The Osano Privacy Program Maturity Model

Benchmark and Grow Your Organization's Privacy Program

osano

Table of Contents

The Osano Privacy Program Maturity Model:

Benchmark and Grow Your Organization's Privacy Program

Building a privacy program is hard—but maintaining and maturing one to meet evolving regulations, support operational challenges, and withstand external events can make it feel impossible. To make this task more approachable, it's essential to understand where you stand today and what you need to accomplish tomorrow to take your program to the next level.

We developed the Osano Privacy Program Maturity Model to serve as a framework and guide for privacy professionals seeking to better understand and benchmark their privacy program and its growth trajectory. We consulted with privacy experts, reviewed the current state of privacy program literature, and analyzed the regulatory and operational landscape that privacy programs exist within. As a result, this model formalizes a spectrum of knowledge and insight into what makes a privacy program effective.

In the ensuing sections, you'll learn:

- How to use this model to guide your privacy program's operations
- What the different levels of privacy program maturity are
- Which elements are essential for a holistic privacy program, and
- How you can make the most use of your time and resources as a privacy professional in the endeavor of maturing a privacy program.

osano

How to Use This Maturity Model

You do not have to be mature to be compliant: This maturity model is meant to help you understand how effective your organization is at operationalizing compliance. It does not measure compliance per se; what actually constitutes "compliance" will vary depending on your governing law, industry, unique organizational factors, and jurisdiction. It's possible that you could be perfectly compliant with a given law but score quite low on this model. That would indicate that you're operating inefficiently and are at risk of expending too many resources and potentially falling out of compliance in the future. Scoring high on this model indicates that your privacy program is sustainable, flexible, and using its resources effectively—not that it is compliant with this or that law.

Growing and scaling your privacy program is a journey: While privacy maturity models can be used to help identify potential compliance gaps, they primarily highlight operational challenges that limit efficiency or reduce effectiveness. Quick wins like moving from a spreadsheet maintained by a single person to a centralized tool can help scale, streamline, and automate—and lessen the risk of a single point of failure.

You do not have to obtain the highest level of maturity to be successful: Depending on your risk, you may choose to prioritize specific criteria to make incremental progress as time and resourcing permit. You may choose to accept a lower level of maturity in some areas that generate less risk for your organization and strive for a higher level of maturity in areas that present increased risk or operational challenges. Your privacy program should be tailored to meet your needs.

Structure

By using this maturity model, you can generate an overall privacy score for your privacy program that represents its maturity. This model identifies 16 key elements of a privacy program that represent discrete aspects of a privacy program, such as governance and accountability, privacy incident and breach response, subject rights request management, and more. By scoring these elements on a scale from one (least mature) to five (most mature), you'll attain an overall score that represents your privacy program maturity.

For example, your organization may not have any kind of data inventory in place. In that case, you would evaluate the privacy element, *Data Inventory and/or Record of Processing Activities* as reactive (or Maturity Level One).

With effort, perhaps you establish your first data inventory but have no real plan for when you'll conduct this exercise again or how to improve the process. In that case, you might re-score the privacy element Data Inventory and/or Record of Processing Activities as provisional (or Maturity Level Two).

Scoring Methodology

By working through the 16 privacy program elements listed in this model and considering which of the five levels best represents the given element's maturity level, you can calculate an overall privacy program maturity score. Each maturity level is assigned a corresponding number of points—e.g., Level One, or reactive maturity, is worth one point, while Level Five, or proactive maturity, is worth five.

In the example on the previous page, you may have scored the *Data Inventory and/or Record of Processing Activities* element with either one or two points depending on whether you considered it to be at Maturity Level One or Maturity Level Two, respectively. Then, you would proceed to the next element in this eBook (*Privacy Impact Assessments*), assign it the maturity level that is appropriate to your organization, and score it accordingly. At the end of the exercise, you'll have a score between 16 and 80, which can be used to assess your overall privacy program's maturity.

The score totals correspond to different levels of overall maturity, as follows:

1. 16–31 points: **LEVEL ONE, OR REACTIVE MATURITY**
2. 32–47 points: **LEVEL TWO, OR PROVISIONAL MATURITY**
3. 48–63 points: **LEVEL THREE, OR FORMALIZED MATURITY**
4. 64–79 points: **LEVEL FOUR, OR MONITORED MATURITY**
5. 80 points: **LEVEL FIVE, OR PROACTIVE MATURITY**

You'll notice that the highest level of privacy program maturity is only achievable through a perfect score in this model; this is intentional. Privacy programs, by their very nature, are never "finished"—compliance and privacy protection are ongoing activities, and there is almost always room for improvement. This scoring methodology reflects that reality.

It's important to note that using this scoring system might yield a relatively high maturity level while your privacy program still has significant gaps. For example, if you score highly on most privacy program elements but very low on one or two elements, the scores could balance out to a relatively mature level. This can cause you to mistakenly believe your privacy program is acceptably mature when it, in fact, has some serious gaps that must be addressed.

That's why it's best to think of this scoring methodology as a general framework to guide your privacy program's development. The specific gaps and weaknesses you identify during the evaluation process should be considered weightier than the ultimate score.

