2021

DATA PRIVACY AND PRIVACY ASSESSMENT ESSENTIALS

A GUIDE FOR PRIVACY, COMPLIANCE, AND BUSINESS LEADERS

BUSINESS ETHICS LEADERSHIP ALLIANCE™
An Ethisphere Community

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

We would like to thank the members of our Business Ethics Leadership Alliance (BELA) Compliance & Data Privacy Working Group for their insights and knowledge in developing this Guide. Each Working Group member has invested considerable time in the review process and feedback loops to help create practical material that can broadly support the goals and actions of privacy leaders/officers, compliance officers, business partners, and third parties.

The privacy and data protection landscape—inclusive of laws, regulations, and practices—is constantly changing. In order to keep pace with those changes, this type of guide will require occasional updates. While this guide focuses in some pivotal elements of privacy team structures, principles, risk assessments, and more, there are numerous workings within the privacy function to consider for future documentation and output. Additional privacy toolkits have been suggested and we will address those in turn. Feedback and shared insights from the entire BELA community will be continuously sought and valued in order to make this possible. At the center is the Compliance & Data Privacy Working Group, we would like to extend the utmost gratitude to the following individuals and their organizations.

Specifically, we would like to thank the following Compliance & Data Privacy Working Group Members:

CO-CHAIRS:

Samantha Vaughan
Sr. Managing Director, Global Privacy Counsel
Dell Technologies

Craig Moss
Executive Vice President,
Ethisphere

WORKING GROUP CONTRIBUTORS:

Karen Benson
AVP, Assistant Chief Compliance Officer,
Royal Caribbean Cruises

Edward Efkeman
Global Head of Privacy, FedEx

Jerry Hanifin
Sr. Counsel—Privacy, Ethics, and Compliance,
Panasonic Corporation of North America

Katherine Licup
Chief Privacy and Information Risk Officer
and Senior Counsel,
Archer Daniels Midland Company

Kevin McCormack
Sr. Vice President and BELA Executive Director,
Ethisphere

Francisco ("Paco") Padilla Borallo
Director and Counsel, Data Protection and Privacy,
Eaton Corporation

Sooji Seo
Vice President and Chief Privacy Officer,
Dell Technologies

Jonathan Steel
Law Vice President, Chief Ethics, Compliance &
Privacy Officer,
Teradata Corporation

INTRODUCTION

The purpose of this guide is to equip privacy leaders, data protection officers (DPOs), chief privacy officers (CPOs), and the data privacy team with context for their program and offer tools to support implementation of the program. The guide also seeks to demystify data privacy to facilitate communication between the data privacy team and the business units and senior management.

We have written this guide for the person responsible for data privacy, whether or not you have the CPO or DPO title. We have also included background and explanations that are intended to help you build awareness in your company about the importance of data privacy and resources to help you implement an effective data privacy program.

Just as the title of the responsible person may differ from company to company, there may also be different names for the assessment process itself. Some companies call it a privacy impact assessment, some a data privacy assessment, and some a data protection assessment. In this guide, we use the term 'privacy impact assessment' and we refer to your role as the 'Privacy Leader'.

In the pages that follow a progressive narrative is presented to help you make better decisions and design your program supported by forms, decision trees, and risk categorizations. While there are many common threads to a data privacy program across companies and industries, there will be nuances for how your program is designed that will be influenced by unique principles, risk classifications, and team structures.

This guide is divided into the following major sections:

- ✓ Foundational elements of a privacy program - roles, principles, benefits, and risks.
- ✓ Process for conducting a privacy impact assessment with guidance on managing a practical risk-based program.

SECTION 1:

FOUNDATIONAL ELEMENTS OF A DATA PRIVACY PROGRAM

This section will provide overall context for your data privacy program and how it fits into your broader enterprise risk management process.

WHY DATA PRIVACY MATTERS

You are now in the position where data privacy falls under your area of responsibilities. There are core elements you need to understand and be able to explain to others in the organization.

Data privacy has become a critical concern to a myriad of stakeholders, including customers, partners, employees, and even investors. Privacy is now considered a fundamental human right as evidenced by regulations in the European Union (i.e., General Data Protection Regulation, or GDPR) and the United States (i.e., California Consumer Privacy Act, or CCPA) and other emerging jurisdictions with ongoing efforts to expand data privacy regulation. In March 2021, Virginia passed a data privacy law, with laws being developed in other states ranging from New York to Utah to Washington. New or amended data privacy laws were passed or are under consideration in countries around the world including Brazil, Canada, and China.

As a legal and regulatory issue, you need to ensure that contracts and terms of use for your data and services are aligned with specific regulatory requirements. Without proper implementation you expose your company to unnecessary risk and potentially litigation and/or regulatory penalties. As the Privacy Leader you need to consistently inform senior management, or the appropriate business owner, of these requirements and the importance of meeting them.

> As current and emerging regulations are enacted to protect the privacy of individuals, it is incumbent upon you to know what data you have, where it is stored, and who has access to it.

Privacy concerns are top of mind for companies, legal departments in particular. The ACC's 2021 Chief Legal Officers survey recognized data privacy, compliance, and cybersecurity, as the most important issues for the third consecutive year.

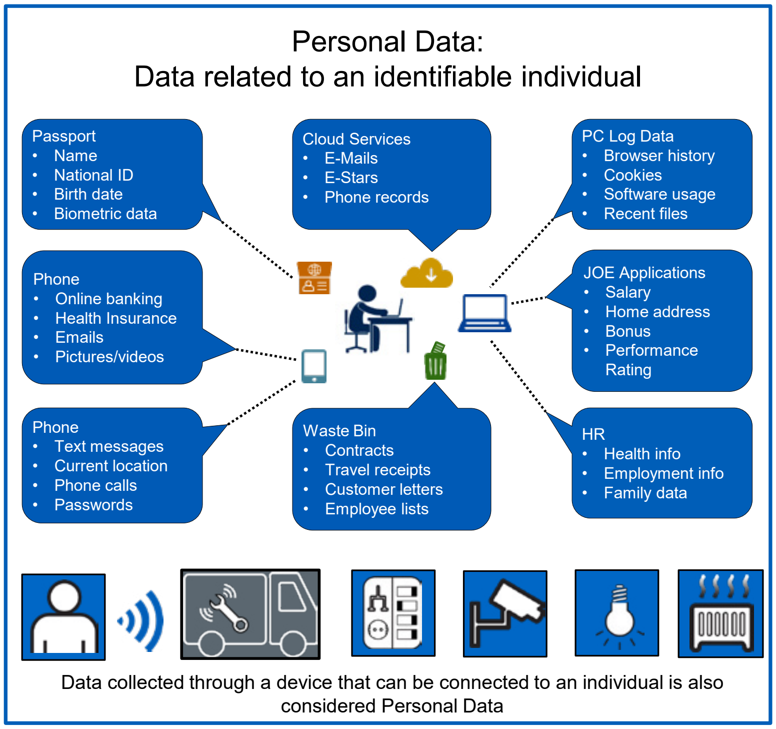
Beyond risk mitigation, committing to a clear data privacy framework can foster trust with stakeholders and enhance the brand loyalty of your customers. You need to think about data privacy positioned as a competitive advantage, especially in this environment. The time invested in data privacy can generate a clear return on investment (ROI) through an enhanced reputation and differentiated offering relative to your competitors.

> You should be presenting privacy as a value driver and competitive advantage for your organization and use this to encourage a shift in thinking that goes beyond what is minimally required by regulation.

Companies in many industries are building or enhancing their trusted customer relationships by shifting their mindset to go beyond regulatory compliance. A well-managed privacy program allows you to make better use of data assets your company has and establishes reasonable limits to data use to maintain customer trust.

Here is an example of how some companies communicate data privacy as a competitive advantage – internally and to their customers.

FIGURE 1: Eaton's summary of personal data and how to process it.



We may only collect, process and transfer Personal Data as follows:

Principle	Description	Example
Legitimate	We must have a legitimate purpose, such as a contractual relationship or, in some cases, consent of the individual	Using personal data based on an Employment contract
Authorized Purpose	We can only use the Personal Data for the purpose for which it was collected originally	Sending an event invitation to someone who registered
Proportionate	Use only as necessary, appropriate, relevant and not excessive in connection with why it was collected	Not collecting bank account information to send an email
Need to know	Access can only be granted if there is a legitimate business "need to know" and required to perform a legitimate task	An event organizer needs to know who is attending

DATA PRIVACY AS PART OF ENTERPRISE RISK MANAGEMENT

In most companies, data privacy fits into a broader enterprise risk management framework. Enterprise risk management is the broad function of assessing the financial, operational, market, reputational and legal/compliance risks your company faces. You need to be aware of where data privacy fits in your company and how it relates to other risks, especially information security, cybersecurity and regulatory compliance.

In recent years there has been a dramatic increase in the focus on environmental, social, and governance (ESG) reporting. In ESG reporting frameworks, data privacy is considered a fundamental human right issue and it is included in the “S”of ESG. Because your data privacy program will be part of your overall ESG reporting and you should review your ESG reporting requirements as you develop your data privacy program. The Sustainable Accounting Standards Board (SASB), the Global Reporting Initiative Standards (GRI) and MSCI, Inc. all prominently include data privacy in their ESG reporting. Even if this is considered a voluntary effort, it is increasingly critical for new models of ethical or impact investing.

Global Reporting Initiative (GRI) 418: Customer Privacy

The reporting organization shall report its management approach for customer privacy using GRI 103: Management Approach…

Protection of customer privacy is a generally recognized goal in national regulations and organizational policies. As set out in the Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises, organizations are expected to ‘respect consumer privacy and take reasonable measures to ensure the security of personal data that they collect, store, process or disseminate’.

TAKING A RISK-BASED APPROACH TO DATA PRIVACY

As with other compliance issues, most companies take a risk-based approach to managing data privacy. Later in this guide we talk about the relationship between the inherent risk a situation poses, the residual risk after the controls are put in place and risk tolerance established by the company.

