ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How to Build a Privacy Program from Scratch

Intellectual Property

Technology, Privacy, and eCommerce

Cheat Sheet

- **Data mapping.** The basic building block on which the entire privacy compliance program is constructed.
- **Policies and procedures.** Implement a data governance policy, as well as policies that control the company's collection, use, and deletion of personal information.
- **Privacy notices.** Notices should tell individuals what personal information a company is collecting, and how they can exercise their privacy rights.
- **Contracts.** Be sure the company's contracts address the use and disclosure of personal information that is being exchanged with third parties.

The privacy law landscape has changed rapidly and dramatically in the past three years. The EU General Data Protection Regulation (GDPR) became effective in May 2018; California's wide-ranging privacy law went into effect in January 2020; and this year, Virginia joined the fray with its own privacy law. Many other US states are considering similar legislation, and a federal bill is also pending.

Over the next few years, companies can expect that their privacy law compliance obligations will only increase in complexity and scope. Given these new and significant compliance burdens, many companies are still in the relatively early stages of building their privacy programs. By following the steps in this article and taking a proactive and systematic approach to privacy compliance, companies will increase operational efficiencies, engender customer confidence, and reduce their risk.

Data inventories and maps

The first step in creating a privacy program is to map the data that your organization holds. A data map is an inventory of facts on how data is collected, used, shared, retained, and secured by the organization. It also provides information about the people involved, internal business functions, external parties, and systems related to those data collection and processing activities.

Why do you need a data map?

Many organizations decentralize the collection of information and often operate independently when collecting data. This may lead to duplicative collection and storage, as well as a few surprises. For example, companies that are not consumer-facing may be surprised to learn they are collecting and processing credit card information.

Data mapping allows you to build a program based on facts, rather than a theoretical view of the organization’s data practices. From there, you can better understand, assess, and document the legal and compliance risks, as well as steps taken to reduce those risks.

Where do you start?

Engage leadership.

For many professionals new to data mapping, it can seem daunting to conduct one. Before you jump right in, you will want to engage leadership and obtain buy-in. You will be asking for the time and energy of colleagues throughout the organization who may not see this exercise as a priority. Having support and direction from leadership will be critical to demonstrate the importance of their contributions.

Collect data.

While there are automated tools that can streamline some of the data collection, for the most part, the process itself is still largely manual (e.g., collecting data via interviews). Many professionals start with a questionnaire to understand the scope of the exercise — specifically, to uncover where the data is being held and to identify the data owners in the organization.

Use what you’ve learned.

While a lot of work on the front end, data mapping will save time in the long run. To understand the laws that apply to your organization, you need an accurate assessment of the types of data you collect, as well as how you are using and processing data as an organization. That information is also helpful in creating a framework for the various data types as they flow through your organization.

If you have a breach, you will know where the data is being held, and if you have a request from a data owner, you will know what you have and where to look. Further, for any new projects or business processes, you can easily assign risks based on the data types involved, and more efficiently manage risk by applying standard procedures to similar projects or initiatives.

Policies and procedures

Once your data mapping is complete, you can start to formulate written policies and procedures that govern how the company processes personal information. As you create the policies discussed in this section, remember to involve any key businesspeople in your company so that the policies align with the company's actual practices and business needs.

Where do you start?

At the outset, you should consider whether to implement a written data governance policy that identifies who at the company is responsible for different sets of personal information (i.e., data stewards) along with the privacy-related principles that your company will use to guide its handling and use of personal information.

Identifying data stewards will help to ensure that the company follows the privacy policies that it promulgates. Furthermore, by having certain principles in place and endorsed by company leadership, you and others at the company will be able to look to them for guidance when facing a situation where other policies do not clearly define how to respond.

Consider including the following principles (all drawn from the GDPR) in your data governance policy.

