A Practice Note describing the privacy impact assessment (PIA) process, including how, when, and why to conduct a PIA. This note explains how conducting PIAs represents an important tool for implementing privacy by design programs and can help organizations mitigate privacy risks.

Managing these different requirements and consistently ensuring proper consideration of different privacy risks can prove challenging for organizations both large and small. Instituting a company-wide privacy impact assessment (PIA) review process can help organizations identify, evaluate, correct, reconcile, and track privacy risks and compliance issues.

This note discusses:
• What PIAs are and how they contribute to the organization’s risk management program.
• Common PIA program elements.
• The general privacy principles and legal requirements that PIAs should consider when assessing privacy risks.
• Best practices for conducting PIAs.

Privacy Impact Assessment (PIA) Programs

The PIA is a business process that organizations use to identify, consider, address, and mitigate potential privacy issues raised by their technologies, products, systems, processes, or other similar activities (collectively, systems). It helps an organization proactively understand and address privacy issues by analyzing the system’s collection, generation, use, and storage of personal information.

Privacy considerations can vary widely among different systems (see Review System’s Privacy-Related Legal Requirements). Some may not raise any privacy considerations, like an application that automatically collects sensor data from ocean buoys. Some may have well known privacy issues with clear solutions, like collecting email addresses at a trade show to conduct a follow-up marketing campaign. Others may raise novel and difficult privacy questions, like implementing a new biometric gait analysis system to track individual employee performance on an assembly line.

Establishing an enterprise-wide PIA process that consistently asks key questions designed to identify and analyze privacy risks creates a clear framework to manage and track them. Documenting the review process through written PIA reports:
• Improves transparency within the organization.
• Helps demonstrate compliance efforts should questions later arise.

PIAs are typically a collaborative and iterative process that require cooperation among different internal groups (see Who Should Conduct the PIA). They usually start with the system sponsor completing a questionnaire or initial report. However, PIAs often require follow-up questions or in-person meetings to:
• Ensure a full understanding of the system’s personal information use.
• Discuss alternatives to mitigate risks.
• Resolve issues.

While they often conclude with a final report and recommendation, most PIA processes require the participants to revisit their conclusions periodically or when system or other technology changes occur (see Common PIA Elements).
**PIA Program Benefits and Legal Requirements**

Formal PIA programs form a cornerstone of effective privacy by design programs and provide many benefits, including:

- Identifying potential privacy issues early in the development process, when system redesigns or revisions may prove easier and save time, money, and effort.
- Mitigating risks, which can lead to:
  - Reduced personal information data breach costs
  - Avoiding potential reputational harm or adverse publicity
  - Improved customer relationships and trust
  - Demonstrating and documenting compliance with privacy laws or corporate policies.
- Increasing privacy awareness within the organization.
- Improving transparency and compliance.
- Ensuring consideration of the customer’s or end user’s perspective during the development process.
- Improving consumer trust and loyalty.

For more on privacy by design programs, see Practice Note, Developing a Privacy Compliance Program: Box, Privacy by Design.

**Legal Requirements to Conduct PIAs**

The U.S. does not have a comprehensive data protection law that regulates consumer data privacy protection. Private U.S. organizations therefore are not under a general legal obligation to conduct PIAs. However, some new state consumer privacy laws with January 1, 2023 effective dates contain provisions requiring impact assessments before engaging in processing activities that may present a heightened risk of consumer harm or disparate impacts (Va. Code Ann. § 59.1-580 and Cal. Civ. Code § 1798.185(a)(15)(B); see Quick Comparison Chart (CPRA and VCDPA)).

The Federal Trade Commission (FTC) serves as the primary federal consumer privacy regulator under its statutory authority to regulate unfair or deceptive business practices (15 U.S.C. § 45). The FTC can take action against companies that:

- Fail to apply reasonable security measures that cause or are likely to cause significant consumer harm.

(See Practice Notes, U.S. Privacy and Data Security Law: Overview: FTC Act and FTC Data Security Standards and Enforcement.)

Conducting PIAs can help an organization mitigate potential FTC enforcement risks by ensuring that:

- Actual practices match its privacy and data security claims.
- Proposed systems do not create risks that may harm consumers or other individuals.

The FTC also issues general privacy guidance and reports that establish best practices and create a common understanding of privacy expectations. The FTC’s current guidance does not direct organizations to implement a PIA system. However, its general privacy best practices do strongly encourage companies to maintain comprehensive data management procedures throughout the life cycle of their products and services (see FTC Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, page 30-32 (Mar. 2012)). Organizations commonly implement PIA programs to help them meet and operationalize this FTC recommendation.

FTC consent orders settling privacy investigations often require the company to implement a comprehensive privacy program that regularly assesses and manages privacy risks (see Practice Note, U.S. Privacy and Data Security Law: Overview: Enforcement).

**Federal Agencies**

Section 208 of the E-Government Act of 2002 requires federal agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates personal information (44 U.S.C. § 3501).

Congress passed the E-Government Act to promote the use of internet-enabled government services and to make the federal government more transparent and accountable, especially regarding personal information use.

Guidance issued to help federal agencies understand their privacy obligations under the E-Government Act includes:

- Office of Management and Budget (OMB)’s general resources, such as:
Conducting Privacy Impact Assessments

- Managing Information as a Strategic Resource (OMB Circular A-130, July 28, 2016)
- National Institute of Standards and Technology (NIST) resources, such as:
  - NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Special Publication 800-122, Apr. 2010), which outlines a risk-based approach and provides specific recommendations for federal agencies
  - NIST Privacy Engineering: Risk Model and Assessment (June 28, 2017)
- Internal agency guidelines, such as:
  - The Department of Homeland Security (DHS) Privacy Impact Assessment Guidance
  - The Department of Justice (DOJ) Privacy Compliance Process

Federal agencies publicly post completed PIAs on their websites. To view internal reports documenting PIAs conducted by select federal agencies, see:

FTC: Privacy Impact Assessments
- DHS: Privacy Compliance Process
- DOJ: Privacy Impact Assessments
- Department of Health and Human Services: Privacy Impact Assessments

While the E-Government Act only applies to federal agencies, private organizations can look to the federal agency guidance and PIA template resources when developing their own programs.

NIST also developed a voluntary privacy framework designed to help private and public organizations understand, address, and improve privacy practices by operationalizing privacy by design concepts (see The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Version 1.0) (January 2020)).