Benefits of the Model and Scoring Methodology

With this model and scoring methodology, organizations can:

- Benchmark their existing privacy program.
- Determine priorities when building a new program or developing an existing one.
- Identify high-risk gaps.
- Track privacy maturity over time.
- Identify areas of investment.
- Communicate priorities across teams and stakeholders.
- Assess readiness to respond to evolving compliance needs.
- And more.

One excellent use of this model is as part of departmental or company objectives and key results (OKRs). It could become an objective to improve the privacy program's maturity and a key result to increase the program's overall maturity from one level to the next over the course of a year or quarter, for example.

Finally, while this document was designed with privacy professionals in mind, it can also serve as a guide for non-privacy experts who need to learn what activities they should pursue to develop more mature data privacy practices at their organization. However, it is unlikely that an organization can attain the more mature levels in this model without a privacy professional, dedicated privacy solutions to support compliance needs, and/or trusted external partners.

In the ensuing sections, we'll describe the overall privacy program maturity levels, the 16 key privacy program elements, as well as more targeted guidance on how to use these specific components of the model.

Overall Privacy Program Maturity Level

The following maturity levels can be applied to either the privacy program as a whole or to the individual privacy elements described later on in this document. Review these different levels and consider where your own privacy program and associated elements fall.

1

Level 1: Reactive

At this level, privacy-related activities are conducted in a reactive, one-off manner, perhaps in response to a breach, major headline, notice of noncompliance from authorities, or as a "band-aid" effort to comply with a new regulation.

Consistency and Standardization

There is no consistency or standardization in how privacy issues are addressed at this level; policies and procedures do not exist, so any repeatable processes are merely coincidental.

Resources, Roles, and Responsibilities

There are no dedicated resources or budget for privacy activities. Whenever the organization decides to pursue data privacy compliance, other departments—such as IT, Operations, Legal, and the like—carry out any requisite tasks.

Monitoring and Improvement

Compliance activities are only measured in terms of whether or not they've been completed, if at all. Their actual impact on the organization's compliance posture is not considered; instead, they are treated as boxes to be checked off.

Compliance activities are often underprioritized, and other business initiatives take up the bandwidth needed to manage data privacy concerns. It's difficult to gain the time and focus to attend to compliance; thus, improving compliance processes receives even less time and focus.

Understanding of Data Privacy

Compliance is thought of as something that can be solved, rather than a continuous process. The organization treats data privacy as an obstacle to be overcome or circumvented and then quickly forgotten.

2 Level 2: Provisional

At this level, there still isn't a privacy program or formal privacy element, per se. However, some basic mechanisms for managing data privacy and compliance needs are in place.

Consistency and Standardization

A privacy program or element at the provisional level has some standardization and consistency, though it may not be formalized or defined in a detailed fashion. Procedures for managing data privacy exist but are not fully documented, comprehensive, or integrated into the organization's operations.

Resources, Roles, and Responsibilities

There may not be a dedicated privacy professional at this maturity level. More likely, privacy and compliance are semi-permanent, ancillary responsibilities held by Legal, Operations, or other team members. If there is a privacy professional working on compliance, they do not or are unable to collaborate much with other stakeholders, which limits their efficacy.

Monitoring and Improvement

Program monitoring and measurement only occur in response to an issue or sudden development that brings privacy to the fore. Proactive monitoring does not take place. There may be plans to improve the privacy program or element, but it is unlikely such plans will be put into action. The program or element may be understood to be imperfect, but developing it further is perpetually unprioritized. A major privacy incident or new regulatory requirement may prompt change, however.

Understanding of Data Privacy

The privacy program or element is understood to be an important function in the organization, but it is still perceived as a blocker. Stakeholders accept compliance's importance but do not understand it or why it's important.

3 Level 3: Formalized

At this level, a privacy program and/or the privacy element exists in the organization, and basic practices and procedures are well documented. This level is characterized by a greater degree of standardization than the previous levels.

Consistency and Standardization

The organization has a formal privacy program or element in place with defined policies, procedures, and standards that are integrated into the organization's operations.

Resources, Roles, and Responsibilities

There are clear roles and responsibilities for privacy management. However, this is primarily restricted to privacy-dedicated personnel; other functions' privacy responsibilities are not well understood.

Monitoring and Improvement

The privacy program or element is semi-regularly reviewed to ensure the organization is meeting compliance objectives. However, monitoring is not treated as a priority, the chosen metrics may be somewhat arbitrary, and reviews are not conducted frequently. The findings of reviews are typically not translated into improvement and adaptation. Improvements are typically triggered by new laws and developments in the organization's privacy posture.

Understanding of Data Privacy

Data privacy is considered at the outset of new initiatives but only at the prompting of any data privacy personnel. Outside of the privacy function, privacy concerns are poorly understood. The organization's privacy expert has the authority to request changes to secure the organization's compliance.

4 Level 4: Monitored

An organization with a monitored privacy program or element is actively managing and assessing its privacy program or element. This level of maturity requires a degree of prioritization for privacy that is not present in the earlier levels.

Consistency and Standardization

Program policies and procedures are documented and applied consistently for the most part. When non-privacy personnel carry out compliance-related activities, however, they may do so in an inconsistent fashion. Generally, deviations from the standard procedure are intentional experiments meant to identify and plug gaps.

