

Privacy—An Introduction to Generally Accepted Privacy Principles

Introduction

Many organizations find challenges in managing [privacy](#)¹ on local, national, or international bases. Most are faced with a number of differing privacy laws and regulations whose requirements need to be operationalized.

Generally Accepted Privacy Principles (GAPP) has been developed from a business perspective, referencing some, but by no means all, significant local, national, and international privacy regulations. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance in an organization. Illustrative policy requirements, communications, and controls, including monitoring controls, are provided as support for the criteria.

GAPP can be used by any organization as part of its [privacy program](#). GAPP has been developed to help management create an effective privacy program that addresses privacy risks and obligations, and business opportunities. It can also be a useful tool to boards and others charged with governance and providing oversight. This introduction includes a definition of privacy and an explanation of why privacy is a business issue and not solely a compliance issue. Also illustrated is how these principles can be applied to [outsourcing](#) scenarios and the potential types of privacy initiatives that can be undertaken for the benefit of organizations and their customers.

This introduction and the set of privacy principles and related criteria that follow will be useful to those who

- oversee and monitor privacy and security programs.
- implement and manage privacy in an organization.
- implement and manage security in an organization.
- oversee and manage risks and compliance in an organization.
- assess compliance and audit privacy and security programs.
- regulate privacy.

¹ The first occurrence of each word contained in appendix A—Glossary is underlined and hyperlinked back to its definition in the glossary in the introduction section and in the *Generally Accepted Privacy Principles* and related criteria tables.

Why Privacy Is a Business Issue

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](#). As business systems and processes become increasingly complex and sophisticated, organizations are collecting growing amounts of personal information. As a result, personal information is vulnerable to a variety of risks, including loss, misuse, unauthorized access, and unauthorized disclosure. Those vulnerabilities raise concerns for organizations, governments, and the public in general.

Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. Governments are trying to protect the public interest and, at the same time, manage their cache of personal information gathered from citizens. Consumers are very concerned about their personal information, and many believe they have lost control of it. Furthermore, the public has a significant concern about identity theft and inappropriate access to personal information, especially financial and medical records, and information about children.

Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, all businesses need to effectively address privacy as a risk management issue. The following are specific risks of having inadequate privacy policies and procedures:

- Damage to the organization's reputation, brand, or business relationships
- Legal liability and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer or employee distrust
- Denial of [consent](#) by individuals to have their personal information used for business [purposes](#)
- Lost business and consequential reduction in revenue and market share
- Disruption of international business operations
- Liability resulting from identity theft

International Privacy Considerations

For organizations operating in more than one country, the management of their privacy risk can be a significant challenge.

For example, the global nature of the Internet and business means regulatory actions in one country may affect the rights and obligations of individual users and customers around the world. Many countries have laws regulating transborder data flow, including the European Union's (EU) directives on data protection and privacy, with which an organization must comply if it wants to do business in those countries. Therefore, organizations need to comply with changing privacy requirements around the world. Further, different jurisdictions have different privacy philosophies, making international compliance a complex task. To illustrate this, some countries view personal information as belonging to the individual and take the position that the enterprise has a fiduciary-like relationship when collecting and maintaining such information. Alternatively, other countries view personal information as belonging to the enterprise that collects it.

In addition, organizations are challenged to try and stay up to date with the requirements for each country in which they do business. By adhering to a high global standard, such as those set out in this document, compliance with many regulations will be facilitated.

Even organizations with limited international exposure often face issues of compliance with privacy requirements in other countries. Many of these organizations are unsure how to address often stricter overseas regulations. This increases the risk that an organization inadvertently could commit a breach that becomes an example to be publicized by the offended host country.

Furthermore, many local jurisdictions (such as states or provinces) and certain industries, such as healthcare or banking, have specific requirements related to privacy.

Outsourcing and Privacy

Outsourcing increases the complexity for dealing with privacy. An organization may outsource a part of its business process and, with it, some responsibility for privacy; however, the organization cannot outsource its ultimate responsibility for privacy for its business processes. Complexity increases when the [entity](#) that performs the outsourced service is in a different country and may be subject to different privacy laws or perhaps no privacy requirements at all. In such circumstances, the organization that outsources a business process will need to ensure it manages its privacy responsibilities appropriately.

GAPP and its supporting criteria can assist an organization in completing assessments (including independent examinations) about the privacy policies, procedures, and practices of the third party providing the outsourced services.