International Considerations and Data Protection Impact Assessments

Organizations with customers, vendors, or operations outside the U.S. can significantly benefit from establishing internal processes that require PIAs for all systems using personal information collected from international sources. Other jurisdictions typically have comprehensive data protection laws that govern personal information processing, imposing different, often stricter, conditions, such as:

- Requiring prior explicit user consent for:
  - Certain data collection techniques, such as the use of website cookies
  - The collection and use of sensitive or special personal information
- Limiting personal information processing to approved legal grounds.
- Allowing individuals to access personal information held about them and, in some countries, correct or erase that personal information and object to and restrict further processing.
- Restricting transfers of personal information to other countries without adequate protections.

Privacy regulators outside of the U.S. have long encouraged companies to evaluate and manage privacy risks through PIAs (see Box, Data Protection Authority Resources on Conducting PIAs and DPIAs). Conducting PIAs can help a U.S. organization understand their unique risks when collecting or using personal information outside the U.S., such as:

- Determining what law applies to the data.
- Identifying restrictions or requirements that differ from those in the U.S.
- Identifying any data localization or cross-border transfer restrictions.

Some non-U.S. laws may also require an impact assessment in specific circumstances. For example, the EU’s comprehensive data protection law requires data controllers to conduct a data protection impact assessment (DPIA) before engaging in data processing activities likely to result in a high risk to the rights and freedoms of natural persons (Article 35, General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)). At a minimum, the DPIA must contain:
Conducting Privacy Impact Assessments

• A systematic description of:
  – The proposed processing operations
  – The processing purposes
  – The data controller's legitimate interest in conducting the activity
  – An assessment of the necessity and proportionality of the processing operations in relation to the stated purposes.
  – An assessment of the risks to the rights and freedoms of data subjects.
• The measures the organization expects to use to address identified risks, including appropriate:
  – Safeguards
  – Security measures
  – Mechanisms to protect the personal information and to demonstrate compliance with the GDPR, considering the rights and legitimate interests of data subjects and other persons concerned

For more on the GDPR's specific DPIA requirements, see Practice Note, Overview of EU General Data Protection Regulation: Data protection impact assessment. See the Data Protection Global Guide for additional information on privacy and data protection laws in other selected foreign jurisdictions.

PIAs and Data Security Risk Assessments

Many organizations routinely conduct data security risk assessments that evaluate the security of information technology (IT) systems and protect against hacking or other cyber attacks. Organizations need adequate security controls to ensure privacy, so privacy and security concerns naturally overlap.

However, privacy laws and protections focus on more than just data security and address, for example, obtaining an individual's notice and consent for collecting personal information, the business's purpose for processing personal information, or how and why a system uses personal information. Similarly, an organization's data security concerns cover its IT infrastructure and all the different confidential data types that the organization holds, not just personal information.

While PIAs and data security risk assessments may sometimes overlap, they serve two distinct purposes and address different organizational concerns. They also often work together. For example, a PIA might:

• Identify specific privacy risks that unauthorized access to a system can cause, like identity theft or financial losses.
• Require specific safeguards, like implementing employee access restrictions or setting a specific data sensitivity classification to mitigate those risks.
• Order a yearly data security risk assessment to evaluate whether the system's technical security controls correctly restrict access to the persons approved in the PIA or provide adequate protections for the established sensitivity classification.

For more on conducting data security risk assessments, see Practice Note, Data Security Risk Assessments and Reporting and Performing Data Security Risk Assessments Checklist.

When to Conduct a PIA

Systems can benefit from conducting a PIA at any time. However, the most effective PIAs occur at natural points in the development cycle, when they have a better chance to influence system strategy and direction. Organizations should consider conducting PIAs when:

• Developing new product or service offerings.
• Considering new internal process, system, or technology implementations.
• Conducting updates or major revisions to products, services, or internal systems.
• Processing sensitive personal information.
• Expanding into new territories or locations.
• Materially changing the type of personal information the system collects, generates, uses, or stores.
• Existing systems with significant personal information use have not received a comprehensive review within a reasonable time frame.
• Engaging third-party vendors who will access or otherwise handle personal information for the organization.

Who Should Conduct the PIA

Organizations with a dedicated privacy team or office typically designate that team to design, lead, and supervise the PIA process. However, organizations can also fit the PIA process into their existing compliance or security assessment processes. When designating an internal group or executive to lead the PIA process, consider the organization's:
Conducting Privacy Impact Assessments

• Structure
• Size
• Culture

For more on different organizational approaches to privacy compliance and privacy office structures, see Practice Note, Developing a Privacy Compliance Program.

While the privacy office may lead the PIA process, effective PIA implementations usually require input and support across different business functions, including:

• The system sponsor or business team implementing the system.
• Legal or privacy compliance groups.
• Information security or IT groups.
• Related business units, for example, the procurement group if the system involves third-party vendors.
• Other relevant stakeholders, for example, union or other employee representatives if the system involves workplace monitoring.

The review team should also engage executive management whenever necessary to ensure that the organization addresses potential risks at the appropriate level, especially when the PIA reveals high or unusual privacy risks.

Common PIA Elements

There are many ways to structure a successful PIA program. The best PIA processes:

• Fit seamlessly within an organization's structure and culture.
• Enable frank and clear conversations about how to address the organization's unique privacy risks.

Large or diverse organizations operating in different countries or with multiple services or product lines might require a highly structured and scalable process run through an integrated software tool. A smaller organization with one primary product line that does not use personal information might establish a more informal process, relying on self-service checklists to flag high-risk activities.

Similarly, organizations that primarily use personal information for internal functions like human resources or marketing may choose a more informal process. While organizations whose core products or services involve processing sensitive personal information, like electronic health records, may require more structured tools. Organizations of all sizes or in industries with low privacy risks can benefit from even a simple checklist that helps employees consider the potential privacy impact of their projects and actions.

When designing the organization’s PIA program, consider its:

• Privacy risk profile, including:
  – The amount of personal information the organization collects, uses, or stores
  – The sensitivity of personal information that the organization uses
  – The importance of personal information to the organization’s core operations
  – Sector- or industry-specific privacy risks and obligations (see Sector-Specific Requirements)
• Maturity
• Size and geographic scope
• Regulatory profile

PIA programs should aim to:

• Ensure compliance with applicable privacy-related legal, regulatory, and policy requirements.
• Identify the risks and effects of collecting, generating, using, sharing, and storing personal information.
• Evaluate potential protections and alternative processes to mitigate identified privacy risks.

