Reducing Risk, Seizing Opportunity: A Security Industry Guide to Privacy

securityindustry.org

INTRODUCTION

Security technology firms play an important role in ensuring the privacy of personal information. This is both a responsibility and an opportunity, and it has the potential to either help or hinder business growth, depending on a company's actions.

This guide was developed with the goal not just of mitigating data breaches and other threats – as crucial as that is – but also recognizing and reinforcing the privacy rights of individuals. It sets a baseline for sound privacy practices, while also addressing the supply chain and its role in the data life cycle. It addresses basic and general privacy practices but does not cover topics that might be applicable only to specific security technologies, such as facial recognition.[1]

[1] This guide describes general recommendations and does not purport to address specific regulatory or legislative requirements or to offer legal advice. Individuals and companies should seek the guidance of qualified legal counsel, where appropriate.

Objective

It is critical for members of the security industry, particularly product engineers, integrators, consultants and others whose products, services and solutions manage, process or store personal information, to understand the interplay of design principles, policies, practices and procedures in securing – or failing to secure – privacy. This guide aims to:

- Describe general privacy principles
- Help members of the security industry to better understand privacy and its importance to stakeholders
- Identify practical steps that should be taken to protect privacy

Security professionals can use this information for multiple purposes, including:

- Ensuring the privacy of personal information that is handled by their own businesses
- Embracing privacy as a market differentiator and providing products and services to customers that ensure the protection of personal information
- For integrators and consultants, especially, becoming a trusted advisor to customers as privacy becomes more heavily regulated and more likely to be a cause of civil actions

Use

A major impact of an industry guide to privacy is the potential reduction in risk – business, operational, legal, liability, technical and reputational. Multiple privacy risks are specifically associated with the deployment of security and surveillance technologies and systems. These include, but are not limited to:

- Their role and relationship in the supply chain
- Appropriate purpose and justification
  - Legal requirements
- Measurement of risk and controls
  - Security of the security system itself
  - Insider threats
  - External data breaches (cybersecurity)
  - Accidental data breaches (e.g., social engineering, phishing, data leakage)
  - Lack of employee training

The potential misuse or failure to protect private information with which one has been entrusted adds another risk. Security professionals can use this guide to mitigate that risk not only for themselves, but also for end users who are seeking reliable, holistic solutions that free them to focus on their core business.

Principles

There are several core privacy principles at the foundation of many of the regulatory and legislative requirements throughout the world. Depending on the government under which a business operates, there are between six and 13 principles, with Australia, for example, espousing 13 and Europe's General Data Protection Regulation (GDPR) built on six. The following nine principles are common to most regimes. They are the basis of the recommendations in this guide and should inform privacy policies and practices that are developed by members of the security industry, whether for themselves or for customers.

- **Accountability** – Implement and deploy a structured and proactive approach to privacy management
- **Notice** – In all governance regimes, there is a notice requirement; for example, a sign notifying people of video surveillance being conducted
- **Purpose identification** – Consists of two elements: the specified and legitimate purposes for which the data is being collected and the justification for the processing of that data
- **Consent** – Include the concept of real choice so that individuals are not forced to accept one option before the collection of any personal or tracking information
- **Collection limitation** – Collect only that information that is required to achieve the business purpose and do not use the information for any other purpose
- **Use, disclosure and retention limitations** – Limit use of personal information to the specified purpose; retain information only as long as is necessary to fulfill the stated purpose (or as required by law); dispose of information in a safe and timely manner
- **Accuracy** – Take reasonable steps to ensure that personal data is accurate; offer data subjects the opportunity to correct errors

- **Security** – Protect personal information against unauthorized access or disclosure, both physical and logical, by implementing robust security practices
- **Transparency** – Communicate privacy practices in plain language, including what data is being collected, how the data is being used and with whom the data is being shared; inform data subjects of their rights and responsibilities

Recommendations

Privacy risks can lurk anywhere within an organization. A broad approach is necessary to enable companies to understand what data is being collected and when, where it is being stored and if it is being shared (and with whom), be it in sales, marketing, human resources or any other department. Once that information is identified, policies and procedures can be implemented to reduce risk.

The first step in protecting privacy is collecting the following information:

- What personal data is being collected?
- When is it being collected?
- Why it is being collected?
- Where it is being stored?
- When and how is it is being disposed of? (This includes both digital data and paper-based data)

With this data map in hand – along with a thorough understanding of the risks faced by the organization and other stakeholders, as well as applicable laws and regulations – ask the following questions:

- Is it necessary to collect this information? If yes, where should it be stored?
- Who should have access to the data and when?
- Should this data ever be shared and why?
- How long should the data be retained and how should it be disposed of?

After ensuring that only the data necessary for the business purpose is being collected, take steps to secure the data by controlling access to it both internally and externally:

- Establish strong authentication processes, including multifactor authentication
- Implement a password management policy that forces regular password changes
- Adopt the principle of least privilege for all
- Continuously monitor networks for unusual activity
- Layer networks and applications where possible; a flat network increases risk
- Encrypt the data; make sure the data is secure in transit, at rest and when archived
- Do not share the data with third parties if it is not necessary; when sharing, insist on formal agreements that require third parties to protect the data

Communicate openly and transparently with those from whom you are collecting data; use plain language to provide the following information:

- Why you are collecting the data
- The steps you are taking to protect the data
- What rights the data subject has (access, correction, redress)
- With whom you will share the data
- How long you will keep the data

When collecting data, obtain consent from the individual providing their personal information:

- Where possible, consent should be explicit, meaning the data subject signs a consent form or expresses consent in some other concrete way
- Security systems often preclude the ability to obtain explicit consent; in such cases, signs posted on or near the systems should alert users, in plain language, to the collection of personal data

Train employees, including operators and maintenance personnel, in data collection and privacy practices, as people are often the weakest link in any privacy/security protocol. At a minimum, training should occur during onboarding, after a major policy update and annually.

SUMMARY

This guide provides security companies with basic but important steps to minimize privacy risks for themselves and their customers and begin building a robust privacy program that can:

- Increase the scope of interaction with customers, employees and the supply chain
- Reduce liability
- Create and maintain a trusted brand image
- Improve customer relations
- Inherently address major aspects of legislation and regulations

With data breaches proliferating and privacy concerns growing, security companies can use this information to improve their own practices, as well as meet a critical need for their customers.

About the SIA Data Privacy Advisory Board

The SIA Data Privacy Advisory Board provides information and best practices to help SIA members handle sensitive data in a safe and secure manner to protect the personally identifiable information of their employees, partners and customers from potential breaches. The board leverages the collective expertise of industry professionals, law enforcement, security practitioners and data privacy experts to inform and educate SIA member companies about methods for mitigating the risk of data breaches.

SIA
SECURITY INDUSTRY ASSOCIATION

securityindustry.org