The spotlight on data privacy was driven by new regulations which are now accelerating around the world. The legal requirements of most regulations are relatively similar. As the Privacy Leader, you need to understand the common legal and regulatory requirements, though the legal requirements are really the minimum bar for a robust data privacy program. When evaluating your risk, you should be considering these requirements as well as the reasonable expectations of your customers in how you protect your data.

As with assessing other compliance and operational risk you and your company needs to understand the probability and potential negative impact of compromised data. In communicating and building your program inside the organization you will need to work across the enterprise to explain the risks and establish an acceptable level of risk tolerance beyond the minimum legal requirements.

As the Privacy Leader, you will need to simplify the issue of data privacy and explain the relevance to the executive team and the business units. Here are

> Privacy Leaders and attorneys should focus on reducing risk to the extent you are able, understanding that you may not be able to negotiate to ZERO risk with your business units. Therefore, your senior leadership team may need to accept, and plan for, a certain level of risk.

some factors to communicate and consider about data privacy risks that can help guide you and senior management to establish your company's risk tolerance:

- **Brand Reputation Risk** – Data privacy breaches can have an impact on the company's reputation in the eyes of investors, customers, regulators and other stakeholders.

- **Financial and Legal Risk** – Companies can be held legally and financially liable if third party data is compromised in a breach.

In many cases you will need to help your company establish an acceptable risk tolerance level and you may need to negotiate with business units on what risk can be tolerated. Here's an example for you to consider. A vendor performing a low-value, but time sensitive, contract for services has access to personal information, but not the ability to obtain high-limit insurance or fully cover your financial liability should there be an information compromise. In a case like this, you and your legal team should try to negotiate to the legal standard of protections required per jurisdiction and the optimal indemnity provisions possible. If significant risk remains, advise your senior leadership team to seek their consideration and acceptance.

What is an Acceptable Risk?

Real examples of risk tolerance issues:

- Small important vendor can't afford insurance – Will your business unit accept risk and associated liability?

- A large vendor refuses to mirror your data access request policy provisions – Do you proceed?

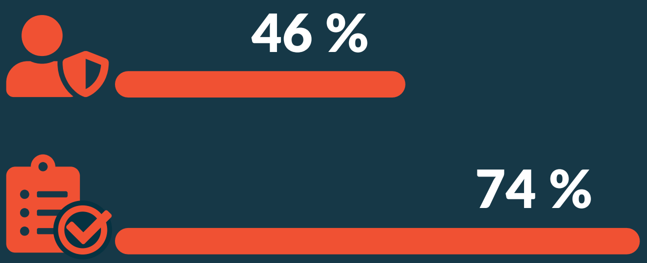
- Your marketing department wants to re-use data for a purpose that was not specifically covered in the original privacy notice – Do you allow it?

- Different customers have different data retention policy requirements that make it difficult for you to comply with all – What is a reasonable response to your customers?

DATA PRIVACY IN THE ORGANIZATIONAL STRUCTURE

There is no single right way to structure your data privacy role or teams within your organization. There are several factors that will influence, including: industry, size of organization, geographic footprint, functional department structure, and more factors. In particular you will want to consider the relationship between data privacy, information security, information technology, records management, data governance, cybersecurity, legal, and compliance to determine your structure to enable authority and decision-making.

At a high level, it may be in your interest to think about reporting lines and the clear delineations of roles and responsibilities in order to avoid duplication and gaps in accountability. In some organizations the data privacy function reports to the information technology leader along with the information security and cybersecurity functions.



According to the Association of Corporate Counsel (ACC) 2021 Chief Legal Officers survey "privacy ranks as the second most common function that reports up to the CLO (46 percent) after compliance (74 percent)."

Regardless of the formal reporting structure, it is critical for you to build active communication channels with related functional areas. We talk more about the value of cross-functional teams later in this guide.

In some organizations, data privacy is considered to be part of the legal or compliance department, frequently reporting to either the Chief Compliance Officer or Chief Legal Officer/ General Counsel. ***Figure 2*** shows an example of how **FedEx** structures the privacy function.

Figure 3 is one example from **Royal Caribbean** of how data privacy fits into a broader data governance structure. Note how the Data Governance Advisory Committee includes representatives from a range of functional areas.

FIGURE 2: FedEx Privacy Function Structure

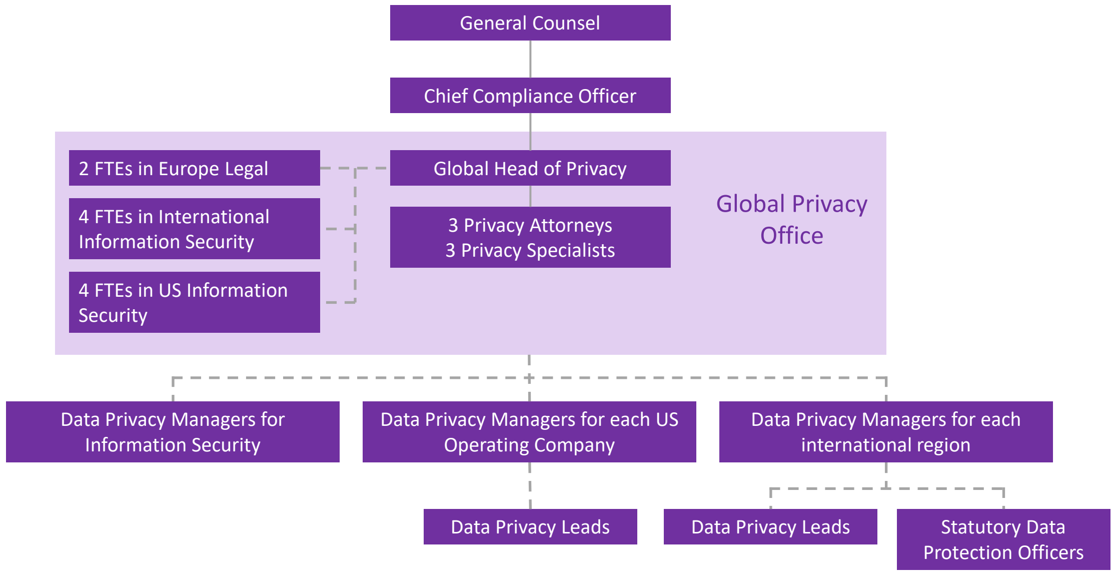
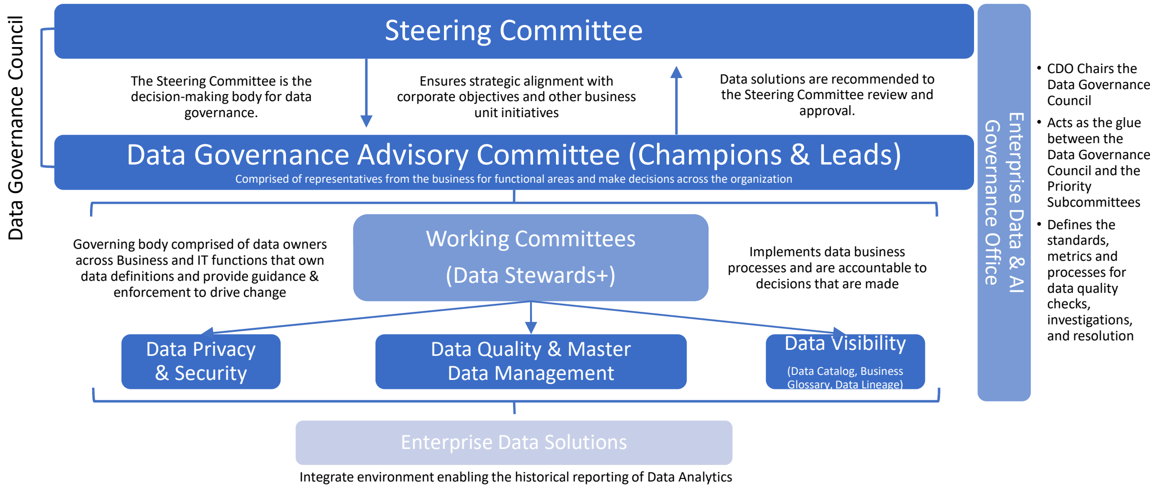
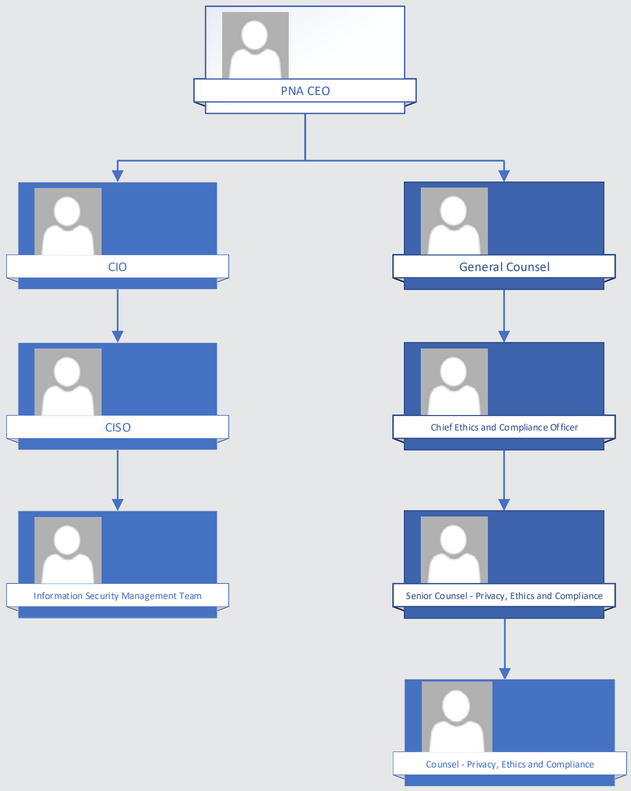

General Counsel
Chief Compliance Officer
2 FTEs in Europe Legal
Global Head of Privacy
4 FTEs in International Information Security
3 Privacy Attorneys
3 Privacy Specialists
Global Privacy Office
4 FTEs in US Information Security
Data Privacy Managers for Information Security
Data Privacy Managers for each US Operating Company
Data Privacy Managers for each international region
Data Privacy Leads
Data Privacy Leads
Statutory Data Protection Officers

FIGURE 3: Royal Caribbean Data Governance Framework


Data Governance Council
Steering Committee
The Steering Committee is the decision-making body for data governance.
Ensures strategic alignment with corporate objectives and other business unit initiatives
Data solutions are recommended to the Steering Committee review and approval.
Data Governance Advisory Committee (Champions & Leads)
Comprised of representatives from the business for functional areas and make decisions across the organization
Governing body comprised of data owners across Business and IT functions that own data definitions and provide guidance & enforcement to drive change
Working Committees
(Data Stewards+)
Implements data business processes and are accountable to decisions that are made
Data Privacy & Security
Data Quality & Master Data Management
Data Visibility
(Data Catalog, Business Glossary, Data Lineage)
Enterprise Data Solutions
Integrate environment enabling the historical reporting of Data Analytics
Enterprise Data & AI Governance Office
• CDO Chairs the Data Governance Council
• Acts as the glue between the Data Governance Council and the Priority Subcommittees
• Defines the standards, metrics and processes for data quality checks, investigations, and resolution

This example from **Panasonic Corporation of North America** provides insight into their privacy program hierarchy.