PIA processes typically involve:

• Conducting a threshold privacy review (see Threshold Privacy Review).
• Clearly describing the system under review (see Detailed System Description).
• Identifying applicable laws or other privacy requirements (see Review System’s Privacy-Related Legal Requirements, Consider Company-Specific Privacy Restrictions, and Consider General Privacy Principles).
• Analyzing the system’s potential privacy risks (see Conduct Privacy Analysis).
• Mitigating the system’s potential privacy risks, when possible (see Mitigate Identified Risks).
• Tracking and confirming completion of any required mitigation actions or system revisions (see Reflection and Feedback).
Conducting Privacy Impact Assessments

For a model PIA report, see Standard Document, Privacy Impact Assessment. For additional PIA tools and resources, see Box, Data Protection Authority Resources on Conducting PIAs and DPIAs.

Threshold Privacy Review

Not every corporate system may need or benefit from a PIA, particularly if it does not involve personal information or otherwise trigger significant privacy impacts. Most PIA processes begin with a smaller screening evaluation, known as a threshold privacy review (TPR).

A TPR typically presents the system sponsor with a small set of basic questions designed to:

• Understand the system's general scope.
• Determine need for a more detailed PIA.

The questions typically:

• Request a brief system overview.
• Identify the personal information or tracking activities that the system uses.
• Determine whether the system leverages previously approved privacy notices, processes, IT systems, or vendors.

The TPR should allow the system reviewer to quickly and easily screen out systems with no or minimal privacy implications. Organizations that establish standard operating procedures for repetitive activities with privacy impacts can also use the TPR to screen out pre-cleared activities, while sending outliers or exceptions through the full PIA process.

For a model TPR, see Standard Document, Threshold Privacy Review.

Detailed System Description

Properly identifying and mitigating privacy risks first requires a clear and accurate system description. Documenting the system’s personal information use is one of the PIAs core tasks. The required information typically falls into three primary categories, which are:

• What personal information the system collects, generates, uses, shares, or stores (see Identify System’s Personal Information and Categorize System’s Personal Information).
• Why the system uses personal information (see Understand Personal Information’s Use Purpose).
• How personal information flows through the system (see Describe Information Flows).
• The system Sponsor usually prepares the system description by answering questions designed to help identify personal information use. The Sponsor may also provide charts, data flow maps, database field lists, or other technical information that help the review team understand how the system uses personal information.

Some PIAs may require going beyond the written description or questionnaire answers to fully understand the system’s operation. Complex systems like customer relation management (CRM) or human resources (HR) software applications may also require more active involvement.

For example, the PIA reviews may require extensive demonstrations or other testing to understand different feature sets, data flows, and system actions. Reviewing a new third-party mobile application for internal use might require technical testing to identify what information the application accesses.

PIA reviewers should:

• Collaborate with the system Sponsor to ensure the system description provides a complete and accurate picture.
• Conduct in-person interviews to answer any follow-up questions.

Identify System’s Personal Information

PIA documentation should:

• Clearly identify how the organization defines personal information.
• Fully identify and describe the personal information that each system collects, generates, uses, shares, and stores.

Personal information, broadly defined, is information that an organization can use to identify, locate, or contact a specific individual either:

• Alone
• When combined with other information reasonably available to it

It often includes information that relates to an identifiable individual or expresses an opinion about that individual. However, the precise definition of personal information varies under different U.S. federal, U.S. state, and other national privacy and data security laws (see Review System’s Privacy-Related Legal Requirements).
State laws may also establish broader or narrower personal information definitions. For example, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) that will replace the CCPA starting January 1, 2023 both adopt broad personal information definitions that includes any information that directly or indirectly identifies, describes, or can reasonably link to a particular consumer or household, including inferences generated from other personal information (Cal. Civ. Code § 1798.140(o); see Practice Note, Understanding the California Consumer Privacy Act (CCPA): Personal Information). By contrast, Nevada’s online privacy law narrowly defines personal information to include only specific pieces of identifying information, like the person’s first and last name, address, Social Security number, or identifier used to contact that person (NRS 603A.320; see Nevada’s Personal Information Sales Opt-Out Law Checklist).

**Common examples of personal information include an individual’s:**

- Name
- Home or other physical address
- Email address
- Telephone number
- Social security number (SSN)
- Birth date or location
- Passport number
- Driver’s license number
- Financial account information, like bank account, credit card, or debit card numbers
- Credit history
- Personal characteristics, like:
  - Photographs
  - Fingerprints
  - Handwriting
  - Face geometry
- Other unique biometric data
- Precise geographic location
- Health or medical information

Data elements that on the surface may not seem like personal information can become personal information if the system transforms or connects them to an identifiable individual. For example, a data field tracking defective items as part of a quality assurance system may become personal information if the system connects that data to individual manufacturing line employees. Data generated by systems through inferences or algorithms that create profiles also can be personal information (see Describe Information Flows).

Organizations often use the personal information definition from their privacy-related policies when reviewing privacy-related risks. For an example of privacy-related corporate policies, see Standard Documents, Personal Information Protection Policy (Internal) and Website Privacy Policy.

The system description should err on the side of over-including data elements that may qualify as personal information. **This allows the PIA reviewers to:**

- Consider personal information use broadly.
- Narrow the personal information scope as they identify the privacy risks and laws that uniquely apply to that specific system.

The system description should also identify any anonymized or pseudonymized data so the PIA reviewers can consider:

- The effectiveness of the techniques used.
- The potential for re-identification.

True anonymization is often difficult to accomplish, and the PIA should carefully scrutinize anonymization claims. For more guidance on anonymizing personal information, see NIST: De-Identification of Personal Information (Interagency Report 8053, Oct. 2015) and NIST: De-identification.

Some PIA processes require the system Sponsor to identify all the data elements that system collects, generates, uses, shares, or stores. It then assigns the task of determining which data elements qualify as personal information to the PIA reviewers.

For more on the different federal and state personal information definitions, see Practice Note, U.S. Privacy and Data Security Law: Overview and State Data Breach Laws Protected Personal Information Chart: Overview.

