPAL AUTHORS
Eric LACHAPELLE, PECB
Bardha AJVAZI, PECB
Fitim RAMA, PECB
During the past years, we have witnessed huge record losses because of many information security incidents involving personally identifiable information (PII) that have affected both individuals and organizations. Some examples of various incidents involve legal liability, identity theft, and recovery costs. Therefore, organizations should implement an international information security standard that provides guidelines on how to protect their privacy networks and PII, to align with the increased usage of information and communication technologies (ICT) that process PII.

In response to on-going privacy related incidents happening to large corporations, small companies, and to famous individuals, in 2011, ISO has developed the ISO/IEC 29100 Privacy framework and ISO 29101 Privacy framework architecture to provide a higher level framework for securing Personally Identifiable Information PII with Information and Communication Technology systems. Organizations can use these standards to design, implement, operate and maintain their ICT systems that will allow the protection of PII and improve organization’s privacy programs through industry best practices.

About ISO/IEC 29100

ISO/IEC 29100 is intended to be used by persons and organizations involved in designing, developing, procuring, architecting, testing, maintaining, and operating information and communication technology systems where privacy controls are required for the functioning of PII.

This privacy framework is developed with the purpose of serving as assistance to organizations to define their privacy safeguarding requirements related to all information involved through these attributes:

- by specifying a common privacy terminology;
- by defining the actors and their roles in processing PII;
- by describing privacy safeguarding considerations; and
- by providing references to known privacy principles for IT.

Although there are several existing standards related to security such as (ISO 27001, ISO 27002, and ISO 27018 etc.), ISO/IEC 29100 focuses more on the processing of PII.

PII is any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person.

Examples of PII are:
- First and last name
- Location information
- Credit card numbers
- Age
- Criminal record
The continually increased complexity of ICT systems have made it difficult for organizations to ensure that their privacy is protected, and with the high commercial use of PII, achieving compliance with various applicable laws has become harder nowadays.

Therefore, the ISO/IEC 29100 standard has eleven substantive privacy principles (presented in the chart below) that are developed to take account of applicable legal and regulatory, contractual, commercial and other relevant factors. All these principles are developed by a number of states, countries and different international organizations worldwide.

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

Besides that these principles can be used to guide, design, develop, and implement privacy policies and controls, they can also be used as a reference point in the monitoring and measurement of performance benchmarking and auditing aspects of privacy management programs in an organization.

Moreover, the basic elements that encompass the ISO/IEC 29100 Privacy Framework are presented in the figure below, which is taken from the WG5 in the ISO/IEC/FIDIS/ITU-T Joint Workshop on Identity Management Standards, Lucern, Switzerland, 2007. In addition, the figure shows that PII Providers and PII Receivers are identified as Actors. PII providers can be users of an information communication technology system, data owners or subscribers, whereas the application providers or administrators are known as the PII receivers. Privacy preferences are set by PII providers while the safeguarding controls are applied during the information lifecycle that include the collection, storage, usage, transfer and deletion of information.
Why is it important for the PII to be protected?

Personally identifiable information may include very confidential data that are intended only for restricted use. Their protection is crucial for the main purpose that nondisclosure of information may result in many consequences (see next section). The main reasons why organizations protect their PII are the following:

- to protect the PII principal's privacy
- to meet legal and regulatory requirements
- to practice corporate responsibility
- to increase consumer credibility, and
- to reduce the number of security breaches

*43% of companies have experienced a data breach in the last year, which is up 10% from a year ago.* Ponemon Institute report

Consequences of not protecting PII

Furthermore, by not taking serious considerations against protecting PII, many organizations may come across issues which will result in huge costs. When a security breach occurs, not only will the information be harmed, but it also causes a domino effect, in which case your clients or your client's clients may be damaged. This chain of destruction will bring many unintended problems to organizations, such as exaction of fines and court trials, dissatisfied stakeholders, an outrageous increase in disaster recovery costs, and last but not least harm of reputation. Below a list of only a few most recent incidents that have occurred in various organizations:
2014 Sony Pictures Entertainment Hack

• On November 2014, confidential information including information about employees, internal e-mails, executive salaries, copies of unreleased films etc. were exposed. It is believed that this cyberhack has cost Sony Pictures approximately $15 million damage recovery. In addition, the leak of information (especially e-mails between employees) has caused chaos between many well-known celebrities, and a high number of court trials have been sentenced.

2014 Home Depot Data Breach

• On September 2014, hackers had broken into an installed payment system which resulted in 53 million stolen customer e-mails and 56 million customer credit card accounts. It is believed that this incident has cost the company $34 million to overcome this situation.

2012 TD Bank Data Breach

• On March 2012, TD Bank experienced data breach of which as many as 260,000 customer’s personal information such as account information, Social Security numbers etc., were exposed, resulting in $625,000 settlement.

What are the Benefits of having a Privacy Framework?