Resources, Roles, and Responsibilities

The program is adequately resourced, and there is enough privacy personnel to address the bulk of the organization's compliance needs. Privacy management has a dedicated budget within the organization, and this budget is regularly reviewed to ensure the program has the resources it needs to be effective. Non-privacy personnel understands that they may need to consider compliance factors in the course of their work but are not fully consistent in doing so.

Monitoring and Improvement

Processes and procedures are reviewed to assess their efficacy and identify gaps. These reviews occur on a regular cadence, and their results are analyzed to determine how the program can achieve a multitude of outcomes, such as greater efficiency, compliance, speed, cost-effectiveness, and more.

Understanding of Data Privacy

The broader organization is regularly kept informed of and involved in data privacy issues. Senior management is particularly kept abreast of privacy-related activities, and data privacy may be a formal factor that contributes to the organization's objectives and goals.

5 Level 5: Proactive

At the proactive level, the privacy program is a central part of the organization's operations and strategic roadmap. Furthermore, the privacy program itself is highly strategic in how it contends with current and anticipated privacy compliance challenges.

Consistency and Standardization

The privacy program is fully integrated into the organization. Different teams understand compliance procedures and carry them out correspondingly, rarely, if ever, deviating from best practices.

Resources, Roles, and Responsibilities

The privacy program is resourced with adequate budget, staffing, and authority to carry out compliance activities and provide education and training on the broader organization's compliance responsibilities.

Monitoring and Improvement

The program is continuously monitored to anticipate gaps and needs before they arise. The privacy program itself, regulatory landscape, and the organization's operations are all carefully monitored to ensure optimal compliance. The privacy program has a strategic roadmap that predicts future needs and challenges while remaining flexible enough to adapt to unexpected developments.

Understanding of Data Privacy

Privacy may be considered a key differentiator for the organization in the marketplace, and senior leadership is aware of and involved in the organization's compliance posture. Privacy is prioritized in every department involved in the processing of personal data.

Maturity Level of Privacy Program Elements

The following 16 elements constitute the major aspects of a mature data privacy program. In highly regulated or highly unique industries or spaces, there may be additional requirements not covered by this list, but the average business should find most aspects of compliance operations well represented by this list.

The included elements are:

1. Notices
2. Inventories and/or Records of Processing Activities
3. Privacy Impact Assessments
4. Privacy Incident and Breach Response
5. Resourcing
6. Privacy Awareness and Training
7. Privacy Culture
8. Consent Management
9. Subject Rights Request Management
10. Data Minimization and Purpose Limitation
11. Contract Management
12. Vendor Risk Management
13. Security
14. Privacy by Design
15. Governance and Accountability
16. Program Management

This document describes each element using the following format:

MATURITY LEVEL	NOTES
1 Reactive	
2 Provisional	
3 Formalized	
4 Monitored	
5 Proactive	

RECOMMENDED NEXT STEPS

The Maturity Level column provides a space for you to mark down your self-assessed maturity level to calculate your overall privacy program maturity score. Descriptions for each maturity level can be found in the section titled "Overall Privacy Program Maturity Level."

In the Notes section, you'll find brief descriptions of the given privacy element in its more immature or more mature stages as well as any important unique factors to consider.

In the section titled Recommended Next Steps, you'll find specific actions you can take to increase the maturity of the given element.

As you review each element, you can mark down your estimated maturity level for the given element and track the points associated with each maturity level (e.g., Level 1 yields one point, Level 2 yields two points, and so on). You can also follow along using the Osano Privacy Maturity Model Scorecard, which allows you to mark down your score for each element and determine your overall maturity score.

1 Notices

How well does your organization provide notice to data subjects? Your privacy program should provide notice to data subjects regarding a spectrum of information on your data processing activities, including the purpose for collection, data subjects' rights, how the data will be retained and disposed of, to whom the data will be transferred and how, what security measures have been deployed, and more. Moreover, such notice should be disclosed in a clear, conspicuous, consistent, and timely manner.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** An immature notice and disclosure management process may have some or all of the following characteristics: • Incomplete, inconsistent, inadequate, or confusing privacy notices. • Infrequent updates. • Lack of transparency around data processing activities. As a result, individuals won't understand what your organization is doing with their data, what rights they have in regard to that data, and whether or not your organization can be trusted with their personal information. Not only does this damage your relationship with groups like potential stakeholders, but it also puts you at risk of violating data privacy regulations. **More Mature** In contrast, a mature notice and disclosure management process involves: • Clear and concise notices that are easily understandable by data subjects. • Notices that are available in the languages of your data subjects. • Privacy notices that avoid nested, hidden, or externally linked sections where key provisions may be lost. • Clear explanations of data subjects' privacy rights and how to exercise them. • Providing data subjects with disclosures before their data is shared with third parties. • Regularly reviewing and updating notices to assess for ongoing compliance with data processing activities, best practices, and legal requirements.