For a comparison of personal information definitions from select countries, see Data Protection: Country Q&A Tool: Questions 3 and 11.

For a sample questionnaire to help assess an organization’s personal information collection and handling practices, see Standard Document, Privacy Audit Questionnaire.
Categorize System’s Personal Information

All personal information is not created equal. The nature or type of personal information often alters the system’s privacy requirements or risk assessment. Sectoral privacy laws may also apply to specific types of data, like health or financial information (see Sector-Specific Requirements and Activity-Specific Requirements).

Some types of personal information carry greater risks to both the organization and individuals if misused, lost, or stolen. For example, the username and password for a stolen bank account may lead to a significant financial loss, but a stolen list of postal addresses may not generate the same financial loss or consumer harm.

Laws outside the U.S. may also afford special protections or impose heightened obligations for categories of personal information considered sensitive, including:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Political opinions
- Trade union membership
- Sexual orientation
- Criminal records

For more on classifying personal information, see Practice Note, Developing Information Security Policies: Data: Information Classification and Risk-Based Controls.

Understand Personal Information’s Use

Purpose

System descriptions should also clearly identify:

- The system’s overall purpose
- How each personal information data element fits into or supports the system’s overall purpose

Evaluating and addressing privacy risks often requires understanding the purpose for collecting and using personal information. For example, some situations require the organization to notify the individual about the collection activities and processing purposes or to obtain consent (see Practice Note, Drafting Privacy Notices).

Drafting the appropriate privacy notices requires a clear understanding of the system’s purpose for using and collecting personal information.

Purpose limitation and data minimization also represent important ways to mitigate potential privacy harms (see Data Minimization). Understanding the system’s central purpose and core business goals helps the PIA review team craft appropriate mitigation strategies.

Describe Information Flows

Data maps represent a common method for identifying and describing how personal information moves through a system. They often include diagrams or other tools that help PIA reviewers visualize the system’s data flows. Organizations typically structure data maps by following the way information flows through the data life cycle:

- Collection
- Use
- Storage
- Transfer
- Destruction

The data map should answer questions like:

- Where does personal information enter and exit the system?
- Where does the system physically collect, store, and distribute personal information?
- How do people, both internal and external, access personal information?
- How does the system share or acquire personal information with other systems?
- How does the system restrict or track personal information access?
- When and how does the system delete personal information?

Data maps can answer these questions at an overview level, or they can provide detailed descriptions for each element. The system’s unique potential privacy risks will often impact the level of detail required. PIA reviewers should seek additional detail as part of the iterative PIA process when necessary.

The PIA’s description section should also explore all the different ways a system can acquire personal information. For example, systems can:

- Collect personal information directly from individuals.
- Collect personal information passively through data about individuals’ actions, including metadata.
- Collect personal information indirectly from third parties who provide information about other individuals.
- Generate personal information using other data that they collect through inferences or algorithms.
Conducting Privacy Impact Assessments

- Identify non-personal information by linking it to personal information in other systems or data sets.

To capture this information, the data map section describing the system’s collection points should specifically identify information sources, for example:
- Directly from the individuals.
- From a specific third party or other system.
- Generated automatically through observation or from an algorithm.

Fully understanding the data flows and sources allows the review team to:
- Identify and evaluate key privacy issues.
- Determine the content of any privacy notices that the system’s data collection activities may require (see Practice Note, Drafting Privacy Notices).

Generating a data flow map may also require the system Sponsor to work collaboratively with other stakeholders, especially when third-party vendors provide, support, or use the system. A data flow map generated in isolation, without input from relevant stakeholders, may not provide a full picture of how the system works or handles personal information.

Ensure the system sponsor identifies relevant:
- Geographic locations.
- People or groups of people who require personal information access.
- Other systems that receive or provide personal information to or from the system under review.
- Exit points where personal information can leave a system, including by individuals’ actions using features like report exports, file downloads, or printing physical copies.

For more on data mapping, see Practice Note, Drafting Privacy Notices: Preparing to Draft the Privacy Notice.

Review System’s Privacy-Related Legal Requirements

The PIA reviewers should use the system description to identify and consider what privacy-related legal requirements the system must meet.

Reviewers should consider, for example:
- General U.S. privacy requirements established by the FTC (see Practice Note, U.S. Privacy and Data Security Law: Overview: FTC Act).
- Industry or sector-specific requirements (see Sector-Specific Requirements).
- Privacy requirements or restrictions that may affect specific activities (see Activity-Specific Requirements).
- Laws from other relevant geographic locations (see Location-Specific Requirements and Cross-Border Personal Information Transfers).
- Internal restrictions from corporate statements, policies, or voluntarily adopted codes of conduct (see Consider Company-Specific Privacy Restrictions).
- Generally accepted privacy principles (see Consider General Privacy Principles).

A comprehensive review of privacy legal requirements is beyond the scope of this Note. For a general overview of U.S. privacy laws, see Practice Note, U.S. Privacy and Data Security Law: Overview.

Sector-Specific Requirements

Organizations operating in specific sectors should consider how sector-specific legislation may affect the system under review, including:

- Healthcare. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related amendments in the Health Information Technology for Economic and Clinical Health Act (HITECH) cover protected health information held by healthcare providers and other covered entities (see Practice Note, HIPAA Privacy Rule).
- Financial services. The Gramm-Leach-Bliley Act (GLBA) and related state laws and regulations cover the treatment of non-public personal information (NPI) held by financial institutions (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules).
- Consumer credit and background checks. The Fair Credit Reporting Act (FCRA) regulates the collection, dissemination, and use of consumer information by consumer reporting agencies (CRAs) (see Practice Note, FCRA Litigation: Key Issues and Considerations). State employment laws may also affect an employer’s personal information use for background checks (see Background Checks Toolkit).
- Education. Several federal and state laws regulate the use of students’ personal information, including:
  - The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g)
Conducting Privacy Impact Assessments

- The Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h)
- State statues like California’s Student Online Personal Information Protection Act (SOPIPA) (Cal. Bus & Prof. Code § 22584)
  - (See Practice Notes, Student Privacy: Education Service Provider Requirements and Student Privacy State Laws for Education Service Providers Chart: Overview.)