Implementing and maintaining a Privacy Framework based on the ISO/IEC 29100 standard, has crucial benefits for every organization and individual dealing with personally identifiable information, such as:

• It serves as a basis for preferred additional privacy standardization initiatives, for example a technical reference architecture, the use of specific privacy technologies, an overall privacy management, assurance of privacy compliance for outsourced data processes, privacy impact assessments and engineering terms,
• It defines privacy safeguarding requirements as they relate to all personally identifiable information and communication systems,
• It is applicable on a wide scale and sets a common privacy terminology, defines privacy principles when processing PII, classifies privacy features and relates all described privacy aspects to existing security guidelines,
• It is closely linked to existing security standards that have been widely implemented into practice,
• It places organizational, technical, procedural and regulatory aspects in perspective and addresses system-specific matters on a high-level, and
• It provides guidance relating information and communication system requirements for processing personally identifiable information to contribute to the privacy of people on an international level.

Why should you use ISO/IEC 29100?

The ISO/IEC 29100 Privacy Framework serves as a base for other relevant standards that are internationally applicable and general in nature. In other words, this standard takes into account organizational, technical, procedural and regulatory matters, by setting common privacy terminology and principles. It also lists privacy features to be upheld in conjunction with security guidelines.

Moreover, a Privacy Framework will contribute to improvements in privacy, assistance in maintaining good governance, reducing overhead costs related to security, and serve as a good marketing strategy to promote your credibility with internationally known ISO standards.

These are only some of the reasons why every organization should highly focus on having security specialists who are certified in information security and have appropriate knowledge and experience to link data security with the company’s goals, in addition to working under the legal and regulatory requirements.
Why is PECB a Worthy Choice?

Implementation of the Privacy Framework with IMS2 methodology

Considering the well documented benefits of implementing a Privacy Framework based on ISO/IEC 29100, makes the proposal easier to decide on.

Most companies now realize that it is not sufficient to implement a generic, “one size fits all” privacy framework. For an effective response, with respect to maintaining the privacy framework, such a framework must be customized to fit to a company. A more difficult task is the compilation of a privacy framework that balances the requirements of the standard, the business needs and the certification deadline.

There is no single blueprint for implementing ISO/IEC 29100 that will work for every company, but there are some common steps that will allow you to balance the frequent conflicting requirements and prepare you for a successful certification audit.

PECB has developed a methodology (please see example below) for implementing a Privacy Framework; the “Integrated Implementation Methodology for Management Systems and Standards (IMS2)”, and it is based on applicable best practices. This methodology is based on the guidelines of ISO standards and also meets the requirements of ISO/IEC 29100.

IMS2 is based on the PDCA cycle which is divided into four phases: Plan, Do, Check and Act. Each phase has between 2 and 8 steps for a total of 21 steps. In turn, these steps are divided into 101 activities and tasks. This ’Practical Guide’ considers the key phases of the implementation project from the starting point to the finishing point and suggests the appropriate ‘best practice’ for each one, while directing you to further helpful resources as you embark on your ISO/IEC 29100 journey.
The sequence of steps can be changed (inversion, merge). For example, the implementation of the management procedure or documented information can be done before the understanding of the organization. Many processes are iterative because of the need for progressive development throughout the implementation project; for example, communication and training.

By following a structured and effective methodology, an organization can be sure it covers all minimum requirements for the implementation of the framework. Whatever methodology used, the organization must adapt it to its particular context (requirements, size of the organization, scope, objectives, etc...) and not apply it like a cookbook.

Steps for obtaining a PECB Certification

To ensure that organizations or individuals achieve planned and desired results, the following steps will serve as guidance on how to become **PECB Certified Lead Privacy Implementer**.

<table>
<thead>
<tr>
<th>For organizations:</th>
<th>For individuals:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.Implement the privacy framework</td>
<td>1.Participate in the training course</td>
</tr>
<tr>
<td>2.Perform internal audit and reviews</td>
<td>2.Register for the certification exam</td>
</tr>
<tr>
<td>3.Select preferred certification body</td>
<td>3.Sit for the certification exam</td>
</tr>
<tr>
<td>4.Perform a pre-assessment audit (optional)</td>
<td>4.Apply for the certification scheme upon successful exam completion and fulfillment of certification requirements (stated on our website)</td>
</tr>
<tr>
<td>5.Perform the stage 1 audit</td>
<td>5.Obtain certification</td>
</tr>
<tr>
<td>6.Perform the stage 2 audit (on-site)</td>
<td></td>
</tr>
<tr>
<td>7.Perform a follow-up audit (optional)</td>
<td></td>
</tr>
<tr>
<td>8.Register the certification</td>
<td></td>
</tr>
<tr>
<td>9.Assure continual improvement by conducting surveillance audits</td>
<td></td>
</tr>
</tbody>
</table>

For further details relating the types of trainings and certifications that PECB offers, please visit our website: [www.pecb.com](http://www.pecb.com)