1. Notices

RECOMMENDED NEXT STEPS

To increase the maturity of your privacy notice and disclosure management process, you can take the following actions:

- Understand who your data subjects are. What kind of voice and tone will make sense to them? What language do your policies need to be in?
- Review and update notices and disclosures to ensure that they are clear, concise, and meet legal and regulatory requirements.
- Conduct regular privacy impact assessments and maintain your data inventory and/or record of processing activity (RoPA) to identify any new data processing activities that require notice and disclosure to individuals. This is especially crucial since, without an understanding of how your organization is processing data, you won't understand what information you need to disclose to data subjects.
- Provide individuals with information on how they can exercise their privacy rights, such as the right to opt in or out of data collection and to access, delete, or modify their personal data.
- Listen to feedback. Are there easy ways for data subjects or stakeholders to connect with your privacy team? Are there common themes that you need to address in your policy for improved awareness?
- Train employees on what data processing activities need to be cataloged and disclosed in privacy notices.
- Develop notices and disclosures that are clear and accessible.

2 Data Inventory and/or Record of Processing Activities

To achieve good data governance and compliance with data protection and privacy regulations, it is essential to understand the following:

- What personal data your organization collects.
- Why it's being collected.
- Where it's stored.
- Where and how it's transferred.
- With whom data is shared.
- And similar information.

Under the GDPR, this practice is a formalized requirement known as a record of processing activity, or RoPA. While many data privacy laws do not require a RoPA or do not refer to this document in the same way, establishing a catalog of data processing activities across your organization is crucial for a well-functioning data privacy program. Data inventories and/or RoPAs document all of the collection, storage, processing, and sharing of personal data that your organization conducts. This document enables organizations to gain visibility and control over their data, thereby ensuring that they can effectively protect personal data and meet their regulatory obligations. It also serves as a tool that can help you identify risks (such as the use of new vendors), plan data strategies, and understand the critical dependencies your data ecosystem relies on.

2. Data Inventory and/or Record of Processing Activities

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** An organization with a data inventory and recordkeeping process at the lower ends of the maturity spectrum will likely: • Have not taken any steps to identify and document the personal data they collect and process or do so irregularly and without rigor. • Lack the ability to say with specificity or certainty what data the organization holds, where it is located, who has access to it, and how it is used. This can result in difficulties complying with regulatory requirements, responding to data subject requests, and protecting personal data from unauthorized access, disclosure, or misuse. **More Mature** A data inventory and recordkeeping process that has a higher maturity will involve the following: • Regular reviews and updates of data inventory records to ensure they remain accurate, comprehensive, and up to date. • The creation and maintenance of a centralized data inventory repository that documents all personal data elements, processing activities, legal basis for processing such data (if applicable), storage locations, data flows, and similar information. • The definition of data retention policies and procedures to ensure personal data is retained only for as long as necessary. Note that a data inventory can appear to be comprehensive when it, in fact, fails to capture the reality of data processing activities at your organization. You may be aware of certain data processing activities that you lack clarity on and can take steps to improve your understanding and records of them. However, there may be data processing activities you lack knowledge of entirely and thus won't know to investigate and record them. For this reason, thorough and proactive investigation is essential for a comprehensive data inventory as well as training your colleagues on the need to self-report new data processing activities.

2. Data Inventory and/or Record of Processing Activities

RECOMMENDED NEXT STEPS

Consider the following activities to increase your data inventory and RoPA maturity:

- Conduct a comprehensive audit to identify all personal data elements, data processing activities, storage locations, and data flows. This could be by way of automated discovery, questionnaires and/or interviews with relevant stakeholders, or a combination of both. The key step is ensuring you get accurate and timely information from those knowledgeable about systems, processes, and business needs.
- Develop a standardized template that can be used to document all personal data elements and their associated processing activities. Ensure there are clear guidelines for documenting and maintaining these records, including the definition of data categories, naming conventions, and metadata standards to ensure that the records are consistent and easily searchable.
- Establish clear guidelines for data retention and disposal, including data retention policies and procedures that are aligned with regulatory requirements.
- Train your colleagues on how to report data processing activities, particularly as you onboard new vendors and suppliers and implement changes in your system, as well as on privacy-by-design and data minimization principles to ensure they don't collect or process more data than is necessary.
- Regularly review and update data inventory records to ensure they remain accurate and comprehensive.
- Determine who is responsible for maintaining these records, define an appropriate cadence for reviews, and find ways of scheduling updates.

3 Privacy Impact Assessments

Data privacy impact assessments (DPIAs) and other privacy risk assessments are essential exercises for identifying sources of privacy risk. With a healthy assessment process, you can identify when these risks can be mitigated, when they are unacceptably high, and when they are tolerable. Regular assessments of this type encourage privacy by design, as they force stakeholders to consider privacy risks before beginning a project or initiative.

Please note that we use the term *privacy impact assessment* to cover any assessment that identifies and quantifies privacy risk, such as GDPR-mandated DPIAs and the privacy impact assessments required under some U.S. laws.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** At the least mature level, your organization may not be conducting privacy impact assessments at all—instead, you might only consider those privacy risks that are immediately apparent and may not take thorough steps to mitigate those risks. Relevant stakeholders may not be alerted to privacy risks, and ultimately, your organization will launch initiatives that introduce unwarranted risks to personal data. This can result in privacy breaches and legal or reputational damage to the organization. **More Mature** In contrast, a mature privacy impact assessment process involves a systematic and comprehensive analysis when there is a high degree of privacy risk associated with all projects or initiatives that involve personal data processing. Your assessments will identify: • What data will be collected. • How it will be used. • Where it will be stored. • Who will have access to it. • How it will be protected.