FIGURE 4: Panasonic Corporation of North America Privacy Program


PNA CEO
CIO
General Counsel
CISO
Chief Ethics and Compliance Officer
Information Security Management Team
Senior Counsel - Privacy, Ethics and Compliance
Counsel - Privacy, Ethics and Compliance

If as the Privacy Leader you have the resources to support a broader team of professionals to support the function, you may want to consider a mix of contributors. This could mean a combination of lawyers and non-lawyers. Non-lawyers are often responsible for overall program management while lawyers will be responsible for contracts and negotiating data privacy agreements with third parties.

Relationship Between Data Privacy, Information Security, and Cybersecurity

You will also need to differentiate among data privacy, data protection, information security, and cybersecurity, and how these elements are structured and function together within the organization. There is also an important distinction to be made between information security and cybersecurity and how both relate to your data privacy role.

Information security defines what needs to be protected as well as determining confidentiality, integrity, and availability. Confidentiality ensures that only those authorized to access the information can access it. Integrity is ensuring the data is not modified, manipulated, or destroyed. Availability suggests that the data is consistently available whenever it is needed. Cybersecurity is about protecting systems and data from being compromised or "attacked" by threat actors which includes both external and internal parties. In other words, cybersecurity is responsible for implementing the controls necessary for the protection of systems and information.

Here are some simple definitions of each area:

DATA PRIVACY: focuses on Personally Identifiable Information (PII), Personal Health Information (PHI) and the rights of the individual to have control over how their information is collected and used – typically driven by meeting regulations.

DATA PROTECTION: can have multiple meanings. It can mean the protection of PII or it can be used more broadly to talk about how a company protects all confidential business information (e.g. business information, PII).

INFORMATION SECURITY: the process of protecting all information in all forms to make sure it remains confidential, is available to those that need it and is not altered (sometimes referred to as Confidentiality, Integrity, Availability).

CYBERSECURITY: technologies and processes to protect networks, devices and data from attack, damage, or unauthorized access.

FOUNDATIONAL ELEMENTS OF A DATA PRIVACY PROGRAM

ROLE OF THE PRIVACY LEADER

Depending on the structure and executive level of the Privacy Leader, companies will use different titles. Examples include:

a. Privacy Officer
b. Data Privacy Officer
c. Head of Privacy
d. Data Privacy Manager
e. Chief Privacy Officer

In many cases data privacy is not the only responsibility of the individual in that position. Increasingly, those that have ultimate responsibility for privacy may also have some degree of ownership in areas such as compliance, information security, or other legal/regulatory responsibilities. Additionally, relevant regulation may determine what responsibilities are required for someone in the privacy position.

GDPR Data Protection Officer

GDPR, for example, requires the appointment of a Data Protection Officer with the following responsibilities, which are similar to responsibilities outlined by other data privacy regulations:

- ✓ Serve as a point of contact for data subjects and supervisory authorities
- ✓ Raise awareness within your organization of how data privacy laws affect data processing requirements
- ✓ Conduct data protection impact assessments
- ✓ Monitor your organization's compliance with relevant data privacy rules and monitor data privacy risks arising in your organization's activities
- ✓ Maintain records of processing
- ✓ Conduct data security and processing audit
- ✓ Ensure staff are trained on data processing requirements

Effective Training and Communication

One of your most critical roles is to build awareness in your organization of data privacy. To effectively implement data privacy policies and procedures all employees and others with whom you work need to be trained on the rules and know how to follow them. Communication is a high priority area.

To build awareness you need to go beyond once-a-year training to include short, frequent communications. Think of it more as an ongoing communication program, rather than an annual training program. As you develop training and communication materials think about three stages of messaging to your employees:

- ✓ **Awareness** – What is the issue?
- ✓ **Commitment** – Why is it important to the company and to 'me' in my job?
- ✓ **Action (how-to)** – What do you want 'me' to do and how should I do it?

Building knowledge around awareness, commitment, and action for data privacy can take place through traditional instructor-led training, e-learning, and a wide range of other types of communications to reinforce the message. Training and communications should be tailored to risks, responsibilities and business functions, and local challenges. In many cases, compliance training on topics like data privacy focuses too much on trying to make people aware of the legal issues and not enough on commitment and action.

Training for all employees is a good foundation, but roles will vary across an organization and across geographies. It is important to customize data privacy training and communication for departments or employees using specific scenarios they may face in their jobs. To be effective, your communication for the marketing department will be slightly different than the communication to the human resource or information technology departments.

As we mentioned, to build a data privacy culture you will need to reinforce your formal training program with short frequent communications. There are a lot of ways to do this. You should pick the methods that best fit your company. Here are a few examples:

- ✓ A column in your company e-bulletin or newsletter
- ✓ A weekly email with a data privacy tip
- ✓ FAQ
- ✓ Posters, postcards or sticker for the workplace
- ✓ Screen-savers
- ✓ Data privacy topic of the month

Importance of Cross-Functional Collaboration

Ultimately, the goal is to embed data privacy into operations in a practical way and not have it stay in a separate silo. The creation of a formal cross-functional data privacy team will be a valuable step in achieving the goal. Data privacy has a clear relationship to the legal and IT functions in your company, but think beyond that.

Your cross-functional team should include the functions that regularly use the data and/or have relationships with the third parties that do. These could include sales, marketing, human resources, procurement, finance and research and development. You want to include people that are senior enough to have authority and overall visibility into how their function operates. It can be challenging to get their time commitment. One approach that can work is to form the team around defining and achieving a specific time-bound goal in 6 months or less. Seek their involvement to help define a data privacy goal that is practical and impactful for all. This gives the team a specific objective and those you approach will not see the team as “another open-ended committee and series of meetings.”

Importance of Goal-Setting to Drive Change

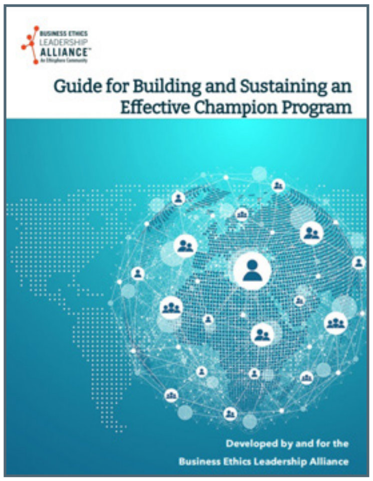
Use measurable, time-bound goals to drive change in how people behave. Focus on results rather than process to make more rapid progress. Here’s an example of how to turn a weak goal into a powerful goal.

WEAK GOAL:
Train selected business units on new privacy impact assessment process.

POWERFUL GOAL:
Engage 5 high-risk business units to complete the new privacy impact assessment process for at least one project in 3 months.

As you develop the data privacy program and the related policies, it is important to get input from all functions to make sure that the policies are practical. Privacy needs to become a consideration in how each department plans and assesses their risk. We cover “privacy by design” later in this guide, which goes into more detail on how to embed privacy into how your business operates.

Getting input during development is a great way to break data privacy out of a silo and show how it can be embedded into their function with a minimum of disruption – and ideally as a way to add value. Beyond the initial program development, you will need the support and cooperation of these functional areas to make the program come to life. Ultimately, it is likely that you will want to identify a data privacy “Champion” or “Ambassador” in each function and forming the cross-functional team early will lay the foundation for that. If you have an existing champion program you might see if you can use a segment of that champion network to concentrate of data privacy.


BUSINESS ETHICS LEADERSHIP ALLIANCE

Guide for Building and Sustaining an Effective Champion Program

Developed by and for the Business Ethics Leadership Alliance

Building Senior Level Support for Data Privacy

Gaining senior management support for data privacy is a critical step. Their visible support is an essential component of building awareness and commitment in your company. Here is an example of how one Privacy Leader included in building the business case for senior management approval for the data privacy program's budget and implementation plan. Note the focus on linking data privacy to value-creation and the establishment of two types of metrics: program maturity metrics and resulting performance metrics.

- Privacy Office needs to define the problem statement and objectives that they want their C-Suite/Board Level commitment/support.
- Consider external whitepapers to help define the privacy maturity stage (compliance/risk/value) the executive leadership team/privacy office wants to achieve.
- Externally benchmark with peer companies on their privacy maturity stage to ensure you bring an "outside in" perspective.
- Consider external whitepapers on Privacy Function State of Union to assess appropriate privacy function budget - privacy resources, contractors, outside counsel/consultants spend and technology investments.
- Conduct an independent operational privacy compliance maturity assessment to identify gaps and prioritize focus areas based on the operational maturity stage an organization wants to achieve. Consider existing data points at an enterprise level on privacy compliance/accountability/risks metrics and leverage internal/external privacy audit findings to articulate a narrative to senior executives on what do they want "privacy to be when it grows up". Focus the narrative on privacy as a core business value vs a privacy risks/compliance function only.
- Create a business proposal that is multi-year privacy transformation journey with C-Suite executive(s) sponsorship (at least 1 executive sponsor should be in the business) to advocate to the CFO, Vice-Chairman or COO.
- Establish privacy metrics (Key Performance Metrics and Key Result Indicators) in core lines of business/functions as part of team member's performance plan and develop a reporting cadence to drive executive awareness and accountability.
- Leverage various internal governance committees to present on privacy KPIs and KRIs to demonstrate operational privacy maturity improvements/challenges.