- The company will process personal information in accordance with applicable laws and in a manner that is transparent to data subjects (e.g., the individuals to whom the information relates).
- The company will collect personal information for specific and legitimate purposes and not further process that personal information in a manner that is incompatible with those purposes.
- The company will limit its collection of personal information to information that is relevant and necessary for its purposes.
- The company will strive to maintain accurate and up-to-date personal information.
- The company will keep personal information for no longer than is necessary for the purposes for which the personal information is processed.
- The company will maintain appropriate technical, administrative, and physical security measures to protect the personal information against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- The company will properly document its compliance with applicable privacy laws so that it can demonstrate that compliance if necessary.

What other policies are needed?

Consider the various stages of the "data lifecycle" and designing policies that address each phase.

Data collection

If your company is considering collecting a new set of personal information, you may want a policy that instructs the company to conduct a privacy impact assessment. The assessment will allow you to weigh the potential benefits of collecting the information against any risks to the privacy of the data subjects, so you can determine potential risk mitigation strategies.

The company should seek to provide privacy notices to data subjects at or before the point of collection of their personal information, so the data subjects have a full understanding of what happens with their data. For this reason, create a policy that describes the circumstances in which the company will provide a privacy notice to a data subject, as well as what information needs to be included in such notice.

Finally, consider a policy relating to your company’s data map or data inventory so when a new set of personal information is collected, the map or inventory is updated accordingly.

Data use

The next stage of the data lifecycle addresses the company’s use of personal information after collection. It is important to create policies that designate who is permitted to access different types of data, as well as delineate the purposes for which data may be used.

For instance, will all employees have access to all personal information collected by your company? Will your company combine or synthesize personal information across different data sets? What technical measures will your company put in place to maintain any access and use restrictions, and will employees who break these rules face discipline? Your written policies can set out these rules in a clear way.

Privacy laws can provide a variety of rights to data subjects. If your company is collecting personal information, you can expect to receive inquiries and requests from data subjects who want to exercise these privacy rights.

Consider creating a policy that dictates how your company will respond to such requests, considering things like how the company will verify the identity of the person making the request, what exceptions might apply, and how the company will ensure it adheres to the request.

Data protection

Next, you should address how the company will protect the personal information it processes against loss, theft, and unauthorized disclosure. Many companies create written information security policies that describe the administrative, technical, and physical measures they maintain to protect personal information.

Those policies might require the company to conduct regular risk assessments to identify new or changed threats and close any gaps in their defenses. Consider creating a written security incident response plan so that if your company suffers a data security or privacy incident, it will know how to deal with the incident quickly and effectively.

Data disclosure

You will then want to consider policies that apply to your company’s disclosure of personal information to third parties. Such policies could address when to attach a “Data Protection Addendum” to a contract with a vendor or a customer, as well as what due diligence the company should undertake prior to bringing on a new vendor.

If your company intends to transfer personal information across country borders, consider a policy that addresses how the company will comply with any privacy law-imposed restrictions on such transfers. For instance, if your company will be transferring personal information from the European Union to the United States, which of the approved data transfer mechanisms (e.g., standard contractual clauses, binding corporate rules, etc.) will be put in place to protect the data being transferred?

Setting this out in a written policy will help the company to both recognize when such data transfer mechanisms are required, and select the appropriate mechanism for any particular transfer.

> The company should seek to provide privacy notices to data subjects at or before the point of collection of their personal information, so the data subjects have a full understanding of what happens with their data.

Data retention

The last stage of the data lifecycle is the retention and destruction of the personal information. You can create a policy that defines the circumstances when the company will dispose of personal information, as well as how the data will be securely disposed.

If the company will be storing or archiving the personal information, a data retention schedule can help set the dates on which the data will be destroyed. Setting and following a data retention schedule will reduce the amount of personal information your company controls and, in turn, reduce the level of exposure if the company suffers a breach.

Training and management

Two final matters to consider with your written policies are training and policy management. Who will be responsible for training your company’s employees in connection with these policies, and how will that training be delivered and recorded? Who will be responsible for managing these policies, both for updating purposes and for enforcing them? It is important to identify the people or roles that are assigned these tasks so that the company complies with its own policies.