3. Privacy Impat Assessments

	NOTES (Continued)
	You'll involve stakeholders and subject matter experts in the process and mitigate identified privacy risks through the use of appropriate safeguards. Moreover, you'll have a process in place to ensure the overall assessment workflow functions smoothly. That includes understanding how well your assessment identifies privacy risks and mitigation techniques, that it's conducted at the right time and without unnecessary delays, and that stakeholders are consulted throughout the project lifecycle.

RECOMMENDED NEXT STEPS

To further mature the privacy assessment process, consider whether you've taken the following actions:

- Develop or identify a standardized privacy impact assessment template that includes all relevant privacy risk assessment questions.
- Provide training to employees on the importance of privacy impact assessments and how to conduct them effectively.
- Implement pathways to embed templates in processes such as product reviews, legal sign-off, financial approvals, or pre-release QAs.
- Ensure you and/or relevant stakeholders have insight into all projects that involve the collection or processing of personal data to allow for triage and determination of whether a privacy impact assessment is applicable.
- Review and update assessments on a regular basis, particularly in response to changes in technology or the regulatory environment.
- Understand the legal requirements for conducting assessments, as they can vary by jurisdiction.
- Ensure assessments are conducted early in the development process and that they are reviewed and updated as necessary throughout the project lifecycle.
- Involve stakeholders from across the organization, including legal, security, engineering/product, IT, operations, finance, procurement, marketing, and HR, to ensure you can identify and address all privacy risks.
- Document the assessment process and the results, including any mitigating measures that were implemented.
- Log any risks and appropriate risk treatments as part of your risk management program.

4 Privacy Incident and Breach Response

Data breaches are growing more common and more expensive, and they aren't limited to just the big players. Consider the fact that:

- The average data breach costs businesses **$4.35 million**.
- Annual cybercrime in the U.S. alone costs businesses over **$10 billion**.

Mitigating risk and designing controls with robust security measures has never been more important. However, security and privacy teams have accepted that even the most robust controls and precautionary measures are not foolproof.

Because of this, privacy professionals must develop a plan to prepare for, respond to, and mitigate the impact of privacy incidents and breaches. Doing so effectively requires a clear understanding of whose data you have, where that data lives in your organization, where it is processed, who it has been shared with, and the controls behind which that data is protected.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** With immature privacy incident practices, your organization may lack formal response plans, incident reporting practices, and employee training processes on how to recognize and respond to potential incidents. **More Mature** On the other hand, a mature breach response process will involve a clear and detailed plan for identifying, reporting, investigating, and mitigating incidents and breaches. Such plans should also include a communication strategy for notifying affected individuals and relevant authorities as well as guidelines for post-incident review and improvement. This includes regular testing and improvement of response procedures as well as ongoing monitoring and risk assessments to identify potential weaknesses. These plans will be coordinated across many departments, specifically cybersecurity and legal teams, to ensure breach response plans support forensic investigation and legal privilege.

4. Privacy Incident and Breach Response

	NOTES (Continued)
	Privacy professionals should keep in mind that incidents and breaches can have a significant impact on an organization's reputation and financial stability. It is therefore critical to establish strong practices that ensure timely detection, swift response, and effective remediation of incidents and breaches.

RECOMMENDED NEXT STEPS

To improve your privacy incident and breach response practices, consider taking the following actions:

- Develop and maintain clear incident response plans that are regularly reviewed and updated.
- Establish a reporting mechanism that enables employees to easily report incidents and breaches.
- Provide regular training and awareness programs for employees to help them identify and respond to potential incidents.
- Conduct regular incident readiness assessments to identify potential gaps and areas for improvement.
- Create a post-incident review process to identify lessons learned and improve incident response plans.
- Ensure the organization has appropriate processes and tools to support the incident response process, including being able to provide relevant information and deliverables to support any incident management software and forensic analysis investigation.
- Establish clear communication channels for internal and external stakeholders, including employees, customers, regulatory bodies, and law enforcement agencies.
- Continuously monitor and stay up to date with changes to relevant laws and regulations regarding incident reporting and notification requirements.

5 Resourcing

Without adequate resources, there is little a privacy program or privacy professional can accomplish. It can be challenging to advocate for adequate budget, tooling, and staffing; privacy is so often seen as a cost center, and stakeholders who are unfamiliar with the demands of privacy may be inclined to reduce cost as much as possible. In a mature privacy program, privacy resources are distributed based on actual need and resourcing changes as those needs change.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** When your privacy program has immature resourcing practices, there may not be a single individual whose primary role is privacy management. Instead, privacy may fall under the purview of individuals in other departments like operations, IT, or security. These individuals may address privacy concerns based on their capacity and do so in a highly reactive manner. When there is a privacy professional, they may lack the resources required to procure the technology and tooling that they need to be effective. Not only will they have an excessive workload, but the extra work will also spill over to IT and development teams who may suffer an increased workload spent developing and maintaining in-house solutions to privacy challenges—or who may de-prioritize such solutions in favor of completing their primary responsibilities. Due to the lack of adequate staffing and tooling, there may be significant errors in executing a given privacy task, such as subject rights responses, or there may simply be no solution in place for regulatory requirements, such as for website cookie consent.

