27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Privacy, Cybersecurity and ISO 27001
How are they related?

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Introduction

Concerns about privacy are as old as mankind. From the protection of one's body and property in ancient times, it has become a strict connection with when, how, and to what extent data and information about a person are communicated to others. And, regardless of body, property, or information, privacy is subject to three critical factors.

First, while people have a desire to protect their privacy, they invariably choose to sacrifice it in exchange for perceived benefits, like money, prestige, or convenience, disregarding the potential dangers and losses. Second, the governments'/organizations' will to legislate over privacy is not always according to individuals' best interests; it is sometimes in the name of a "greater good."

And, finally, technology. As a key point in dealing with privacy, technology is increasingly providing the means for persons, organizations, and governments to gather, aggregate, and analyze more and more information in a faster way, making privacy breaches, accidental or intentional, increasingly severe and comprehensive.

On the other hand, this same technological environment, known as cyberspace, can provide solutions to help properly protect the privacy of individuals, organizations' business, and governments' affairs, while at the same time allow them to fully enjoy modern life securely. These solutions, together with other non-technological measures, are known as cyber security.

The purpose of this white paper is to present a view of how privacy concepts should be considered in cyberspace activities, and how standards and frameworks already available on the market can help direct, implement, operate, and improve cyber security in a comprehensive way.

What should be considered as privacy?

Although some meanings of privacy may be straightforward: "the state of being away from other people" or "the state of being away from public attention," the boundaries and content of what is considered private, and what constitutes an invasion of privacy, differ among cultures and individuals (some languages do not even have a specific word for "privacy"). However, these common themes often arise:

The right to be let alone: when a person chooses seclusion from the attention of others if he/she wishes to do so, including the state of being immune from scrutiny or being observed in private settings.

Limited access: the ability to participate in a group, regardless of its size, without having others collect information about them.

Control over information: the degree by which a person can have influence over information about himself/herself.

States of privacy: privacy is not a binary thing, having degrees related to how many people are "secluded" from oneself. Some common levels considered are ***solitude*** (complete separation from others), ***intimacy*** (only a pair or small group of individuals share a relationship), ***anonymity*** (when someone desires to be in public without being recognized), and ***reserve*** (when someone requires others to respect his/her need to restrict communication of information concerning himself or herself).

Secrecy: related to any information one wishes to conceal because, in his/her opinion, it has the potential to be used to his/her disadvantage.

It is important to note that although these concepts are mainly directed to people, they are applicable, in some degree, to organizations and governments as well (e.g., organizations and governments also have the desire to conceal information they judge can be used to their disadvantage).

Additionally, it is important to consider that privacy can be viewed as something absolute, since many times wrongdoers make use of privacy aspects to conceal their activities (that being one of the greatest arguments for those who want to limit privacy rights).

Risks to privacy in cyberspace

When we consider "cyberspace" as "the electronic world created by interconnected networks of information technology and the information on those networks," the Internet being its most remarkable example, and the current and expected levels of computational capacity, we can devise the following risk landscape:

Threat scenarios	Vulnerabilities	Risks
• Powerful and portable computing devices (e.g., smartphones, tablets, and laptops) increasingly facilitating information collection, aggregation, and dissemination • Increasing number of third-party relationships (e.g., connection and application providers) • Increasing concentration of cyberspace infrastructure (e.g., datacenters and communication backbones) • Laws and regulations compromising privacy • Professionalization of attackers (e.g., individual crackers and state-funded teams)	• Increasing number of people performing activities in the cyberspace • Increasing number of sources to collect data (e.g., IP cameras, biometric, GPS, RFID, etc.) • Uneducated/unaware users regarding cyberspace privacy • Lack of privacy protection concerns in applications / systems development • More valuable data being electronically stored and processed on a massive and centralized scale (e.g., data warehouses) • Information shared, combined, and linked together with greater frequency • Use of common credentials to access multiple systems	• Collection of information not required for primary purpose • Maintenance of information beyond rightful time of use • Disclosure of sensitive information about one's life or business • Promotion of incorrect information that compromises reputation • Identity theft • Applications / systems without proper privacy protection functionalities / controls

Note: The order in which the threat scenarios, vulnerabilities, and risks are presented does not mean that there is a specific or stronger link between certain items.

As you can see, while some risks in cyberspace are not much different from those in the physical world, the difference being in the speed the impact can spread and its magnitude, others are strictly related to this new technological environment, like application and systems risks.