Privacy notices

There is no overarching US federal law requiring a privacy notice. However, some industry-specific laws (HIPAA, GLBA, etc.), state laws, and the laws of an increasing number of non-US jurisdictions do require a privacy notice.

A well-constructed privacy notice provides data subjects and regulators alike with an accurate, transparent reflection of your company’s use of data in compliance with applicable law. A poorly constructed privacy notice invites the potential for complaints, regulatory scrutiny, and potential legal action.

To whom do you provide privacy notices?

Generally, if you are collecting, using, processing, or taking some other action with an individual's data, you should provide that individual with a privacy notice. It's important not to forget about our employees when crafting privacy notices, or internal privacy policies.

Companies often focus solely on customer, but it's important to remember thatin many cases, employee data may be the most sensitive data a company maintains. For instance, you may only collect the names and emails of customers, but you likely collect social security numbers health, , and financial information for employees.

When are they required?

Privacy notices are generally provided to the individual at the moment of data collection. However, in some cases you may be collecting data from a third party. For example, you may receive leads from a third-party partner; or an individual may purchase a product as a gift for another person and provide you with the gift recipient's personal data as part of that purchase. You'll need to determine when and how to present these individuals with your privacy notice.

Do you need to get consent?

Whether consent is required, and the type of consent needed, will depend on the applicable law, the type of data, the legal basis for processing data, and in some cases, the processing activities being carried out.

For instance, under the Children's Online Privacy Protection Act (COPPA), if you are collecting or processing the data of a child under the age of 13, you may need parental consent. Under the GDPR, explicit consent is required when processing special categories of personal data, such as sexual orientation or biometric data.

Privacy notice content

The information you include in a privacy policy will depend on what is required under the applicable law. At a minimum, a privacy notice will generally contain:

- *Contact information* – for both the organization and a responsible party to whom data subjects can direct questions or complaints related to the notice.
- *Data collection* – the types of data collected, the sources of data, and how it is collected. This will be informed by your data mapping exercise. As a note, depending on the applicable law, you may need an entirely separate Cookie Policy, but most privacy notices generally include a reference to cookies and the data collected using this technology.
- *Purpose of processing/legal basis* – this provides data subjects with an understanding of why and how their data is being used. Under the GDPR (Art. 6), this includes the legal bases you rely on to lawfully process data.
- *Recipients of the data* – the third parties with whom you share personal data. Certain laws, such as the GDPR and CCPA, require a greater level of granularity.
- *Data retention* – information regarding how long you retain personal data.
- *Data protection* – a high-level overview of the data protections in place.
- *Additional considerations* – depending on the applicable law, you may have to include items

like data transfers outside the European Union; rights of the data subject; data localization; or specific requirements mandated by federal laws. Remember that your privacy notice is a living document that will change over time based on changes in the law and business processes. Regularly review your privacy notice to ensure it’s up to date.

How do you respond to inquiries and requests?

Understand your obligations.

It’s critical to understand your obligations under applicable law when responding to requests. A number of privacy laws require you to respond within a specified timeframe, though extensions may be permitted under certain circumstances. You want to be sure you clearly understand what the data subject is asking — access to their information, erasure, opting out of the sale of their data, etc. Make sure you have a process in place to receive, evaluate, track, and respond to inquiries and requests.

Have a ready response.

Crafting a deliberate response beforehand will help ensure adherence to your obligations, deliver consistent messaging, and provide a better experience to your data subjects.

It's important to remember that even if a particular privacy law doesn’t apply, you may still need to be prepared to answer questions. For instance, non-profits are exempt under the CCPA. However, it’s likely that your members or customers may still ask questions about your CCPA compliance. While you don’t have to be an expert in all privacy laws, maintaining awareness of the changes in the privacy landscape and being prepared to respond to questions is critical.

Understand your business needs.

Even if a law doesn’t apply to you, it may apply to your corporate clients. Be prepared to respond to any potential requirements imposed by your clients as a result, and to find creative ways to address these issues. Your business team may decide to take a position on a particular privacy matter, even if they are not obligated to do so. For example, they may decide either as a logistical or public relations matter to simply give all data subjects the same rights of access, erasure, etc.