Activity-Specific Requirements

Some systems may also involve activities subject to specific laws or regulations or that require a heightened level of scrutiny because they involve sensitive data. PIA reviewers should consider the privacy concerns that certain activities or specific types of personal information may raise, including:

- Artificial Intelligence (see Practice Note, Artificial Intelligence Key Legal Issues: Overview)
- Biometrics (see Practice Note, Biometrics in the Workplace and Article, Biometrics Litigation: an Evolving Landscape)
- Children’s privacy (see Practice Note, Children’s Online Privacy: COPPA Compliance)
- Email marketing (see Practice Note, CAN-SPAM Act Compliance)
- Employee personal data (see Practice Notes, Privacy in the Employment Relationship and Best Practices for Data Privacy and Security in the HR Space and U.S. Employee Privacy Compliance Toolkit)
- Genetics (see Practice Notes, Discrimination Under GINA: Basics and GINA Compliance for Health and Welfare Plans)
- Internet of things (see Practice Note, The Internet of Things: Key Legal Issues)
- Mobile phone applications and precise location tracking (see Practice Note, Mobile App Privacy: The Hidden Risks)
- Social security numbers (SSN) (see State Social Security Number Protection Laws Chart: Overview)
- Telemarketing (see Practice Notes, Telephone Consumer Protection Act (TCPA): Overview and TCPA Litigation: Key Issues and Considerations)
- Tracking technologies and online behavioral advertising (OBA) (see Practice Note, Tracking Technologies: Privacy and Data Security Issues)
- Video privacy (see the Video Privacy Protection Act of 1988 (VPPA) (18 U.S.C. § 2710))
- Workplace monitoring (see Practice Note, Electronic Workplace Monitoring and Surveillance)

Location-Specific Requirements and Cross-Border Personal Information Transfers

PIA reviewers should also carefully look at where a system collects and stores personal information to consider the applicability of U.S. state or other national laws. For example, systems collecting personal information from California or Nevada residents must consider how new privacy laws in those states impact their systems (see Implementing the California Consumer Privacy Act (CCPA) Checklist and Nevada’s Personal Information Sales Opt-Out Law Checklist).

Similarly, a U.S.-based system that monitors an individual’s behavior occurring in an EU member state might need to consider the EU GDPR’s potential application (see Practice Note, Overview of EU General Data Protection Regulation: Territorial Scope).

The reviewers also should consider whether cross-border data transfer restrictions apply if the personal information crosses national borders from:

- The collection location to the storage location.
- The storage location to any later access point.

(See Practice Notes, Cross-Border Personal Data Transfers: Overview and Global Data Localization Laws: Overview.)

For example, an organization that relies on controller-to-processor standard contractual clauses (SCCs) to support personal information transfers from the EU to the U.S. may need the PIA reviewers to verify the SCCs can provide the level of adequate protection required under the GDPR or to identify specific supplementary measures required to protect the transferred personal data. See Legal Updates:

- Schrems II: controller to processor standard contractual clauses valid but EU-U.S. Privacy Shield invalid (ECJ)
- EDPB adopts recommendations on Schrems II and first dispute resolution decision at 41st Plenary Session
Conducting Privacy Impact Assessments

- EDPB and EDPS adopt joint opinions on European Commission’s draft sets of standard contractual clauses
- European Commission adopts final versions of standard contractual clauses under EU GDPR
- EDPB adopts final version of recommendations on supplementary measures for data transfers to third countries in response to Schrems II (50th Plenary)

For more on transferring personal data outside of the EU, see:
- Practice Note, Overview of EU General Data Protection Regulation: Cross-border data transfers
- GDPR Cross-Border Transfers Checklist
- EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker
- Article, Schrems II: FISA and EO 12333 Overview
- Article, EDPB Supplementary Measures Recommendations and German DPA Guidance Post Schrems II.

See the Data Protection Global Guide for additional information on privacy and data protection laws in selected non-U.S. jurisdictions.

Consider General Privacy Principles

Organizations may also want to review systems for alignment with generally accepted privacy principles and norms that customers or system users may expect it to follow. This supports the PIAs primary risk mitigation purpose, particularly when it helps identify system issues that may harm customer relationships if not properly addressed.

Privacy as an Individual Right

Some frameworks consider privacy an individual right with three core aspects, which are:

- **Communications privacy.** This addresses a person’s ability to maintain privacy in their conversations with others through postal mail, email, telephone calls, text, and similar communication channels. U.S. statutes that address this type of privacy include:
  - The Electronic Communications Privacy Act of 1986 (ECPA), which regulates electronic communications
  - The Computer Fraud and Abuse Act, which regulates unauthorized computer use and computer tampering

- **Information privacy.** This addresses a person’s ability to control information about them, including how others share and collect it. Intrusions to consider include:
  - Excessive or unexpected personal information collection
  - Disclosing personal information without consent
  - Otherwise misusing personal information
  - (See, for example, In re Goldenshores Technologies, LLC, FTC No. 132 3087 (Mar. 31, 2014) (FTC enforcement action against a flashlight app collecting mobile phone call data without clear notice).)

- **Physical privacy.** This addresses a person’s ability to maintain their own physical space. Systems that intrude on physical privacy should receive high scrutiny during the PIA process and are often subject to additional legal protections, such as those under Illinois’ Biometric Information Privacy Act (BIPA) (740 ILCS 14/1 to 14/99). Intrusions to consider include:
  - Actions that search or scan a person's home, possessions, or body
  - Surveillance activities
  - Biometric information uses
  - (See, for example, Neal v. Fairfax Cty. Police Dep’t, 812 S.E.2d 444 (Va. 2018) (police department’s passive use of automated license plate recognition (ALPR) systems

Consider Company-Specific Privacy Restrictions

The PIA should review the system for compliance with the organization’s internal policies and public statements on privacy and data security. The FTC may consider enforcement actions when public statements do not match actual practices (see Legal Requirements to Conduct PIAs).

PIAs should also identify whether the organization participates in any applicable self-regulatory industry codes of conduct or other voluntary programs, such as:

- The Asia-Pacific Economic Cooperation (APEC) forum’s Cross-Border Privacy Rules (CBPR) system (see CBPRS: Cross Border Privacy Rules System)

Participation in voluntary programs may require the organization to adopt specific privacy-related policies or offer choices not strictly required under U.S. laws, such as a free independent recourse mechanism for privacy complaints.
could violate Virginia’s Data Act, which regulates unnecessary collection and storage of personal information by government agencies.)