5. Resourcing

	NOTES (Continued)
	More Mature In an organization with mature resourcing practices, there will be adequate staffing to address the organization's entire privacy needs. Those personnel will have access to compliance solutions that streamline the transactional, tedious, and time-consuming aspects of privacy management, such as consent management, subject rights requests, vendor onboarding and review, privacy assessments, legal documentation, and more. Moreover, the program will have cross-functional support from other stakeholders, who will themselves have adequate capacity to handle privacy responsibilities. When fully optimized, resourcing is periodically adapted and updated such that the privacy program always has access to what it needs to be effective, but it doesn't create an undue burden on the organization's overall budget.

RECOMMENDED NEXT STEPS

The following key steps can help you mature your organization's privacy program resourcing:

- Formally define your organization's specific privacy needs and identify which are suitable for or require technological solutions, which are better suited by in-house efforts, and which should be done manually. This includes developing an understanding of the specific needs of the organization, including the size of the organization, the types of data collected and processed, and the level of data risk.
- Regularly review and update tooling as needed to ensure their continued effectiveness and alignment with the organization's needs.
- Use this model to assess the current state of your privacy program and identify gaps. With this information, develop the business case to acquire the resources needed to close the gaps.
- Align the privacy program's goals and objectives with the organization's strategic vision and mission and communicate them clearly to the senior management and stakeholders.
- Establish a cross-functional privacy governance structure that involves representatives from different departments and functions, such as legal, IT, marketing, HR, and security. As more stakeholders across the organization become involved with data privacy and understand its needs, securing necessary resources will become easier.

6 Privacy Awareness and Training

As a privacy professional, there's only so much you can do to ensure personal information is protected on your own. Because personal data is processed across an organization, an effective privacy program encourages collaboration with various other departments. This ensures that data custodians with more knowledge of intricate processes or systems than you do can be privacy champions. To accomplish this, privacy professionals need to spread awareness and conduct training to educate employees and stakeholders about the importance of privacy, how to handle personal data in accordance with legal and regulatory requirements, and what specific actions to take to streamline privacy risk management.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** At its most immature level, there is no privacy awareness or training taking place at your organization, or it may only be offered retroactively after privacy breaches or incidents. In contrast, mature privacy awareness and training practices are conducted regularly and are measured and improved over time. You'll test colleagues to evaluate the efficacy of the training, report on results, and identify gaps in both the organization's knowledge of privacy-related topics as well as the training materials. **More Mature** Privacy professionals should keep in mind the importance of tailoring training and education for different roles and levels of the organization as well as the need to address emerging privacy issues and technologies. Because privacy is an evolving space, you'll want to update your training over time.

6. Privacy Awareness and Training

RECOMMENDED NEXT STEPS

To mature your privacy awareness and training practices, take the following steps:

1. Develop a comprehensive privacy training program. This should be customized for your organization. Some starting points will be to:
   - Understand your organization's geographical footprint so you can determine what laws, regulations, customs, and cultural norms may be applicable.
   - Establish a privacy committee or governance council so you can embed champions to act on your privacy program's initiatives and gather feedback on how to successfully operationalize your program.
   - Determine what compliance requirements need to be operationalized and aligned with processes such as performing privacy impact assessments and fulfilling subject rights requests.
   - Create a training program so that your colleagues and co-workers understand their obligations and try to create a privacy-first culture. This should also be rolled out to new hires as they join your organization.
   - Share and present your organization's privacy policies, and try to relate policy elements to different stakeholders' roles and responsibilities.
   - Report on KPIs, metrics, training outcomes, and risks to senior leaders so that they have oversight of the program and insight into training needs.
2. Design a process to ensure consistent rollout to all employees (including new hires) and contractors, consultants, or other workers with access to data and/or company systems.
3. Tailor training to specific job roles.
4. Explore different training methods to address your organization's unique education needs.
5. Identify the best means of delivering training within your budget, such as e-learning modules or recorded trainings, in-person training sessions, and simulations.
6. Find ways to make privacy training fun and engaging. You could develop interactive quizzes, host games with prizes, create a shared playlist, send out a newsletter, or anything else that educates your colleagues on the importance of privacy while keeping them engaged.

7 Privacy Culture

While there is an overlap between privacy awareness and training and a culture of privacy, they are not exactly identical concepts. For one, a robust training and education process contributes to a culture of privacy but does not guarantee it. The degree to which your organization adopts a culture of privacy will depend in part on the personalities of your colleagues, the industry you operate within, and the products and services your organization provides.

The culture surrounding privacy issues at your organization can be the "X factor" that elevates your privacy program to new heights. Because data privacy activities are often interdisciplinary and interdepartmental in nature, other stakeholders' understanding of and attitudes toward privacy will have a major impact on privacy professionals' ability to do their jobs. In an organization with a mature privacy culture, the work becomes much easier; in an organization with an immature or absent privacy culture, executing basic tasks can feel like herding cats.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** In an immature culture of privacy, privacy is not a priority and may be seen as a hindrance to business operations. Your colleagues may not be aware of privacy policies or may not understand their role in protecting personal information. Privacy risks may be discounted as a "one-off" exception every time. **More Mature** A mature culture of privacy, in contrast, integrates privacy into the organization's values, policies, and operations. Employees are trained and aware of privacy policies and their role in protecting personal information. Privacy leaders have a seat at the decision-making table and advise on privacy risks arising from proposed strategies. Different team members consider privacy early in the respective processes they own, such as the software development lifecycle, marketing initiatives, website analytics, and more. Privacy professionals should keep in mind that creating a culture of privacy requires ongoing effort and communication by all, including senior leadership and junior employees. It is important to engage with employees at all levels of the organization to build awareness and ensure that privacy is viewed as a core value.