The fact that these principles and criteria have global application can provide comfort to an outsourcer that privacy assessments can be undertaken using a consistent measurement based on internationally known fair information practices.

What Is Privacy?

Privacy Definition

Privacy is defined in *Generally Accepted Privacy Principles* as “the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.”

Personal Information

Personal information (sometimes referred to as personally identifiable information) is information that is about, or can be related to, an identifiable [individual](#). It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are as follows:

- Name
- Home or e-mail address
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

Some personal information is considered sensitive. Some laws and regulations define the following to be [sensitive personal information](#):

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of sensitive information.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as *nonpersonal information*. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is deidentified or [anonymized](#). Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over nonpersonal information due to other regulations and agreements (for example, clinical research and market research).

Privacy or Confidentiality?

Unlike personal information, which is often defined by law or regulation, no single definition of confidential information exists that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a "need to know" basis. Examples of the kinds of information that may be subject to a [confidentiality](#) requirement include the following:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organization to organization and, in most cases, are driven by contractual arrangements. For additional information on criteria for confidentiality, refer to the AICPA and CICA *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (see www.aicpa.org/TrustServices or www.webtrust.org).

Introducing Generally Accepted Privacy Principles

GAPP is designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities.

The privacy principles and criteria are founded on key concepts from significant local, national, and international privacy laws, regulations, guidelines,² and good business practices. By using GAPP, organizations can proactively address the significant challenges that they face in establishing and managing their privacy programs and risks from a business perspective. GAPP also facilitates the management of privacy risk on a multijurisdictional basis.

Overall Privacy Objective

The privacy principles and criteria are founded on the following privacy objective.

Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in *Generally Accepted Privacy Principles* issued by the AICPA and CICA.

Generally Accepted Privacy Principles

The privacy principles are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

² For example, the Organisation for Economic Co-operation and Development has issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the European Union has issued Directive on Data Privacy (Directive 95/46/EC). In addition, the United States has enacted the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act. Canada has enacted the Personal Information Protection and Electronic Documents Act and Australia has enacted the Australian Privacy Act of 1988, as amended in 2001. A chart comparing these international privacy concepts with generally accepted privacy principles can be found online at www.aicpa.org/privacy. Compliance with this set of generally accepted privacy principles and criteria may not necessarily result in compliance with applicable privacy laws and regulations, and entities should seek appropriate legal advice regarding compliance with any laws and regulations.

The following are the 10 *generally accepted privacy principles*:

1. **Management**. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice**. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent**. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection**. The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal**. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access**. The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties**. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy**. The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality**. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement**. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

For each of the 10 privacy principles, relevant, objective, complete, and measurable criteria have been specified to guide the development and evaluation of an entity's privacy policies, communications, and procedures and controls. *Privacy policies* are written statements that convey management's intent, objectives, requirements, responsibilities, and standards. *Communications* refers to the organization's communication to individuals, [internal personnel](#), and [third parties](#) about its privacy notice

and its commitments therein and other relevant information. *Procedures and controls* are the other actions the organization takes to achieve the criteria.

Using GAPP

GAPP can be used by organizations for the following:

- Designing, implementing, and communicating privacy [policy](#)
- Establishing and managing privacy programs
- Monitoring and auditing privacy programs
- Measuring performance and benchmarking

Establishing and managing a privacy program involves the following activities:

- **Strategizing.** Performing privacy strategic and business planning.
- **Diagnosing.** Performing privacy gap and risk analyses.
- **Implementing.** Developing, documenting, introducing, and institutionalizing the program’s action plan, including establishing controls over personal information.
- **Sustaining and managing.** Monitoring activities of a privacy program.
- **Auditing.** Internal or external auditors evaluating the organization’s privacy program.

The following table summarizes and illustrates how GAPP can be used by an organization to address these business activities.