The PIA’s analysis section should consider the system’s potential effects on each of these different privacy aspects.

**OECD Privacy Guidelines**

The Organization for Economic Co-operation and Development (OECD) published one of the first global privacy frameworks in 1980, which it updated in 2013 (OECD Privacy Guidelines (2013)). The OECD developed the Privacy Guidelines to build international consensus around general data protection principles, and they form the basis for many privacy laws around the world.

The OECD Privacy Guidelines focus on the principles of:

- **Collection limitation.** Organizations should:
  - Limit personal information collection
  - Obtain the data using lawful and fair means
  - When appropriate, provide individuals with notice and the opportunity to consent

- **Data quality.** The organization should ensure that the personal information it collects is:
  - Relevant to the purposes of use
  - Accurate, complete, and current

- **Purpose specification.** The organization should tell individuals why they collect personal information and how they plan to use it at the time they collect it.

- **Use limitation.** The organization should:
  - Limit personal information use and sharing to the purposes they disclosed when collecting the data
  - Not use personal information for incompatible purposes

- **Security safeguards.** The organization should employ reasonable security safeguards to protect personal information from risks of loss or unauthorized use, access, destruction, modification, or disclosure.

- **Openness.** The organization should be open and transparent about their personal information use, policies, and practices.

- **Individual participation.** The organization should provide individuals with the right to access, review, correct, and challenge the accuracy of personal information the organization collects.

- **Accountability.** The organization should hold itself accountable for implementing the privacy principles.

Evaluating a system’s alignment with this well-known international norm can help the organization identify and better understand its potential privacy risks. Complying with the guideline’s principles also helps the system mitigate common privacy risks.

**Conduct Privacy Analysis**

The PIA’s primary goal is to lower the organization’s privacy risks. With a clear understanding of the system and the privacy-related legal requirements, the PIA reviewers can start the process of identifying and mitigating potential privacy risks.

**Consider a PIA for an electronic marketing system within the U.S., when:**

- The system description section reveals that the marketing email templates do not contain an unsubscribe mechanism.
- The data flow map does not indicate that the system runs marketing emails through the organization’s marketing email opt-out suppression list before sending them.

The PIA reviewers conducting the privacy analysis would flag these system items as creating a possible privacy compliance issue with U.S.-based email marketing laws (see Practice Note, CAN-SPAM Act Compliance).

**Mitigating the identified privacy risks might involve:**

- Requiring the system to insert an unsubscribe mechanism into each email, by default.
- Adding a filter to suppress all email addresses with active marketing opt-out requests.

Evaluating potential privacy risks and identifying ways to avoid or lower the risk of harm is not always so straightforward or clear (see Identify and Understand Potential Risks and Mitigate Identified Risks). The process of evaluating potential harm and mitigating privacy risks often requires:

- Revisiting the system’s design or attributes.
- Creatively seeking ways to address concerns while accomplishing the system’s core business objective.

A successful PIA process is not only about the final written report. It works best when the PIA participants collaborate to review the system, identify risks, and determine the best way to address them. The PIA reviewers should encourage a frank and open conversation with the system sponsor and other stakeholders during the privacy analysis and risk mitigation phases.
Conducting Privacy Impact Assessments

Identify and Understand Potential Risks
Understanding the potential privacy risks that the system may generate is crucial to conducting a thorough PIA. When conducting the evaluation, organizations should consider potential risks to both:
• Their own operations
• Individuals whose personal information they hold
Many organizations also consider the larger or cumulative impact the system may have on society, particularly for novel technologies or use cases that may affect personal liberty, like new tracking or surveillance techniques (see Privacy as an Individual Right).

Types of potential organization-related risks to consider include:
• Legal liabilities, such as those from data breach lawsuits or similar actions
• Financial harms
• Reputational harms and loss of consumer trust
The PIA reviewers should also ensure the analysis section reflects and considers the organization’s corporate values and brand proposition. Actions taken in violation of the organization’s publicly stated values can cause significant harm and lead to brand diminution, even if they do not result in legal liability.

Types of potential individual-related risks to consider include:
• Economic loss
• Discrimination
• Physical harm, including harms to health or safety
• Reputational harm
• Deception or a subversion of the individual’s choice
• Unwarranted intrusions
• Other intangible harms when privacy, if considered a fundamental human right, is lost or subverted
Organizations should recognize that privacy risks are sometimes hard to identify and quantify. To learn more about the FTC’s views on consumer privacy injuries, see FTC: Informational Injury Workshop (Dec. 2017) and FTC Commissioner Ohlhausen Speech, Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases (Sept. 19, 2017).

The FTC has specifically warned organizations to carefully consider and mitigate the unique risks to consumers that big data projects leveraging personal information may cause (see FTC Report: Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (Jan. 2016)).

The PIA reviewers should also consider any specific risks unique to the personal information’s type or nature and identify ways to better address them (see Categorize System’s Personal Information and Mitigate Identified Risks).

Evaluate and Classify Risks
Evaluating a potential privacy risk also requires understanding both its severity and the likelihood that it might occur. The PIA should:
• Align risk mitigation efforts with the harm’s potential effects.
• Consider the mitigation action’s potential effectiveness in addressing the identified privacy risk or harm.
PIAs often use a sliding scale or matrix to consider these various factors and determine the best way to mitigate the system’s privacy risks. Significant harms with a high likelihood to occur may require extensive mitigation, while unlikely harms with trivial consequences might not require changes. The PIA should:
• Weigh these different considerations
• Recommend reasonable mitigation actions to appropriately address the identified privacy risks and harms
PIAs focus on identifying and mitigating the risks of potential privacy harms. However, PIA reviewers should also consider potential harms that may result from a data breach, successful cyber attack, or other unauthorized system use or abuse. These events can negatively affect the confidentiality, integrity, or availability of the system or the personal information that it holds. For more information on how PIAs and data security risk assessments work together, see PIAs and Data Security Risk Assessments.