7. Privacy Culture

RECOMMENDED NEXT STEPS

To improve the maturity of your organization's privacy culture:

- Implement privacy-focused initiatives, such as privacy impact assessments and privacy by design, to embed privacy into your organization's operations.
- Ensure privacy leaders have visibility into business strategy.
- Secure top-level buy-in to data protection by senior leaders.
- Develop and communicate clear privacy policies and procedures that align with the organization's values and goals.
- Provide regular privacy training to all employees to ensure they understand their role in protecting personal information.
- Encourage employee feedback and engagement to continuously improve privacy practices and culture.

8 Consent Management

Consent is a key component of both privacy ethics and regulatory compliance, and consent management is equally crucial—that is, obtaining, managing, and documenting the consent of individuals for the collection, use, and sharing of their personal information. When your organization collects data from data subjects, does it ask for consent to do so in a clear, unambiguous, and nonforceful manner? Organizations need to consider the nature of consent management requirements as per their governing law, such as whether consent must be opt-in, opt-out, include specific language or consent controls, and so on. You'll also need to consider how to operationalize data subject consent preferences, how to prove and record consent preferences without violating privacy, and additional factors.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	Effective consent management must have policies and procedures in place for obtaining consent, operationalizing that consent (i.e., turning data trackers on or off, blocking or permitting data sharing, etc.), documenting consent, and reversing consent preferences when it is revoked. **Less Mature** With an immature consent management process, an organization may only meet some or none of these requirements. For example, visitors may indicate they don't consent to data collection on your website, only for some data trackers—but not all—to be blocked. Or consent may be asked for in a misleading manner, such as by requiring additional clicks to opt out of data collection rather than opt-in.

8. Consent Management

	NOTES (Continued)
	More Mature A mature consent management process involves clear, transparent, and user-friendly procedures for obtaining, documenting, and managing consent. This includes providing visitors with clear and understandable information about the purposes and scope of data collection, using plain language, and providing accessible options for opting in or out. Privacy professionals should regularly review and update their consent management process to ensure it functions correctly, remains compliant with governing laws, and reflects the data processing activities at their organization. Important factors to consider in consent management include the scope and sensitivity of personal information collected, the jurisdictional requirements for consent, and the potential risks to individuals if their consent is not properly managed.

RECOMMENDED NEXT STEPS

Effective consent management requires a degree of technical operationalization that privacy professionals may find difficult to accomplish on their own. To make this task easier, privacy professionals should:

- Implement a consent management platform (CMP) to secure, record, and act on visitor consent preferences.
- Regularly assess consent procedures.
- Educate website or application stakeholders such that they highlight new data collection mechanisms to ensure they can be blocked pending visitor consent preferences.
- Schedule regular reviews to check whether consent management mechanisms operate in line with changing privacy regulations and best practices.

9 Subject Rights Request Management

Subject rights request management refers to receiving, processing, and responding to requests from data subjects to exercise their data privacy rights, such as the right to access, rectify, delete, or restrict the processing of their personal data. Data subject rights requests can be one of the most visible aspects of your organization's data privacy operations. Consumers (and, depending on the governing law, employees or other commercial partners) won't always be aware of what work you do on a day-to-day basis, but they will notice if your privacy program is unable to meet their request within required timeframes or if your response contains errors. A streamlined subject rights request management process is critical to both complying with the law and preserving your organization's reputation for trustworthiness.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** With immature subject rights request management, your organization may not fully understand the relevant details associated with data subject rights under governing law, such as response deadlines, the requirements for fulfilling subject rights requests, individual rights held by data subjects, and more. Data subject requests may be received through general-purpose email inboxes, and information about rights may not be provided to data subjects. There may be no established process or system for tracking and fulfilling requests, leading to inconsistent handling and potential noncompliance. **More Mature** In a monitored or proactive process, you'll have established procedures for receiving and processing requests and regularly measure those procedures and the subject rights management workflow for efficacy. This includes everything from disclosing data subject rights to accepting requests via a dedicated channel, verifying identities, tracking and prioritizing requests, automating requests, discovering data, transmitting data, and communicating with the requestor in a clear and timely fashion. Keep in mind the importance of timely and accurate responses to subject rights requests—delayed responses serve as a signal to data subjects and authorities that your organization is noncompliant and can't be trusted with personal information.

9. Subject Rights Request Management

RECOMMENDED NEXT STEPS

To mature your subject rights request workflow, consider taking the following actions:

- Transition from manual processes relying on email and spreadsheets to more automated workflow management solutions. Manually tracking and managing data subject rights requests contributes to missing deadlines, delivering erroneous or incomplete information to the data subject, and generating yet more data to manage.
- Implement a system for tracking and prioritizing requests.
- Train your colleagues who interact with stores of personal data on how they can help fulfill data subject rights requests.
- Establish a dedicated channel for accepting requests and communicating with requesters.
- Conduct a thorough data inventory to ensure you're aware of where personal data is stored in your organization.
- Automate common request types, like data summaries, but retain an expert in the loop to verify and review.
- Provide appropriate information about data subjects' rights in your privacy policy.
- Track metrics related to subject rights requests. Analyze and present trends to management for improving the subject rights request process on an ongoing basis.