Contracts

Contracting can sometimes impose an even greater burden and financial liability on companies than many US laws, and if not managed properly, can create a web of requirements too tangled to unravel.

Despite the risks, contracting can also be an opportunity for risk mitigation. By creating a uniform approach to contracting, companies can limit their risk exposure and match their contracting provisions to their processes, rather than the other way around.

How do you approach the contract?

Before the redlining even begins, it is essential to understand how privacy fits within your organization. For example, does your organization’s systems and processes support the terms being asked and do you have coverage if something goes awry?

Understand your data.

Understand the type of data being exchanged and your organization’s position on security and risk. This is where your data mapping comes in handy. You should have a good understanding of the data types your organization is trying to protect and the laws that apply to that data. The type of data exchanged will impact the contract vehicle necessary to share the data, as well as baseline terms to be included (e.g., destruction of the data under HIPAA).

Understand your business.

Understanding the key business concerns is important in any contract, including understanding the leverage you have and how much risk the organization is willing to take on.
Understand your cyber insurance policy.

Who bears the cost associated with a breach is often contested, so it is important to know whether and how much your insurance policy will cover. Some policies will only cover legally required costs or will only allow costs where you are conducting the notices (no reimbursements).

Understand your systems.

While many laws take a flexible approach to security, contracts can include security protocols above and beyond regulatory levels. What standard do you use — NIST, ISO, etc.? What can you offer without requiring your IT to map controls? What are their concerns with giving access to your systems for audit purposes? Do you have an IT specialist to work with to go over these issues as they arise?

Understand your processes.

Often, major points of negotiation surround when notification is triggered and how fast. Understand your incident response policy so you know whether you can meet the timeline and content requirements of the customer. If receiving notification, understand how long you would need to provide proper notification.

Understanding these items, which can change over time, will make it much easier to tackle privacy provisions.

What are some common sticking points?

Privacy data is sensitive and valuable. Before an organization provides any data, there should be an agreement in place addressing (1) what it can be used for, (2) how to protect it, (3) responsibilities for a breach, and (4) when happens when the project is over.

Privacy contracts and provisions come in many forms and flavors: nondisclosure agreements, data sharing/use agreements, business associate agreements, etc. Aside from required regulatory language, below are examples of key issues to consider.

Check your definitions.

Know what an incident is, what a breach is, and who gets to make the determination of when one occurs (hint: you want it to be you). A safe harbor for encryption can protect both parties — ensuring security for the buyer and protection from losses for the vendor.

> While you don’t have to be an expert in all privacy laws, maintaining awareness of the changes in the privacy landscape and being prepared to respond to questions is critical.

Notification

Does an incident trigger notification or a breach? How fast can you notify? Often, contracts will include language that will trigger notification when there is a suspected or actual incident. If timing on notification is short, contact information should be clear and quick. While a list of information about the incident looks nice on paper, if notification is going to happen in real time, you might be better served with cooperation language.

International transfers of personal information

Will the parties be sending personal information across country borders? If so, the contract may need to set out which data transfer mechanism will be used to protect the data and comply with any relevant privacy law restrictions.

For instance, if a company will be transferring GDPR-covered data from within the European Union to another country outside the European Union, the contract may need to append the EU-approved “Standard Contractual Clauses.” If the parties instead want to restrict such cross-border transfers to avoid these issues entirely, the contract should specify that restriction.

Liability

Liability and indemnification clauses that apply to data breaches are often contested. Losses can include claims by individuals, regulatory fines or penalties, costs of mitigation, and even contractual obligations of third parties (if you are a subcontractor).

As a buyer, you want broad protection to cover all costs for a breach. You want to be protected for a violation of laws, security breach incidents, and a failure to meet contractual obligations. As a seller, you will want to limit these expenses in some way — not serve as an insurance policy. You will be looking to limit indemnification to gross negligence or willful misconduct, material failure to maintain security protocols, or a cap on damages paid that reflects the risk you want to take on for the business.