Mitigate Identified Risks
Mitigating identified privacy risks often involves:
• Changing the system’s structure and controls
• Establishing specific policies and procedures for handling personal information
way to address them. The PIA reviewers should encourage a frank and open conversation with the system sponsor and other stakeholders during the privacy analysis and risk mitigation phases.
Conducting Privacy Impact Assessments

The actions required to mitigate each system’s privacy risks vary. However, organizations can leverage common data protection concepts to help them mitigate privacy risks, including:

• Ensuring data accuracy (see Data Accuracy)
• Only using personal information for clearly identified business purposes and minimizing unnecessary data use (see Data Minimization)
• Routinely deleting unneeded data (see Data Destruction)
• Enabling privacy by default (see Default Settings)
• Enforcing strong data security measures (see Data Security), including organizational and system controls that restrict:
  – Personal information access within the organization (see Sharing Data Internally)
  – Sharing personal information with others, including vendors (see Sharing Data Externally)

For example, systems using sensitive information may generate a privacy risk profile that requires specific mitigation actions, including:

• Stricter access controls. Sensitive data typically requires much narrower or stricter access controls.
• Additional consent or notice requirements. For example, an OBA campaign involving a person’s medical condition requires different controls than one promoting vacation packages because the NAI Code of Conduct requires advertisers to obtain opt-in consent before using sensitive data (see Activity-Specific Requirements).

(See Categorize System’s Personal Information.)

Ranking and rating the different harms and risks also allows the PIA review team to prioritize and develop a comprehensive picture of the system’s overall risk (see Evaluate and Classify Risks). If the overall risk remains high, even after considering possible mitigation actions, the PIA reviewer may recommend not proceeding with the system.

Data Accuracy

Inaccurate data harms both the organization and the individual because it leads to inaccurate decisions or conclusions. The risk of harm from inaccurate data increases when:

• A system automatically makes decisions based on the personal information it collects or generates.
• The organization relies on it to make important decisions.

Inaccurate data can also lead to inadvertent personal information disclosures or lost data, for example, if a system sends important medical test information to the wrong address.

Algorithms and artificial intelligence systems pose particular challenges because they may incorporate or reflect unconscious bias or lead to inaccurate conclusions (see FTC: Using Artificial Intelligence and Algorithms and FTC Report, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (Jan. 2016)).

The PIA should:

• Consider what harms inaccurate data may cause.
• Develop appropriate policies or procedures to ensure the system’s data remains accurate.

The mitigation strategy could be simple, such as requiring new account creators to type in their email and password twice to make sure they match or allowing individuals to view and manually correct OBA interest categories the organization assigns to them. Other mitigation actions might require more complex actions, such as requiring routine testing of an algorithm’s output for accuracy or unintended results.

Data Minimization

Limiting personal information collection, generation, and retention to that required only for the system’s purpose can also reduce privacy risks, like potential data breaches. The organization cannot lose what it does not have. PIA should always ask whether:

• The system uses the least amount of personal information required to accomplish the business purpose.
• Accomplishing the business purpose requires all the personal information elements the system collects or generates.

For example, a general CRM database accessible to all company employees does not require a customer’s SSN. Keeping the system data relevant to its purpose by deleting the unnecessary SSN field through the PIA process is a simple way to avoid potential liabilities (see State Social Security Number Protection Laws Chart: Overview).

PIAs should particularly question personal information collected in unexpected ways or in ways that would surprise consumers (see FTC: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012), pages 8 and 33).
Conducting Privacy Impact Assessments

The PIA should also explore opportunities to transform personal information into non-personal data or up-level it whenever possible. For example, a security log might require the exact time an individual accessed a web page, while a marketing system tracking potential consumer interests only requires a general timeframe, such as within the last week.

Employing data minimization as a mitigation technique on the marketing system can protect privacy and help avoid embarrassing customer interactions. A salesperson cannot inadvertently (and creepily) tell a customer, “I see you accessed our site at 12:31 am last night,” if the marketing system tracking website visits removes unnecessary data by up-leveling the exact time-stamp to general time frames.

**Data Destruction**

Data destruction complements data minimization as a tool for mitigating privacy risks. System designers often overlook the importance of data destruction to healthy systems. Retaining old or outdated data can lead to avoidable privacy mistakes, for example, by sending sensitive information to an old address. It can also unnecessarily increase the organization’s data breach risks. Some data protection laws require destruction once the organization meets the disclosed collection purpose (see International Considerations and Data Protection Impact Assessments).

PIAs should explore:

- How long the system needs to keep personal information to accomplish the business purpose.
- When the system plans to delete stale, unnecessary, or irrelevant personal information.
- What process is in place to ensure the personal information’s deletion when its useful life ends.
- Whether and how the system can automate the data deletion process.

The review should always tie the data retention period to the business purpose or legal retention requirements. The organization may formalize its retention requirements in a data retention policy and schedule (see Practice Note, Drafting a Document Retention Policy and Standard Document, Document Retention Policy). The PIA should help the organization identify which personal information and data elements the organization must keep, delete, or transform after the primary collection purpose no longer supports retention.

When the business purpose requires retaining some personal information for longer periods of time, organizations should not assume they must keep everything. For example, a company may need to retain the name, employment time span, and rehire status of former employees during the life of the company to keep accurate employment records and answer past employment inquiries. However, if not, it may not need all the former employees’ complete files. The PIA should consider requiring the system to purge data elements that do not support the stated historical archive or records retention purpose.

**Default Settings**

Establishing default settings that protect an individual's privacy interests represents one clear and easy way to mitigate risks. The PIA should:

- Examine each of the system’s default settings.
- Consider what setting best protects both individuals’ and the organization’s interests.

The organization should avoid default settings that could result in the disclosure or sharing personal information without the individual’s input or knowledge.

FTC best practices recommend establishing privacy-protective default settings (see FTC: Mobile Health App Developers: FTC Best Practices). The FTC has prosecuted enforcement actions against organizations with harmful or deceptive default settings. For example, in FTC v. Frostwire LLC, the FTC settled an enforcement action against a mobile app whose default settings:

- Immediately shared the user’s files on installation.
- Caused consumers to unwittingly disclose personal files stored on their mobile devices.

(Stipulated Final Order, FTC Case No. 11-23643 (S.D. Fla. Oct. 12, 2011).)

**Data Security**

Ensuring the system provides the appropriate level of data security represents another key risk mitigation technique. The PIA should determine the appropriate level and type of security that the system and the personal information it holds requires (see Categorize System’s Personal Information).