One tricky thing about privacy risks is that since information value greatly depends on the context in which it is evaluated, some information considered harmless, when combined or aggregated with other information, can result in information with great damage potential.

The relations between cyber security and privacy protection

We can define cyber security as any measures taken to protect and secure online information, and the infrastructure on which it resides, from disruption or abuse. The main aspects to be protected are the confidentiality of information stored in Information and Communication Technologies (ICT), the integrity of that information, and the availability and reliability of the ICT.

Considering the previous definitions for cyber security and privacy concepts, we can see that cyber security is intrinsically related to privacy protection:

Cyber security	Privacy protection
Confidentiality of information stored in ICT	The most direct aspect of cyber security regarding privacy protection, encompassing all the discussed concepts (the right to be let alone, limited access, states of privacy, and secrecy).
Integrity of stored / processed information	This relation is more implicit, since the integrity of the rules established to control who has access to information and who can alter it must be preserved to ensure user privacy.
Availability and reliability of the Information and Communication Technologies (ICT)	ICT assets need to be available and reliable in providing the functionalities needed to ensure the proper control of privacy.

These relations can be used as more appealing examples of advantages of implementing cyber security, instead of those more commonly used as “process organization,” “market advantage,” “cost reduction,” etc., which lack focus on specific results and make it harder for interested parties to support security initiatives.

Basic principles of implementing cyber security to support privacy protection

For a proper implementation of cyber security in a way it can support privacy protection, the following objectives should be considered:

Personal autonomy: a person should be capable to make his/her own choices and not be subjected to arbitrary decisions.

Self-evaluation and decision making: a person should be given sufficient, relevant, and proper information and knowledge to evaluate when it is appropriate to relinquish his/her privacy rights.

Need for limited and protected communication: a person requires opportunities to share confidences with other people of his/her choice.

In practical terms, these objectives can be fulfilled in a cyber security environment by:

- Explicit definition of privacy needs and expectations;
- Development of applications and systems based in solid requirements and frameworks;
- Education, training, and awareness of people concerning privacy aspects in cyberspace.

.

Practical tools that help cybersecurity implementation for protecting privacy

And, as in any implementation, selecting the proper framework can save you a lot of trouble and hard work, and for cyber security one of the main sources of good practices are the standards of the ISO 27000 family:

- ISO 27001 (requirements for information security systems management): provides a general framework to help protect information, including privacy aspects. See more information in this article: What is ISO 27001?
- ISO 27032 (guidelines for cyber security): provides guidance for improving the state of cyber security, considering the various security domains, like information security, network security, internet security, and critical information infrastructure protection (CIIP).

As support standards, you should consider:

- ISO 27002: (code of practice for information security controls) provides detail on how to implement security controls defined in ISO 27001 Annex A. See more information in this article: ISO 27001 vs. ISO 27002 .
- ISO 27017 (code of practice for information security controls for cloud services): provides details on controls specifically related to cloud services. See more information in this article: ISO 27001 vs. ISO 27017 – Information security controls for cloud services.
- ISO 27018 (code of practice for information security controls related to the protection of Personally Identifiable Information – PII): provides details on controls specifically related to protection of Personally Identifiable Information – PII. See more information in this article: ISO 27001 vs. ISO 27018 – Standard for protecting privacy in the cloud.

Since you can perform the implementation of cyber security as part of an information security project, you can follow the same steps considered for the implementation of an Information Security Management System (ISMS), as demonstrated in this Diagram of ISO 27001:2013 Implementation, which can be summarized as:

- Obtaining management (and interested parties) support
- Defining requirements
- Defining risks to be treated
- Defining cyber security architecture (process, technologies, competencies development, etc.)
- Implementing cyber security controls

- Operating and evaluating controls performance

Good privacy practices for user

From market good practices, and the previous presented standards, these can be considered more practical examples applicable to users:

Verify services for privacy policies: if an organization does not have an explicit policy related to how they protect your personal information, it is not a good sign about how they handle sensitive information. This same rule is applicable to apps you install on your devices.

Think before you post: in social networks, forums, and chats, post only strictly needed information, because search engines can correlate and aggregate random posts, messages, and profiles and get information you don't want them to have.

Make use of anonymity: when it is not essential for you to identify your sensitive information, make use of credentials with no Personally Identifiable Information, or solutions to navigate anonymously, like TOR.