Budget Considerations

As with other compliance related issues, many companies view data privacy as a cost and not an investment. As a result, there is always pressure to keep costs and headcount as low as possible. But there is a business case for team growth and talent acquisition. The business case falls into two broad areas:

- Gaining a competitive advantage with your customers
- Reducing the amount of money spent on outside counsel

We have already highlighted the importance of positioning data privacy as a value-driver. The other point to highlight in gaining additional budget for you program is the possible cost saving. The cost-saving argument has two prongs:

- Building internal capability reduces the use of expensive outside counsel
- Prevention is ultimately less expensive than responding to and recovering from an incident

14 %

14 percent of CLO respondents to the 2021 ACC Chief Legal Officers survey revealed plans to expand the staff dedicated to privacy. This increase in staffing levels is quickly becoming imperative with privacy as core value and driver of business advantage.

Finally, look for ways that that you can be creative and collaborative with the budget. For example, in one company the salary of a new data privacy manager was paid by legal, the new technology was paid by IT, and the cost for training employees on data privacy was paid by compliance.

DATA PRIVACY PRINCIPLES

Privacy regulation around the world are generally based on the same underlying principles. While your company and industry may influence what principles to elevate above others, here is a quick overview of principles to consider as you design and implement your program.

There are basic data privacy principals that that are the underpinning of the various regulations around the world. In general, the regulations have many common features built upon the following principles:

- ✓ **FAIRNESS AND LAWFULNESS:** You need to ensure that your data collection process does not violate the law, and where the law might be unclear, operate with fairness in mind
- ✓ **TRANSPARENCY AND VISIBILITY:** You must provide notification about the data you are collecting and how it is being used, and your organization must be aware, and have visibility, into where the data is being stored and how it is collected.
- ✓ **PURPOSE LIMITATION:** You should use data only for its intended purpose.
- ✓ **DATA MINIMIZATION:** You should limit the collection of personal data in order to achieve the specific and intended purpose.
- ✓ **ACCURACY:** You need to take reasonable steps to maintain the accuracy of the data and rectify any inaccurate data.
- ✓ **RETENTION AND STORAGE:** You should retain personal information only as long as needed to meet the intended purpose, and then take steps to destroy the data or render unidentifiable as the intended purpose is exhausted.
- ✓ **SECURITY AND CONFIDENTIALITY:** You need to implement both physical and cybersecurity safeguards to keep data safe and secure and maintain the confidentiality of the information.
- ✓ **ACCOUNTABILITY:** You will be responsible for compliance controls as required by law and regulation and that your program has reasonable measures to properly manage risk.

Minimization of Personal Data Acquired

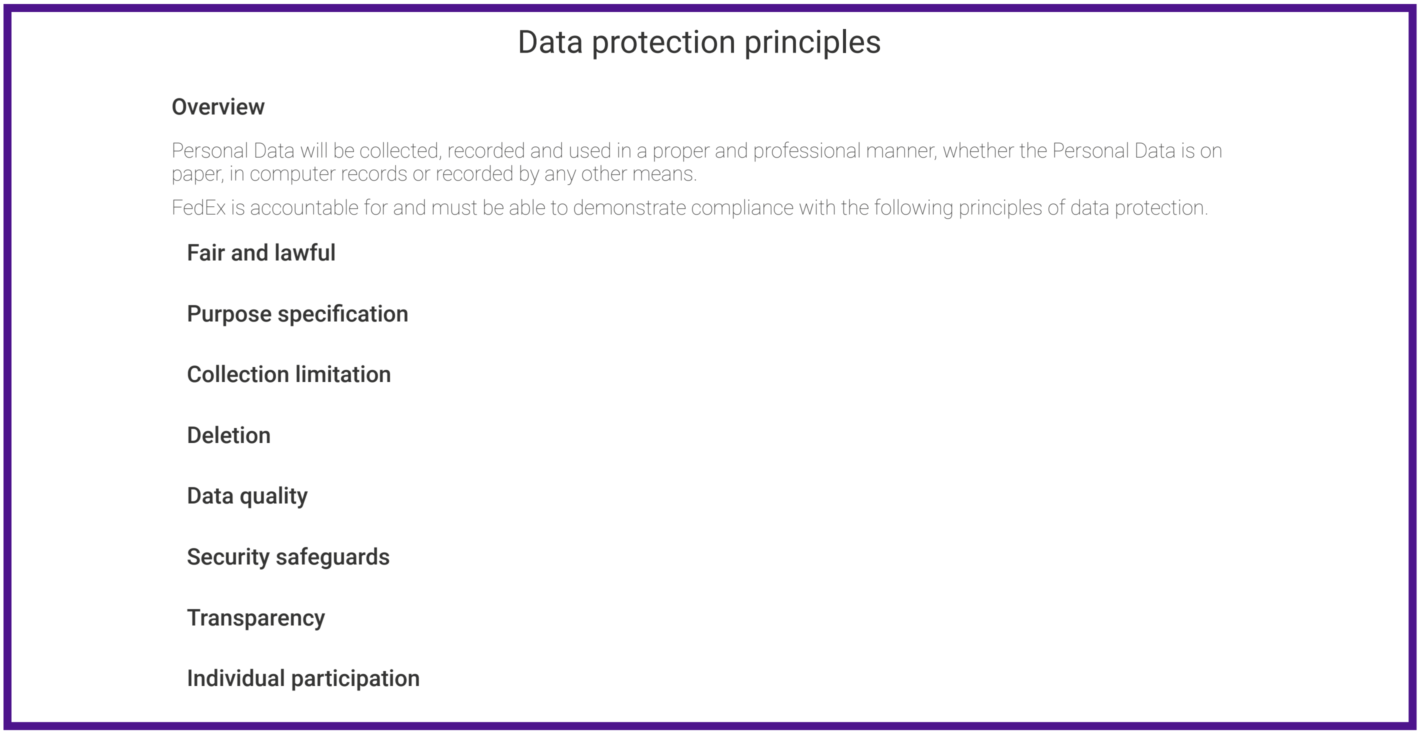
Consider carefully the precise data elements acquired (e.g. geolocation) and whether all are really necessary for the specific purpose. Consider if certain data elements be substituted for others (e.g. Device ID could be substituted for a random user ID number to separate that particular entry from the others, but that does not tie to any other identifier).

Here are examples of how two BELA member companies communicate the data privacy principals:

FedEx lists the following 'data protection principles' as part of their Global Privacy Policy.

This is how **ADM** communicates the privacy principles internally.

FIGURE 5: FedEx Data Protection Principles



Data protection principles

Overview

Personal Data will be collected, recorded and used in a proper and professional manner, whether the Personal Data is on paper, in computer records or recorded by any other means.

FedEx is accountable for and must be able to demonstrate compliance with the following principles of data protection.

Fair and lawful

Purpose specification

Collection limitation

Deletion

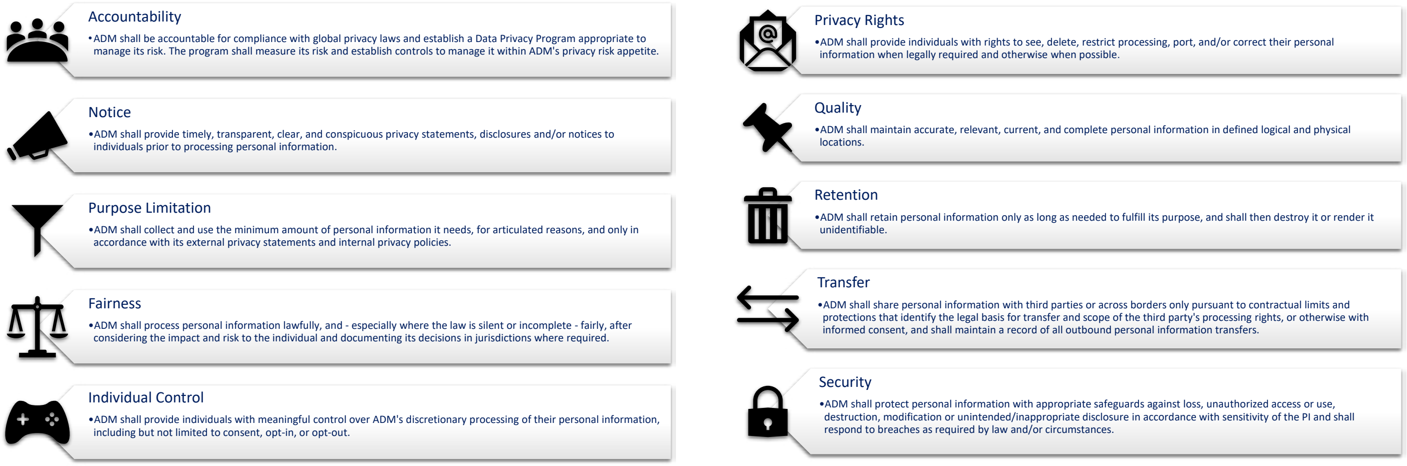
Data quality

Security safeguards

Transparency

Individual participation

FIGURE 6: ADM Privacy Principles Internal Communication



Accountability

- ADM shall be accountable for compliance with global privacy laws and establish a Data Privacy Program appropriate to manage its risk. The program shall measure its risk and establish controls to manage it within ADM's privacy risk appetite.