Systems holding highly sensitive protected health data likely require different security protections than a system managing the organization’s email marketing program. Once a company determines the appropriate security level, it can use data security assessments and audits to evaluate the implementation of those controls (see PIAs and Data Security Risk Assessments).
Conducting Privacy Impact Assessments

For more information security resources, see Information Security Toolkit.

Sharing Data Internally

Access controls represent an important method for reducing privacy risks because they limit personal information access to those with a legitimate business reason. The PIA should:

• Identify which employees require access to the system's personal information to do their jobs.
• Establish clear internal access controls that match those business use requirements.

For example, a PIA reviewing a system's use of detailed employee performance information should ensure the controls restrict access to those whose jobs directly require it, such as the employee, the employee's manager, and members of the HR department directly responsible for the performance review process.

Minimizing the number of individuals with personal information access also allows the organization to comply with data security best practices (see FTC: Start with Security: A Guide for Business and Practice Note, FTC Data Security Standards and Enforcement).

Sharing Data Externally

Sharing personal information with vendors or other parties outside the organization exponentially increases the organization's privacy risks. Increased third-party access and use of the system's personal information reduces the organization's ability to control and protect that data because it becomes more difficult to effectively monitor the personal information and prevent data leakage or misuse.

Some states have also enacted privacy laws that restrict the sale of personal information by an organization, including California, Nevada, and starting January 1, 2023, Virginia (see Practice Note, Understanding the California Consumer Privacy Act (CCPA), Nevada’s Personal Information Sales Opt-Out Law Checklist), and Quick Comparison Chart (CPRA and VCDPA).

The PIA should consider options to streamline or limit third-party access whenever possible. Establishing a strong vendor due diligence program, including audits, is also a key risk mitigation technique. For more on managing vendor privacy risks, see Practice Note, Managing Privacy and Data Security Risks in Vendor Relationships and Standard Document, Vendor Due Diligence: Security and Privacy Questionnaire.

Reflection and Feedback

PIAs are not a one-time process or a document to complete, file, and never review again. Effective PIA programs recognize that many factors change over time, including:

• Laws
• Technology
• Systems
• Company policies
• Customer expectations

Anticipating changes and requiring regular system reviews enables the PIA process to better achieve its risk mitigation goals. The privacy risk analysis otherwise may become stale.

PIAs also often result in recommended or required system changes. Regular reviews allow the PIA team to:

• Confirm implementation of any required system revisions.
• Consider the effectiveness of the risk mitigation actions adopted.

Best Practices for Conducting PIAs

There are various approaches to conducting PIAs. Successful PIA programs with effective results:

• Require a process and a plan. At a minimum, the plan should guide the PIA process by:
  – Defining the scope
  – Determining the steps to follow
  – Identifying specific questions to answer
• Require a clear and detailed description of the system, specifically of how it uses, processes, generates, or collects personal information.
• Integrate the process with the organization's other risk management programs. The organization should rate and track risks identified through the PIA process according to its enterprise risk classification framework.
• Take advantage of pre-existing organizational processes. When addressing privacy issues in existing systems that require changes, consider integrating the PIA process with the organization's:
  – Change management program
Conducting Privacy Impact Assessments

- Project management or software development life cycle (SDLC) processes
- Obtain top-down executive support for embedding privacy by design into the organization's culture. Instead of viewing the PIA process as a burden, the organization can promote PIAs as a map to help employees navigate privacy issues that are important to its customers and overall success.
- Conduct PIAs as early as possible in the life cycle process and trigger new reviews when the system or circumstances materially change.
- Clearly define role and responsibilities. Organizations should determine who:
  - Initiates the PIA process
  - Manages the PIA process
  - Provides oversight
  - Engages privacy leaders and other stakeholders within the organization
- Store PIAs in a central repository for ease of management, quick reference, oversight, and transparency.
- Establish controls to mitigate the identified privacy risks. Many controls relate to information security, but the system may also require non-technical controls, such as implementing new policies and operational procedures to mitigate the identified privacy risks. The PIA report should contain the agreed to controls and recommendations together with the timeline for implementation.
- Conduct internal governance and compliance reviews to ensure employees complete PIAs and any identified action steps according to internal policies and any applicable laws.
- Treat the PIA report as a living document that the organization regularly reviews and updates as necessary throughout the system life cycle.
- Conduct training and awareness campaigns to communicate the PIA program's benefits and importance to the organization's regulatory and internal compliance. The organization should also conduct general training for employees on the importance of protecting personal information and understanding the potential risks created from inadequate or missing privacy controls.
- Require executive or senior organization leaders to approve the PIA's final results and conclusions, particularly when the PIA results in:
  - Required system changes
  - Residual privacy risks the review cannot mitigate
  - Require PIAs for all third-party organizations or systems that store, access, or process personal information, such as service providers, software developers, or cloud providers. Organizations should contractually require third parties to support their risk assessment processes, including PIAs.

Data Protection Authority Resources on Conducting PIAs and DPIAs

France’s Data Protection Authority (CNIL) developed an open-source software tool that data controllers can use to conduct a DPIA required under the GDPR, with software versions in French and English (see CNIL: Privacy Impact Assessment (PIA)).

The CNIL’s program follows the PIA methodology it started developing in 2015 (see CNIL: PIA: An overview of the requirements and methodology) and organizes the DPIA into four sections:

- Context
- Fundamental principles
- Risks
- Validation

The program maps identified risks to potential privacy impacts and categorizes them by developing a scaled score based on the risk’s seriousness and likelihood. It also provides information about the relevant GDPR requirements and privacy considerations in-line and links to a searchable PIA knowledge base to help users better understand their specific risks. Users can then create an action plan to address or remediate risks deemed unacceptable.

PIA or DPIA resources from other data protection authorities include:

- In Australia, Office of the Australian Information Commissioner (OAIC): Guide to undertaking privacy impact assessments and OAIC: 10 steps to undertaking a privacy impact assessment.
Conducting Privacy Impact Assessments

- For Canada:
  - Office of the Privacy Commissioner (OPC): Privacy Impact Assessments
  - OPC: Top Ten Dos and Don’ts for Privacy Impact Assessments
  - Office of the Information & Privacy Commissioner for British Columbia: Privacy Impact Assessments for the Private Sector

For the United Kingdom, Information Commissioner’s Office (ICO): Data protection impact assessments. See also, Legal Update, ICO publishes guidance for organisations conducting privacy impact assessments for artificial intelligence systems.