Protect your device and communications: make sure to install and maintain firewall, cryptographic (e.g., veracrypt and VPN), and anti-malware solutions on your device. The first one prevents your device from being hacked and from remote attacks, the second one helps protect your stored data and data in transit, and the last one can prevent the use of malwares to track your browsing habits. To prevent direct access to them (in case they are stolen), make sure to set passcodes to access them every time you use them. And, finally, avoid at any costs making use of open Wi-Fi communication, and if you have to use it, do not send sensitive information. ISO 27002 can help you with more detailed information in controls 6.2.1 – Mobile device policy, 6.2.2 – Teleworking, and 12.2.1 – Controls against malware.

Use cryptographic solutions in the cloud: today it is almost standard for cloud services to encrypt users' data to prevent unauthorized access. Even so, consider adding your own cryptographic solutions (send your data to the cloud already encrypted).

Set software for privacy: make sure to configure the privacy options available in the software you use. "Do not track me" and "delete history after log off" are some options you can find.

Use your passwords wisely: use different passwords among all services you join, especially those you use for encrypted or secure sites. Think about using password vault software, which generates and remembers strong and unique passwords, and two-factor authentication whenever available. ISO 27002 can help you with more detailed information in control 9.3.1 – Use of secret authentication information.

Follow your instincts: if you feel uncomfortable disclosing information, or think the information required is too intrusive, personal, or irrelevant to the service or content you are trying to obtain, don't do it.

Good practices for organizations and government

As the parties responsible for the cyberspace main infrastructure, and massive user databases, organizations and governments should be highly concerned about the protection of this sensitive information. In the text below you will see some practical examples applicable to organizations and governments that are supported by the previous presented standards. For more information about ISO 27001 and best practices for compliance, please see this ISO 27001:2013 Foundations Course.

Have (and follow) a privacy policy: an organization should have clear guidelines for its users and employees about what information is collected, for what purpose, how it is used, for how long it is kept, and how it is protected. Note that these guidelines shall be compliant with local laws and regulations, so you will need to map these legal requirements, too. ISO 27002 can help you with more detailed information in control 5.5.1 – Policies for information security, and 18.1.1 – Identification of applicable legislation and contractual requirements. For more information about policies development, please see this article: Seven steps for implementing policies and procedures.

Know what you have: a data inventory should be available to tell an organization all the personal information it has about users, who is responsible for it, and who can have access to it. ISO 27002 can help you with more detailed information in controls 8.1.1 – Inventory of assets, 8.1.2 – Ownership of assets, and 9.1.1 – Access control policy. For more information about the asset inventory, please see this article: How to handle Asset register (Asset inventory) according to ISO 27001.

Include privacy requirements in the application / systems development process: simple requirements such as privacy embedded into the design, least privilege user access, privacy as a default setting, and end-to-end security (e.g., from user to database) may be sufficient for software architects, developers, and programmers to understand that privacy concerns must be an essential part of application / system development and maintenance. ISO 27002 can help you with more detailed information in controls 14.1.1 – Information security requirements analysis and specification, 18.1.3 – Protection of records, and 18.1.4 – Privacy and protection of personally identifiable information. For more information about information systems requirements, please see this article: How to set security requirements and test systems according to ISO 27001.

Enforce policies: it is not because there is a policy in place that everyone will follow it. So, you should, whenever possible, ensure that following the policy is the only way to use the system. For example, if the system defines that the minimum password length is six characters, as established in the policy, there is no way a user can set a shorter password. ISO 27002 can help you with more detailed information in controls 6.2.1 – Mobile device policy, 6.2.1 – teleworking, 9.1.1 – Access control policy, 9.4.1 – Information access restriction, and 9.4.2 – Secure log-on procedures. For more information about policies enforcement, please see this article: Seven steps for implementing policies and procedures.

Provide means to educate users: privacy pages, newsletters, video training, and others forms of education should be considered to make users (e.g., clients, employees, third parties, etc.) aware of what they should do to protect their privacy and the privacy of others. ISO 27002 can help you with more detailed information in control 7.2.2 – Information security awareness, education and training. For more information about user training, please see these

articles: 8 Security Practices to Use in Your Employee Training and Awareness Program and How to perform training & awareness for ISO 27001 and ISO 22301.