Notice

- ADM shall provide timely, transparent, clear, and conspicuous privacy statements, disclosures and/or notices to individuals prior to processing personal information.

Purpose Limitation

- ADM shall collect and use the minimum amount of personal information it needs, for articulated reasons, and only in accordance with its external privacy statements and internal privacy policies.

Fairness

- ADM shall process personal information lawfully, and - especially where the law is silent or incomplete - fairly, after considering the impact and risk to the individual and documenting its decisions in jurisdictions where required.

Individual Control

- ADM shall provide individuals with meaningful control over ADM's discretionary processing of their personal information, including but not limited to consent, opt-in, or opt-out.

Privacy Rights

- ADM shall provide individuals with rights to see, delete, restrict processing, port, and/or correct their personal information when legally required and otherwise when possible.

Quality

- ADM shall maintain accurate, relevant, current, and complete personal information in defined logical and physical locations.

Retention

- ADM shall retain personal information only as long as needed to fulfill its purpose, and shall then destroy it or render it unidentifiable.

Transfer

- ADM shall share personal information with third parties or across borders only pursuant to contractual limits and protections that identify the legal basis for transfer and scope of the third party's processing rights, or otherwise with informed consent, and shall maintain a record of all outbound personal information transfers.

Security

- ADM shall protect personal information with appropriate safeguards against loss, unauthorized access or use, destruction, modification or unintended/inappropriate disclosure in accordance with sensitivity of the PI and shall respond to breaches as required by law and/or circumstances.

PRIVACY BY DESIGN

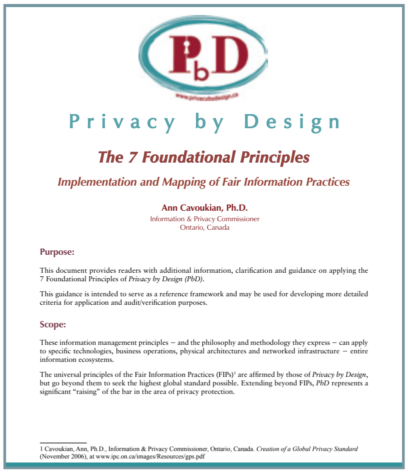
In order to shift from being reactive to more preventative and proactive, it is important to implement Privacy by Design as you plan and develop new products and services. As companies become more digital in nature, many products and services will become digital themselves.

Privacy by Design will be essential at the earliest stages of product development or creation of new service. The principles behind Privacy by Design are a way for you to operationalize the privacy principles outlined above.

> Organizations need to consider data privacy from the first moment they plan to develop a product or service.

Privacy by Design will factor in your guiding privacy principles and operationalize them in your product development process. There are available resources that go into comprehensive detail about what Privacy by Design is intended to accomplish. One helpful resource that is widely referenced is authored by Ann Cavoukian, the former Information and Privacy Commissioner of Ontario. Ms. Cavoukian's publication ***Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices*** outlines the following principles:

1. Proactive not reactive; preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum not zero-sum
5. End to end security – full cycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric



Privacy by Design

The 7 Foundational Principles

Implementation and Mapping of Fair Information Practices

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Purpose:

This document provides readers with additional information, clarification and guidance on applying the 7 Foundational Principles of *Privacy by Design (PbD)*.

This guidance is intended to serve as a reference framework and may be used for developing more detailed criteria for application and audit/verification purposes.

Scope:

These information management principles – and the philosophy and methodology they express – can apply to specific technologies, business operations, physical architectures and networked infrastructure – entire information ecosystems.

The universal principles of the Fair Information Practices (FIPs)[1] are affirmed by those of *Privacy by Design*, but go beyond them to seek the highest global standard possible. Extending beyond FIPs, *PbD* represents a significant "raising" of the bar in the area of privacy protection.

[1] Cavoukian, Ann, Ph.D., Information & Privacy Commissioner, Ontario, Canada. *Creation of a Global Privacy Standard* (November 2006), at www.ipc.on.ca/images/Resources/gps.pdf

DATA PRIVACY AND THIRD PARTIES

In terms of data privacy not only do you need to consider how you are managing data internally, it is critical to consider how this data is being shared with or used by third parties. Different departments and/or different geographic locations need to be considered with how you manage the data internally. Each of the departments or locations can also have a network of third parties through which it is sharing or using data.

Third parties are a key consideration in designing and managing your data privacy program. Think about all of the third parties that your company works with that may access your data. Depending on the nature of your business they may be payroll processors, law firms, marketing agencies, distributors, contract manufacturers, cloud-service providers. The list goes on and on. Each of them may be considered a controller and/or a processor under many data privacy laws.

Data Controllers and Processors

In order to understand the degrees of risk in third party relationships you need to understand each of the role of data Controllers and Processors. A third party can be a controller and a processor.

> As with other compliance issues, third parties are one of your highest risk areas for data privacy and data protection.

✓ **CONTROLLER** determines the purpose of the data and how it is collected and used

✓ **PROCESSOR** processes the data on behalf of the controller

Here are three real-life business examples that can help you understand the nuances – which can be complicated.

1. **COMPANY IS CONTROLLER AND PROCESSOR – THIRD PARTY IS NEITHER:**
   Company A is a U.S home décor online store. It was formerly a 'bricks and mortar' retail store, but has closed its physical locations and shifted to online sales. Company A has arranged for mutual sharing of new customer contact information with Company B, which is a similar U.S. online store, but also sends printed catalogs and has a few physical sales locations. Companies A &B will share new contact information of U.S. customers with each other via weekly feeds, provided the customers did not opt-out of marketing activities. Companies A & B are Controllers of their own information, but once they share the leads with each other, the data is considered the recipient's data and will be used by the recipient in accordance with its own privacy notice.

2. **COMPANY IS CONTROLLER – THIRD PARTY IS PROCESSOR:**
   Company A is an employer; Company B is a consulting firm, who will perform a benefits utilization analysis of Company A's team members. Company A as Controller will control and direct the purpose and means of processing to be undertaken by Company B, the Processor. Company B may not use the personal data for its own purposes, or perform any processing activities that are not at the direction of Company A.

3. **COMPANY AND THIRD PARTY ARE BOTH CONTROLLERS AND PROCESSORS:**
   Company A is an EU subsidiary of Company B. Company A collects information concerning its employees, to locally administer employee payroll, benefits and related processes. Company A also transfers its employee data to its U.S. parent, who independently processes this employee data in the context of administering the larger company (address books, company training or other initiatives). Company A and B are each independent controllers and processors of the employee data.

Controller and Processor Example

Your website collects the email addresses, IP addresses and some other personal data to use in marketing. All of the data collected is then sent on to your marketing agency to run a digital marketing campaign. If you provide the data and the instructions to the marketing agency, then you are the data controller and the agency is the data processor. If you provide the data to the agency and they design and implement the campaign then you are both data controllers and the agency is the data processor.

Reducing data privacy risk with third parties is a shared responsibility between your company and the third party. You should have controls in place for assessing and managing the risk a third party poses. One critical element in making this work is having the internal cooperation and commitment from the people in your company that own the third-party relationship. This goes back to the importance of cross-functional collaboration. You need to make sure that the third party is getting a consistent message about the importance of data privacy.

The privacy impact assessment process we outline in the next section is designed to get you and your business units on the same page around assessing risk and communicating the needed actions to reduce the risk. Most companies today have third parties in different jurisdictions (e.g. countries, states) so the legal considerations need to be taken into account in your communications with third parties.

Managing Third-Party Relationships

Third-party management is a critical area. Regardless of the compliance risk topic, third parties are involved in the majority of cases. Ensuring compliance by third parties over whom you may have little control can be a complex task. You should work proactively with your third parties to ensure that they are complying with your data privacy policies and requirements. Specific elements of a solid third-party risk management program include:

- ✓ Risk ranking your third parties based on their role, the data involved, and the maturity of their internal controls
- ✓ Performing appropriate due diligence
- ✓ Making sure your contracts are aligned with relevant regulations and your policies
- ✓ Communicating your data privacy expectations beyond the contract
- ✓ Monitoring their performance throughout the life cycle of the relationship

Effective third-party management involves cross-functional collaboration. Discuss your compliance requirements with the internal department that owns the third-party relationship. They need to be able to communicate the expectations and obligations beyond the contract to the third parties.

To make your third-party program practical, start with the highest risk third parties. As you introduce a new compliance program, like one for data privacy, you will need to take two tracks.

For new third parties:

- ✓ Integrate data privacy due diligence into the evaluation and selection process
- ✓ Communicate your relevant data privacy expectations as part of the onboarding process

For existing third parties:

- ✓ Communicate with them about your new data privacy program
- ✓ Stress that it is to your mutual benefit to reduce relevant data privacy risks
- ✓ Highlight the importance of the business relationship and seek their cooperation in joining with you to reduce risk

Evaluating a third party's data privacy protection capabilities and controls is often a collaborative process between you and your information security or cybersecurity departments. The appropriate level of evaluation will depend on the type of data involved and the risk. It is important for there to be clarity about which department has the final authority to approve or deny contracting with a third party.

> Make sure that there is alignment between the data privacy provisions in your contracts, your due diligence checklist, your communications and your monitoring program.

Once a third party has been approved, it is important to have some level of performance monitoring that specifically looks at data privacy. Too often companies sign contracts with third parties and fail to monitor if the third party is meeting their contractual obligations for protecting data. Don't wait until a problem happens to check on how things are running. One consideration for you is who is responsible for the monitoring: the information security team or the third-party relationship owner. Regardless of who has primary responsibility, you should include data privacy into the ongoing communications between your business unit and the third party.

SECTION 2:

PRIVACY IMPACT RISK ASSESSMENT: TOOLS & WORKFLOW

KEY CONSIDERATIONS FOR GETTING STARTED

One of the most important activities in your role as a Privacy Leader is building and managing the data privacy risk assessment process. This process establishes the flow of information between you and the business units, assesses the level of risk and determines the controls needed to mitigate the risk. You are also responsible for record-keeping and then reporting to various audiences. Ultimately the audience could range from senior management to the board or governing body to regulators.