This is where your baseline information comes in. What are your insurance limits? Are you willing to cover all expenses for a breach or perhaps cap at insurance levels? Can you even reimburse or does your organization need to be in charge of the mitigation efforts to be covered? Should the parties be responsible for only legally required costs? Further, should you be responsible for a breach because the information was in your custody, or like other indemnities, should there be a negligence or gross negligence standard?

Required security reviews and audits

Audit provisions can be heavily negotiated. Does the third party get access to your system and how fast you have to give them access? While it may seem reasonable to allow a customer to audit your system, be aware of security issues if you have other customer data on the same system.

How can you use this as a business tool?

Contracts can be a way to spot business trends and identify potential data privacy/security issues. If you see provisions over and over, that may be a sign that you need to talk to your business or IT folks about upgrading security, insurance, or recalibrating the organization’s position on how it handles personal data.

Incident response

Why have a plan?

An incident response plan (IRP) aligns the right people in the right place with the right tools to reduce the risk of making harmful and expensive mistakes. IRP is fundamental in defining vocabulary and nonlinear roles and responsibilities to facilitate: (1) compliance with applicable laws, certification audits, insurance obligations, and/or corporate governance obligations; and (2) response and remediation efficiency to save time, money, reputation, and huge headaches such as loss of attorney-client privilege.

Per the 2020 ACC State of Cybersecurity Report, 40 percent of organizations polled had experienced at least one breach over the past year with an average of twenty-four incidents. Of those polled, 75.8 percent had an IRP, 14.2 percent didn’t have one, and 9.9 percent didn’t know.

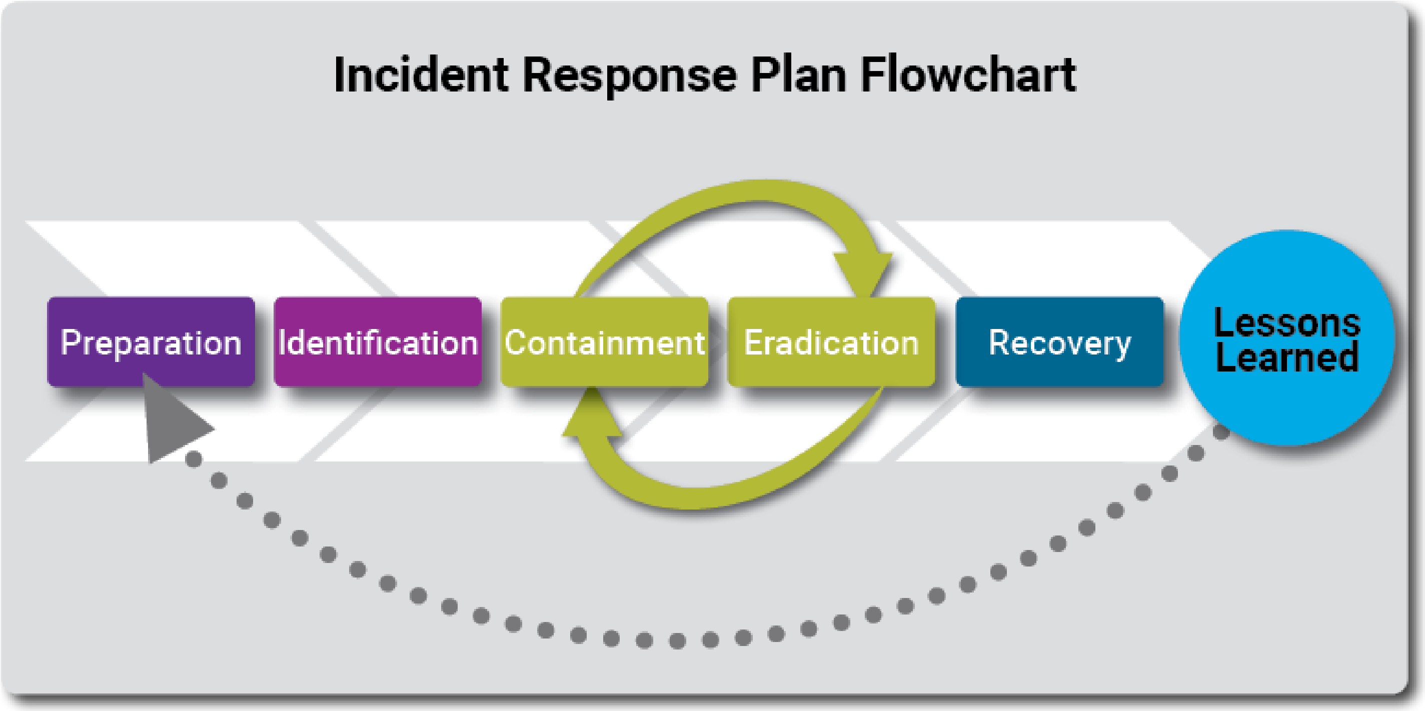
What do I do?