Keep your infrastructure lean and updated: having only the minimal resources necessary to run the business, and updated concerning security patches, will minimize the attack surface someone can use to compromise your users' privacy. ISO 27002 can help you with more detailed information in control 12.5.1 – Installation of software on operational systems, 12.6.1 – Management of technical vulnerabilities, and 12.6.2 – Restrictions on software installation. For more orientation about operational software control, please see this article: Implementing restrictions on software installation using ISO 27001 control A.12.6.2.

Control changes: access of new or updated assets can compromise all your security efforts. Make sure that changes in your technological environment will not affect your security levels. ISO 27002 can help you with more detailed information in control 12.1.2 – Change management. For more information about change control, please see this article: How to manage changes in an ISMS according to ISO 27001 A.12.1.2.

Secure your network and communications: make sure that data from your users are kept safe while in transit (e.g., by the use of VPN, SSL, HTTPS, etc.). Even the organization's internal networks and communications should consider protective measures. ISO 27002 can help you with more detailed information in control 13.1.2 – Security of network services.

Be prepared for data breaches: these kinds of incidents are inevitable (your efforts will only make them less likely to happen), and you should be prepared to respond to them in the quickest and most proper way. A good response will not only minimize damage to users' trust, but may minimize legal problems by showing the organization's due care with users' sensitive data. ISO 27002 can help you with more detailed information in controls 16.1.1 – Responsibilities and procedures, and 16.1.5 – Response to information security incidents. For more information about incident handling, please see this article: How to handle incidents according to ISO 27001 A.16.

Periodic evaluation: by means of audits, vulnerability scans, and penetration tests, an organization can assess and evaluate the effectiveness of its security controls and make proper adjustments to maintain security levels. Simulation of data breaches also should be considered to evaluate the performance of response plans. ISO 27002 can help you with more detailed information in control 18.2.1 – Independent review of information security, 18.2.2 – Compliance with security policies and standards, and 18.2.3 – Technical compliance review. For more information about evaluation forms, please see this article: How to use penetration testing for ISO 27001 A.12.6.1.

Provide a communication channel: users do not want only to be told about what an organization proposes to protect their data. They want to ask questions and be heard about complaints. By making a page, phone number, e-mail, or some other forms of communication available, and responding to users' inputs, an organization can improve its image as a trustworthy data/information keeper. ISO 27001 can help you with more detailed information in clause 7.4 – Communication. For more orientation about communication procedures, please see this article: How to create a Communication Plan according to ISO 27001.

Please note that some of these previous examples also can be applicable to individual users, but are more recommended to organizations and governments because of the costs they can save due to the sheer data volume they handle.

Complementary material

As for documentation support, here are some documentation templates, available at Advisera:

Practice	Document name
Have (and follow) a privacy policy	List of Legal, Regulatory, Contractual and Other Requirements
Protect your device and communications	Mobile Device and Teleworking Policy Bring Your Own Device (BYOD) Policy
Know what you have	Inventory of Assets
Enforce policies	Access Control Policy
Enforce policies	Password Policy
Control changes	Change Management Policy
Include privacy requirements in the application / systems development process	Specification of Information System Requirements
Be prepared for data breaches	Incident Management Procedure
Periodic evaluation	Internal Audit Checklist

So, with some adjustments to your business context, these documents can be used as the basis for your organization's cyberspace and cyber security environment.

Check out ISO 27001 compliance software

To learn how to comply with ISO 27001, while also implementing privacy and cybersecurity controls, sign up for a 30-day free trial of Conformio, the leading ISO 27001 compliance software.

References

ADVISERA – 27001Academy (http://advisera.com/27001academy/)

Kosutic, D., 2012. 9 Steps to Cybersecurity - The Manager's Information Security Strategy Manual.

Westin, A. F., 1967. Privacy & Freedom.

OXFORD DICTIONARIES (http://www.oxforddictionaries.com/definition/english/privacy)

MERRIAM WEBSTER (http://www.merriam-webster.com/dictionary/privacy)

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting

Our offices:
Zavizanska 12, 10000 Zagreb, Croatia
Via Maggio 1 C, Lugano, CH-6900, Switzerland
275 Seventh Ave, 7th Floor, New York, 10001, U.S.

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020
Switzerland: +41 41 588 0722

EXPLORE **ADVISERA**

EUGDPR Academy · 27001 Academy · 9001 Academy · 14001 Academy · 45001 Academy · 13485 Academy · 9100 Academy

16949 Academy · 17025 Academy · 20000 Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.