An important consideration in building a practical program is what level of impact assessment is needed based on the data and the governing jurisdiction. The process that we have outlined here has two levels of data assessment in order the streamline your workflow based on the risk and your company's risk tolerance.

For your company to implement a well-integrated data privacy strategy, you should start by evaluating the inherent risk and the residual risk related to legal violations or the compromise of the data. Inherent risk is the level of risk posed by the situation assuming no controls are in place. Questions you should be asking or thinking about include:

- ✓ What are the highest risk uses of the data?
- ✓ How attractive is certain data to hackers?
- ✓ Who has access to the data in the normal course of business?

As you develop a more mature data privacy program and implement appropriate controls, you reduce the inherent risks to an acceptable residual risk level.

A critical part of an effective data privacy program is understanding and setting an acceptable level of residual risk for data privacy. *How much risk will your company tolerate in a given transaction?* One of the challenges you will have is establishing a consistent risk tolerance throughout your company.

> The term Data Privacy Impact Assessment (DPIA) is specific to the requirements of GDPR. A DPIA is required if the data or type of processing is considered high-risk. More on this in a few pages.

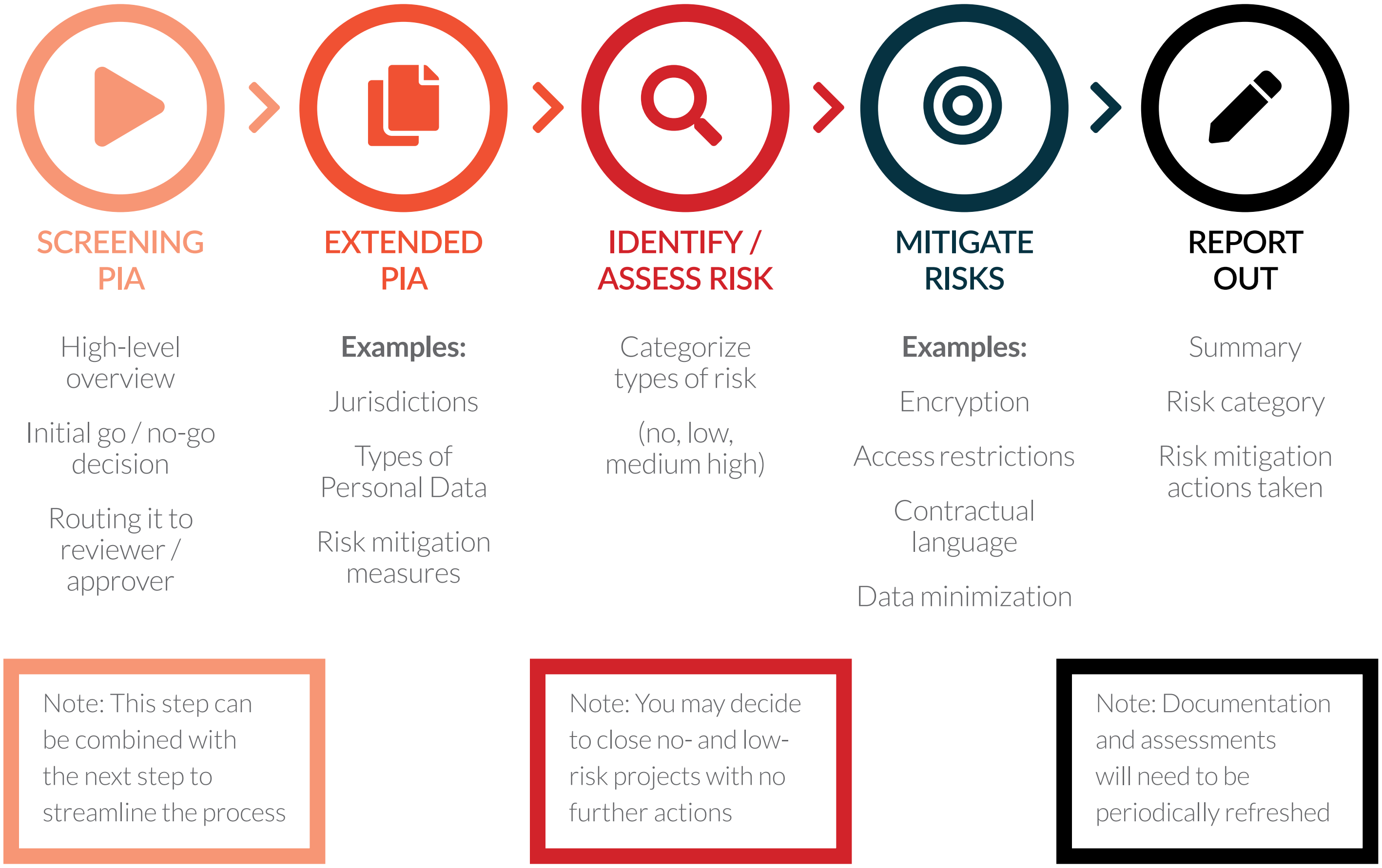
Important Terminology

These are commonly used terms that describe the same thing. The term used varies from company to company. As we mentioned in the beginning, in this guide we are using the term privacy impact assessment.

- ✓ Privacy impact assessment (PIA)
- ✓ Data privacy assessment
- ✓ Data protection assessment

Here is a diagram showing an overview of the workflow. We go into more detail on each step in the process and we provide a form you can use to get your assessment process started.

FIGURE 7: Privacy Impact Assessment (PIA) Overview



SCREENING PIA

High-level overview

Initial go / no-go decision

Routing it to reviewer / approver

Note: This step can be combined with the next step to streamline the process

EXTENDED PIA

Examples:

Jurisdictions

Types of Personal Data

Risk mitigation measures

IDENTIFY / ASSESS RISK

Categorize types of risk

(no, low, medium high)

Note: You may decide to close no- and low-risk projects with no further actions

MITIGATE RISKS

Examples:

Encryption

Access restrictions

Contractual language

Data minimization

REPORT OUT

Summary

Risk category

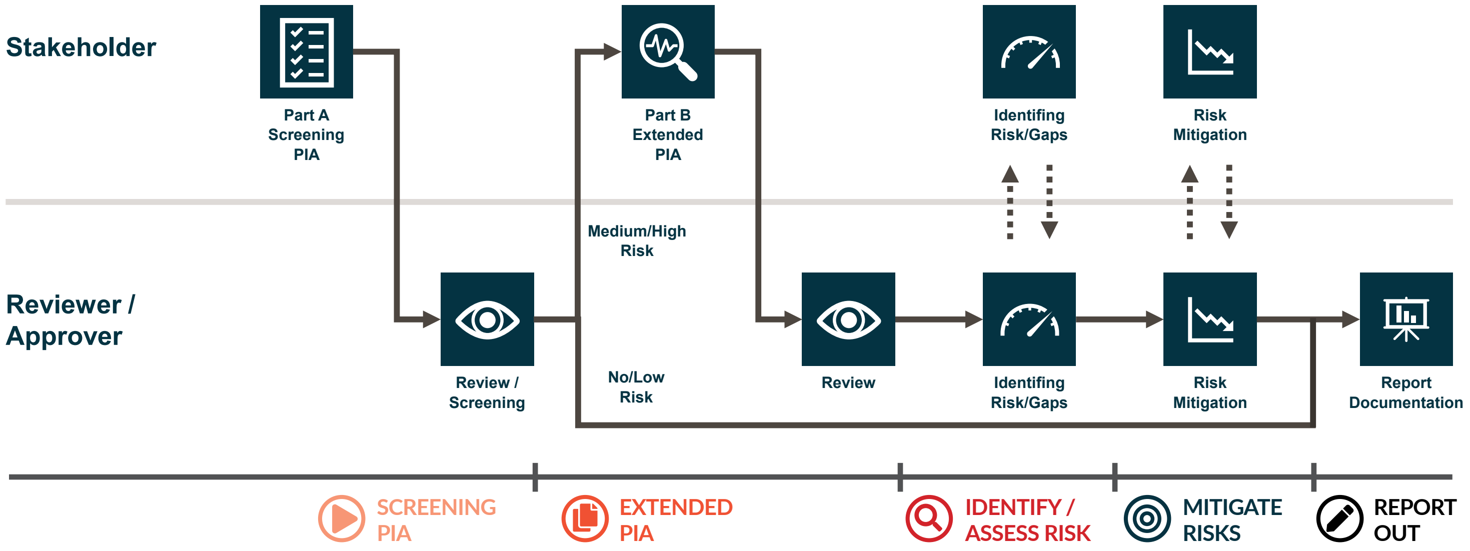
Risk mitigation actions taken

Note: Documentation and assessments will need to be periodically refreshed

The following diagram illustrates the step-by-step process of how you would manage the privacy impact assessment workflow. In the following diagram, you are the Reviewer/Approver and the Stakeholders are typically going to be your business units.

Depending on the nature of your business, you could be dealing with hundreds or even thousands of privacy impact assessments each year. It is critical to develop a workflow that is practical and scalable. For this reason, we recommend two levels of privacy impact assessment: an initial screening and, if warranted, an Extended Privacy Impact Assessment (PIA). In some jurisdictions, the Extended PIA may need to meet certain legal requirements (e.g. the Data Protection Impact Assessment for GDPR in Europe).

FIGURE 8: Privacy Impact Assessment (PIA) Overview - continued



PRIVACY IMPACT ASSESSMENT INTAKE FORM

In this guide we provide a privacy impact assessment intake form that is divided into two parts:

- ✓ **Part A** is used to conduct the initial Screening PIA
- ✓ **Part B** is used as a more thorough Extended PIA if required

The form is designed for you to use to collect data and to educate the business units on Personally Identifiable Information (PII). Here we provide a definition of PII and some examples. These are also included on the form to help you educate your business units on PII and get more reliable and consistent answers from your various business units.