There are numerous sample plans publicly available. Make your plan flexible to manage any type of incident while providing sufficient details for the teams to competently and confidently follow the instructions.

Ownership of the requirements and processes are one way to overcome barriers such as skills shortages that could prevent a high functioning IRP.

If your team would like to institute a tool to facilitate the IRP, some examples may include security incident response platforms (SIRPs), security orchestration and automation (SOAs), threat intelligence platforms (TIPs), security information and event management (SIEMs) and/or security orchestration automation and response (SOAR) tools.

Consistently and regularly pressure test what it feels like during an incident response to reduce chaos and uncertainty. Use all opportunities to practice and refine the experience through lessons learned and stronger preparation.



Conclusion

With new regulatory privacy obligations issued regularly, it is important to take a systematic approach to privacy. Establishing a privacy program will mitigate data breaches, increase operational and organizational efficiency, and result in increased consumer trust. Taking this important step will position your organization for the ever-changing privacy landscape so you can be proactively prepared.

Susan Goebel-Nolan

Senior Staff Counsel

Society for Human Resource Management

Susan Goebel-Nolan is the senior staff counsel for the Society for Human Resource Management, a non-profit HR association headquartered in Alexandria, VA, with over 300,000 members across the globe. In her role as in-house counsel, Goebel-Nolan provides advice on a range of legal issues, with a particular focus on data privacy and corporate compliance. She also serves on both the New to In-house and the IT, Privacy, and eCommerce Networks at ACC.

Alexander "Sandy" R. Bilus

Partner

Saul Ewing Arnstein & Lehr

Alexander "Sandy" R. Bilus is a partner at the law firm of Saul Ewing Arnstein & Lehr. As co-chair of the firm's Cybersecurity and Privacy Practice, Bilus helps clients create and maintain their privacy compliance programs and prepare for and respond to data security incidents. He also represents clients in privacy- and security-related litigation.

Andrea Gehman

Deputy General Counsel

The Johns Hopkins University Applied Physics Laboratory, LLC (APL)

Andrea Gehman is currently the deputy general counsel for The Johns Hopkins University Applied Physics Laboratory, LLC (APL), specializing in privacy, employee benefits, and labor and employment law. Gehman serves as APL's HIPAA privacy officer, responsible for privacy policies and procedures related to APL's dynamic research environment. As part of her practice, she regularly advises on compliance with US and global privacy and data security laws and regulations, with a focus on nonprofit and government contractor privacy requirements.

Jennee DeVore

Senior Director and Counsel, Legal Affairs

Exelixis, Inc.

Jennee DeVore is currently senior director and counsel, legal affairs for Exelixis, Inc. and the Life Sciences Committee chair of the ACC San Francisco Bay Area Chapter. At Exelixis, DeVore supports the general and administrative departments, including corporate information technology and cybersecurity, and is also legal leadership for corporate growth initiatives, including implementing enterprise-wide systems and processes.

Before Exelixis, DeVore served as the data protection officer at a global medical device company. While there, she worked closely with the information security executives to build and run a privacy program and support innovative product development, including a HIPAA compliant medical device.