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
Strategizing	<p>Vision. An entity’s strategy is concerned with its long-term direction and prosperity. The vision identifies the entity’s culture and helps shape and determine how the entity will interact with its external environment, including customers, competitors, and legal, social, and ethical issues.</p> <p>Strategic Planning. This is an entity’s overall master plan, encompassing its strategic direction. Its objective is to ensure that the entity’s efforts are all headed in a common direction. The strategic plan identifies the entity’s long-term goals</p>	<p>Vision. Within an entity’s privacy effort, establishing the vision helps the entity integrate preferences and prioritize goals.</p> <p>Strategic Planning. Within an entity’s privacy effort, <i>Generally Accepted Privacy Principles (GAPP)</i> can be used to assist the organization in identifying significant components that need to be addressed.</p>

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
	<p>and major issues for becoming privacy compliant.</p> <p>Resource Allocation. This step identifies the human, financial, and other resources allocated to achieve the goals and objectives set forth in the strategic plan or business plan.</p>	<p>Resource Allocation. Using GAPP, the entity would identify the people working with and responsible for areas that might include systems management, privacy and security concerns, and stipulate the resourcing for their activities.</p> <p>Overall Strategy. A strategic document describes expected or intended future development. GAPP can assist an entity in clarifying plans for the systems under consideration or for the business’s privacy objectives. The plan identifies the process to achieve goals and milestones. It also provides a mechanism to communicate critical implementation elements, including details on services, budgets, development costs, promotion, and privacy advertising.</p>
Diagnosing	<p>This stage, often referred to as the assessment phase, encompasses a thorough analysis of the entity’s environment, identifying opportunities where weaknesses, vulnerability, and threats exist. The most common initial project for an organization is a diagnostic assessment. The purpose of such an assessment is to evaluate the entity against its privacy goals and objectives and determine to what extent the organization is achieving those goals and objectives.</p>	<p>GAPP can assist the entity in understanding its high-level risks, opportunities, needs, privacy policy and practices, competitive pressures, and the requirements of the relevant laws and regulations to which the entity is subject.</p> <p>GAPP provides a legislative neutral benchmark to allow the entity to assess the current state of privacy against the desired state.</p>
Implementing	<p>At this point, an action plan is mobilized or a diagnostic recommendation is put into effect, or both. Implementing involves developing and documenting a privacy program and action plan and the execution of all planned and other tasks necessary to make the action plan operational. It includes defining</p>	<p>GAPP can assist the entity in meeting its implementation goals. At the completion of the implementation phase, the entity should have developed the following deliverables:</p> <ul style="list-style-type: none"> • Systems, procedures, and processes to address the privacy

ACTIVITY	GENERAL DISCUSSION	POTENTIAL USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES
	<p>who will perform what tasks, assigning responsibilities, and establishing schedules and milestones. This involves the planning and implementation of a series of planned projects to provide guidance, direction, methodology, and tools to the organization in developing its initiatives.</p>	<p>requirements</p> <ul style="list-style-type: none"> • Updated privacy compliant forms, brochures, and contracts • Internal and external privacy awareness programs
Sustaining and managing	<p>Sustaining and managing involves monitoring the work to identify how progress differs from the action plan in time to initiate corrective action. Monitoring refers to the management policies, processes, and supporting technology to ensure compliance with organizational privacy policies and procedures and the ability to exhibit due diligence.</p>	<p>The entity can use GAPP to develop appropriate reporting criteria for monitoring requests for information, the sources used to compile the information and the information actually disclosed. It can also be used for determining validation procedures to ensure that the parties to whom the information was disclosed are entitled to receive that information.</p>
Internal privacy audit	<p>Internal auditors provide objective assurance and consulting services designed to add value and improve an entity's operations. They help an entity accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.</p>	<p>Internal auditors can evaluate an entity's privacy program and controls using GAPP as a benchmark and provide useful information and reporting to management.</p>
External privacy audit	<p>External auditors, notably certified public accountants (CPAs) and chartered accountants (CAs), can perform attestation and assurance services. Generally, these services, whether performed on financial and nonfinancial information, build trust and confidence for individuals, management, customers, business partners, and other users.</p>	<p>An external auditor can evaluate an entity's privacy program and controls in accordance with GAPP and provide reports useful to individuals, management, customers, business partners, and other users.</p>

Presentation of Generally Accepted Privacy Principles and Criteria

Under each principle, the criteria are presented in a three column format. The first column contains the measurement criteria. The second column contains illustrative controls and procedures, which are designed to provide examples and enhance the understanding of how the criteria might be applied. The illustrations are not intended to be comprehensive, nor are any of the illustrations required for an entity to have met the criteria. The third column contains additional considerations, including supplemental information such as good privacy practices and selected requirements of specific laws and regulations that may pertain to a certain industry or country.

Some of the criteria may not be directly applicable to some organizations or some processes. When a criterion is considered not applicable, the entity should consider justifying that decision to support future evaluation.

These principles and criteria provide a basis for designing, implementing, maintaining, evaluating, and auditing a privacy program to meet an entity's needs.