Click here to access the Intake Form which you can use as a template >

SCREENING PRIVACY IMPACT ASSESSMENT

A key part of the initial screening process is to determine what data is being collected and the relevant regulatory issues in the jurisdiction that may apply. The form is completed by the business unit and returned to you. You should then know what data is being collected and how it is being used. Next, review the results of initial screening to determine the regulatory issues and whether it will require an Extended PIA.

The purpose of the Screening PIA (Part A of the form) is to ask the business unit a series of simple questions concerning the project/product/service and exactly what info is collected, stored, transferred and accessed. It also specifically asks about the involvement of third parties.

The business unit needs to provide you with the answers to basic questions like these so you can determine the risk level and the degree of review and risk mitigation required.

- ✓ What is the purpose and proposed use of the personal data processing?
- ✓ Who are the proposed personal data subjects?
- ✓ What types of personal data will be processed?
- ✓ Where are the data subjects and corresponding systems located?
- ✓ Will third parties be involved, what is their role & what data rights will they have?
- ✓ Who will have access to the personal data?

Click here to access a sample Intake Form.

You will be using **Part A** in this step and **Part B** in the next step.

The business unit is responsible for completing Part A and returning it to you for review. Based on your initial review of the data involved, any third parties involved and the associated risk, you will determine if the business unit needs to complete Part B and proceed to an Extended PIA. If an extended PIA is needed you will need to determine if a formal Data Protection Impact Assessment (DPIA), as defined by GDPR, and other similar regulations, is required.

Use the Intake Form as part of your communication program to reinforce your data privacy training by including some definitions and examples.

The purpose of this initial stage is to screen out those situations that are low risk so you can streamline your workflow. If no further action is needed, you can end the assessment process and move the completed Part A of the form directly to the reporting stage.

Here's a list of what CCPA defines as personal information:

- ✓ Direct identifiers: legal name, postal address, social security number, driver's license number or photo, passport information, signature
- ✓ Indirect identifiers: IP addresses, account usernames, cookies, pixel tags, telephone numbers
- ✓ Biometric data: face, retina, fingerprints, voice recordings, health data
- ✓ Geolocation data: device location history
- ✓ Internet activity: search history, browsing history, webpage interaction, advertising interaction
- ✓ Sensitive information: race, ethnicity, religious or political convictions, sexual preferences, employment and education data, financial and medical information

EXTENDED PRIVACY IMPACT ASSESSMENT

Based on your review of Part A, the assessment process may continue. If the initial screening shows there is sensitive or personal data involved, your business unit will probably need to conduct the Extended PIA and complete Part B.

Here are examples of special data categories that would typically require an Extended PIA:

- racial or ethnic origin
- political affiliations
- religious affiliations or beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Data Protection Impact Assessment (DPIA)

Some regulations require a specific type of Extended PIA. The Data Protection Impact Assessment (DPIA) is a legal requirement of GDPR. This specific type of Extended PIA is triggered if data subjects are in the EU jurisdiction and certain data is involved and/or if certain data uses are planned that are considered "high-risk."

GDPR is somewhat vague on their definition of high-risk, but here are some generally accepted guidelines for what would be considered high-risk data or use.

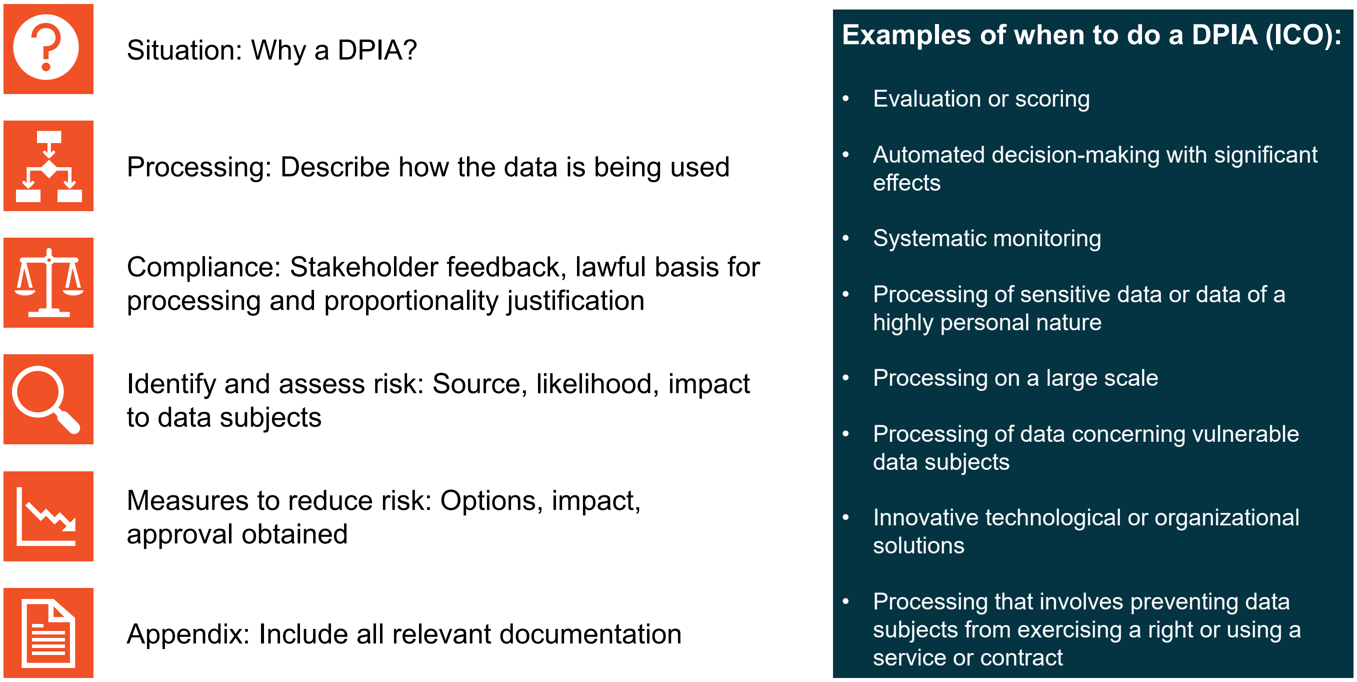
- Collecting data tracking an individual's location or behavior
- Processing personal data related to race, religion, political opinions, trade union membership, sexual orientation

- ✓ Processing genetic or biometric data linked to an individual
- ✓ Collecting or processing children's data
- ✓ Using artificial intelligence / machine learning (A(/ML) to process data and/or make automated decisions
- ✓ If public disclosure of the data could potentially result in physical harm to the individual

There may be other specific legal assessments required by other jurisdictions, so you do need to be aware of new laws and requirements.

Here's a diagram that shows the foundational elements of a DPIA – what it consists of and when it is needed.

FIGURE 9: Data Protection Impact Assessment (DPIA)



Situation: Why a DPIA?

Processing: Describe how the data is being used

Compliance: Stakeholder feedback, lawful basis for processing and proportionality justification

Identify and assess risk: Source, likelihood, impact to data subjects

Measures to reduce risk: Options, impact, approval obtained

Appendix: Include all relevant documentation

Examples of when to do a DPIA (ICO):

- Evaluation or scoring
- Automated decision-making with significant effects
- Systematic monitoring
- Processing of sensitive data or data of a highly personal nature
- Processing on a large scale
- Processing of data concerning vulnerable data subjects
- Innovative technological or organizational solutions
- Processing that involves preventing data subjects from exercising a right or using a service or contract

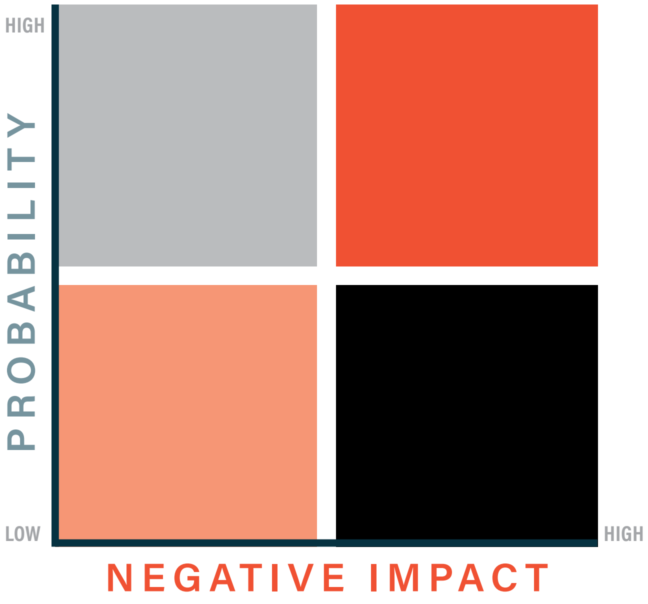
IDENTIFY & ASSESS RISK

At this point in the Extended PIA workflow, you have received the completed Part B of the intake form. Depending on what you find, the risk assessment process may become even more rigorous depending on the data and its use. The most efficient way to identify and assess risk is to have a risk ranking process in place. The risk tolerance of your organization will determine how the risk is classified, and the extent of the mitigation actions required. Most companies have three levels of risk classification: low, medium and high (aka green, yellow, red). Establishing clear risk classification guidelines and agreed upon definitions is critical for minimizing problems along the way. Don't wait until there are problems to establish them.

Establishing agreed upon risk classifications guidelines is an important step in building your data privacy program. It is important to get cross-functional input and senior management approval in the beginning.

One important consideration in conducting your risk assessment is to think about the probability of pre-mortem, i.e., something bad happening, and then to think about the negative impact it would have if it did happen. Here's a simple, useful tool that is commonly used to assess probability and negative impact for all types of risks. You can use it to map your data privacy risks. Obviously, anything that has a high probability and a high negative impact should be prioritized for mitigation in the next stage of your workflow. Conversely, it does not make sense to spend much time, money or political capital on anything that has a low probability and a low negative impact. The hardest decisions are around situations that have a very low probability but a very high potential negative impact. There are many examples of companies that were completely unprepared for low probability situations that did occur with devastating results.

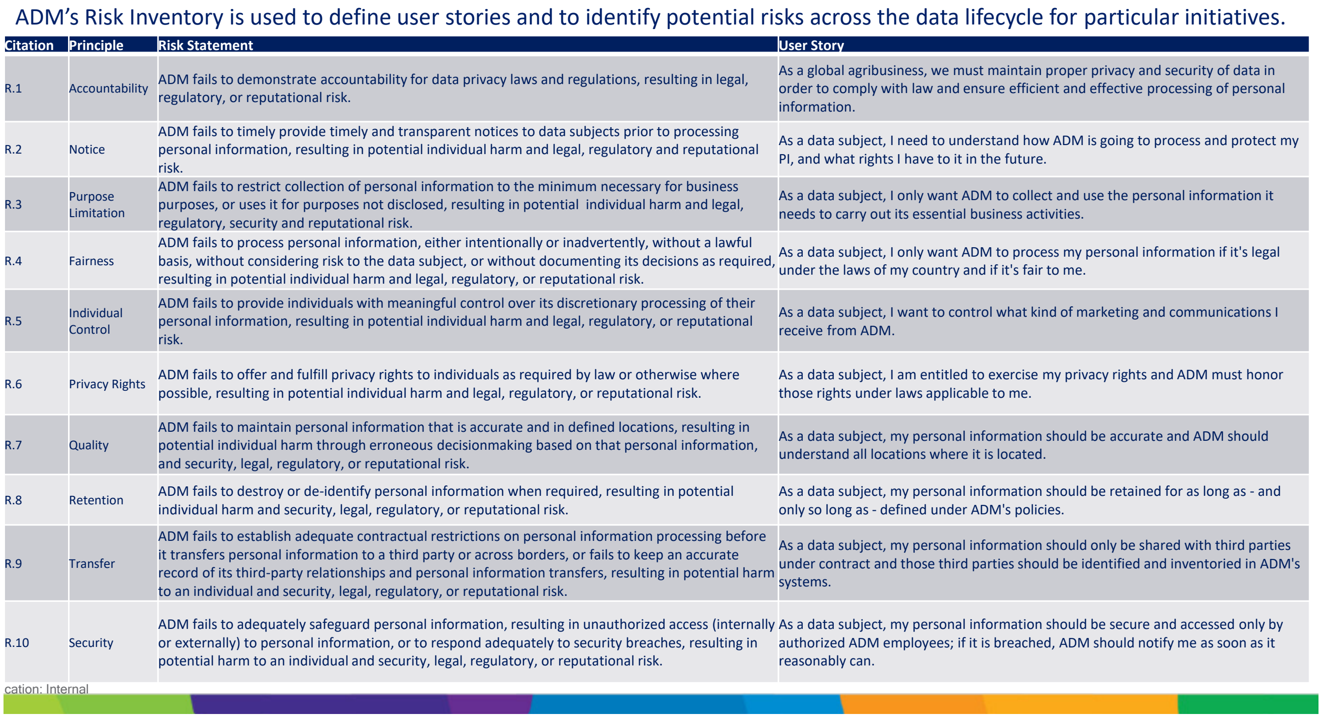
FIGURE 10: Risk Probability/Impact Quadrant



Assessing the risks is a critical step, but communicating them to the business units and relevant third parties must be part of the overall cycle. Without the communication, data privacy will end up in a silo. Here's an example of how one company categories risk and illustrates it through the use of stories.

Referencing again the ACC 2021 Chief Legal Officers Survey, "**about one quarter of respondents**" indicated that the data privacy and data security functions are responsible for managing legal risk.

FIGURE 11: ADM's Privacy Risks and User Stories



ADM's Risk Inventory is used to define user stories and to identify potential risks across the data lifecycle for particular initiatives.

Citation	Principle	Risk Statement	User Story
R.1	Accountability	ADM fails to demonstrate accountability for data privacy laws and regulations, resulting in legal, regulatory, or reputational risk.	As a global agribusiness, we must maintain proper privacy and security of data in order to comply with law and ensure efficient and effective processing of personal information.
R.2	Notice	ADM fails to timely provide timely and transparent notices to data subjects prior to processing personal information, resulting in potential individual harm and legal, regulatory and reputational risk.	As a data subject, I need to understand how ADM is going to process and protect my PI, and what rights I have to it in the future.
R.3	Purpose Limitation	ADM fails to restrict collection of personal information to the minimum necessary for business purposes, or uses it for purposes not disclosed, resulting in potential individual harm and legal, regulatory, security and reputational risk.	As a data subject, I only want ADM to collect and use the personal information it needs to carry out its essential business activities.
R.4	Fairness	ADM fails to process personal information, either intentionally or inadvertently, without a lawful basis, without considering risk to the data subject, or without documenting its decisions as required, resulting in potential individual harm and legal, regulatory, or reputational risk.	As a data subject, I only want ADM to process my personal information if it's legal under the laws of my country and if it's fair to me.
R.5	Individual Control	ADM fails to provide individuals with meaningful control over its discretionary processing of their personal information, resulting in potential individual harm and legal, regulatory, or reputational risk.	As a data subject, I want to control what kind of marketing and communications I receive from ADM.
R.6	Privacy Rights	ADM fails to offer and fulfill privacy rights to individuals as required by law or otherwise where possible, resulting in potential individual harm and legal, regulatory, or reputational risk.	As a data subject, I am entitled to exercise my privacy rights and ADM must honor those rights under laws applicable to me.
R.7	Quality	ADM fails to maintain personal information that is accurate and in defined locations, resulting in potential individual harm through erroneous decisionmaking based on that personal information, and security, legal, regulatory, or reputational risk.	As a data subject, my personal information should be accurate and ADM should understand all locations where it is located.
R.8	Retention	ADM fails to destroy or de-identify personal information when required, resulting in potential individual harm and security, legal, regulatory, or reputational risk.	As a data subject, my personal information should be retained for as long as - and only so long as - defined under ADM's policies.
R.9	Transfer	ADM fails to establish adequate contractual restrictions on personal information processing before it transfers personal information to a third party or across borders, or fails to keep an accurate record of its third-party relationships and personal information transfers, resulting in potential harm to an individual and security, legal, regulatory, or reputational risk.	As a data subject, my personal information should only be shared with third parties under contract and those third parties should be identified and inventoried in ADM's systems.
R.10	Security	ADM fails to adequately safeguard personal information, resulting in unauthorized access (internally or externally) to personal information, or to respond adequately to security breaches, resulting in potential harm to an individual and security, legal, regulatory, or reputational risk.	As a data subject, my personal information should be secure and accessed only by authorized ADM employees; if it is breached, ADM should notify me as soon as it reasonably can.

cation: Internal

MITIGATE RISKS

Once the risks have been identified and assessed, the next step is to take appropriate actions to mitigate the risks. As we mentioned earlier in this guide, the purpose of your program is to reduce risks to an acceptable level, not to eliminate them. In the Identify and Access stage you are evaluating the inherent risk, in this stage you are determining what controls should be put in place to establish an acceptable level of residual risk.

Risk mitigation is another area where cross-functional collaboration is critical. Although you may be responsible for recommending (or requiring) how you want the risk to be mitigated, the implementation is definitely a joint effort. Implementing the specific recommendations may involve your information security or cybersecurity departments. In many companies the ultimate responsibility for the effective implementation of the controls lies with the business unit. If the risk mitigation efforts extend to third parties, the relationship-owner must be involved in communicating the expectations.

As we have said throughout this guide, communication is a critical element of building an effective data privacy program. The critical role of communication is clearly on display with risk mitigation. This is true with your internal departments and with relevant third parties. As we mentioned in the section on training and communications, effectiveness hinges on three goals: build awareness, gain commitment, and explain what action is needed. At this stage, the focus is on explaining what action is needed (hopefully you have already succeeded in building awareness and gaining commitment).

> Be explicit about what controls or processes need to be in place to mitigate the risk. Make sure there is acknowledgement by the other party that they agree with the recommendations and will implement them by the established deadline.

The next step in effective risk mitigation is monitoring. You need to have some method of checking to see that the controls or processes were implemented as agreed and that they are working. Different companies have different approaches to monitoring. Some treat it as a policing activity. We suggest that you position monitoring as a shared learning process. You are collaborating with the business unit and/or third party to see if the controls are practical to implement and if they are working. This creates a more transparent relationship where you all share a common goal of embedding data privacy in operations.

You may want to use a table like this to capture and record the risk levels and begin the risk mitigation process. We've added a few examples. You can expand it to track progress too.

Risk Level from the Identify & Assess Stage	Situation	Jurisdictional Considerations	Suggested Mitigation Action	Responsible Party(ies)	Status of Mitigation Action
Low	Authentication for using an app that otherwise does not process PII	none	Contractual provisions	Product Development	complete
Moderate	Direct marketing campaign	CCPA	Update data map and data deletion process	Marketing, Info Sec, Marketing Agency	Complete – checking effectiveness
High	Large-scale customer data processing	GDPR	Full DPIA	Privacy Officer, Info Sec, Cybersecurity, Marketing, Data Analytics Firm	Underway

REPORT OUT

The last stage in the PIA workflow is reporting and the related record-keeping. There are different important audiences for reporting and record-keeping.

- Senior management
- Board or governing body
- Relevant business unit
- Relevant third-party
- Regulators

The central documents in the workflow are the intake form (Part A and Part B), the risk assessment, the risk mitigation plan and the monitoring.

As the Privacy Leader, you are responsible for collecting the relevant information for the reports, aggregating the information as needed to report to the various audiences, and maintaining the appropriate records.

BUSINESS ETHICS
LEADERSHIP
ALLIANCE™
An Ethisphere Community

Ethisphere's Business Ethics Leadership Alliance (BELA) is a global community of companies who recognize the inherent value of ethical leadership and who are working together to move business forward with ethics and integrity. BELA members are senior legal, ethics, and compliance leaders from 60+ industries in more than 330 companies worldwide. The community shares best practices and expertise and has access to exclusive data, benchmarking, and opportunities to showcase their programs.

Please see bela.ethisphere.com to learn more.