10 Data Minimization and Purpose Limitation

Many data subjects are comfortable with businesses that want to use their personal data for one specific, disclosed, and limited purpose. The trouble comes when organizations hold onto their data indefinitely and use it for a multitude of purposes that aren't disclosed. At the same time, premature deletion of data can hinder operations. A mature privacy program supports the management of personal information (PI) collection, use, and retention in such a way that data is used according to the purpose declared upon its collection. Consent must be secured before PI can be used for any secondary purpose, and PI must be deleted or anonymized when its purpose has been fulfilled.

And of course, prevention is better than cure. Taking steps to minimize data collection can help you in the long term if there is a data breach.

MATURITY LEVEL	NOTES
1 Reactive	**Less Mature** Immature data minimization and purpose limitation practices may involve collecting more data than necessary or using data for purposes outside the original intent. It may be the case that you and other stakeholders lose track of personal data as it moves through and outside of the organization. PI may be transferred to third parties without proper consent or disclosure, even without internal stakeholders' knowledge.
2 Provisional	
3 Formalized	**More Mature** Mature data minimization and purpose limitation practices involve identifying the minimum amount of personal data required to achieve the intended purpose and ensuring the data is only used for that purpose. This includes regularly reviewing and updating data retention policies, limiting access to personal data, and implementing technical controls such as pseudonymization to protect personal data. Furthermore, any data that is transferred to third parties must be carefully tracked and monitored, and agreements must be in place that limit how third parties can use PI. Your organization will inform data subjects about any transfers, their purpose, and what rights they hold in regard to data transfers.
4 Monitored	
5 Proactive	

10. Data Minimization and Purpose Limitation

RECOMMENDED NEXT STEPS

Before you can optimize your PI collection, use, and retention practices, you'll need to understand where and how your organization collects and processes personal data. For this reason, a data inventory and/or RoPA should be your first step.

Ask yourself why:

- Why am I collecting this?
- Why am I sharing this?
- Why am I storing this here?
- Why am I keeping this for so long?

Your privacy policy should also be clear about why you collect PI, and your colleagues who work with personal information should understand that they may only use PI for those specific purposes. Work with your IT and operations team members to ensure that only individuals who need to access personal data can access it, and regularly review and update policies and procedures to ensure data is only used for stated purposes unless permitted by the data subject.

11 Contract Management

Certain jurisdictions require that any processor or service provider handling data have specific contractual provisions in place with the organization they receive data from. These are typically handled by way of data processing addendums that specify the obligations of each party and the security measures that protect the data.

Since modern businesses rely on a small galaxy of vendors, partners, outsourcers, and others to operate, being able to manage the contracts associated with those third parties effectively is essential to protecting the PI they manage. In the context of a data privacy program, contract management refers to the process of ensuring that privacy obligations are incorporated into contracts with third-party service providers and vendors. Privacy professionals need to work closely with legal and procurement teams to identify when contracts need language addressing data privacy, which existing contracts must be updated, and how to negotiate new contracts with privacy-related language.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** An immature contract management process may involve ad hoc contract reviews without standardized privacy language or regular monitoring of vendor compliance with privacy obligations. Personal data may be transferred to counterparties without contractual protections in place, and privacy professionals may lack insight into which contracts lack appropriate language, which incorporate the right language, which need to be updated, and so on. Contract managers are likely siloed from any privacy function at the organization. **More Mature** In contrast, a mature contract management process involves close collaboration with legal and procurement teams on a standardized set of language that protects PI when transferred to a third party or when received from a third party. It takes into consideration the different privacy laws governing the different counterparties and establishes appropriate contract reviews, third-party compliance, and the contract management process as a whole.

11. Contract Management

RECOMMENDED NEXT STEPS

To improve the contract management process:

- Establish regular meetings with your colleagues in the legal and procurement departments and whichever other stakeholders may regularly handle contracts.
- Create an accurate and regularly updated data inventory and/or RoPA to understand when and where data flows to third parties.
- Develop standardized contractual language to implement within as many contracts as necessary. When counterparties object to specific language, have a plan in place for which clauses and terms are essential, which alternatives are acceptable, and so on.
- Review relevant laws, regulations, and rules to see if any specific language should be added to your standard privacy language.
- Conduct regular audits of your third parties to assess compliance with agreed-upon obligations.
- Tie these processes to ongoing reviews such as those performed by security teams or compliance teams.

12 Vendor Risk Management

Related to contract management, vendor risk management provides a method for managing privacy risks that would otherwise be outside of your control. Once your customers' data passes to a third party, there's little you can do to continue to protect it unless you engage in robust vendor risk management processes. There is a significant overlap between vendor risk management and contract management. However, aspects of vendor risk management are not related to contracts; similarly, not all contract-related privacy issues involve vendors. Hence, the two are represented by separate elements in this model.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** The concept of vendor risk may not be present in an organization with immature vendor risk management practices. Not only will the regulatory requirements around mitigating vendor risk be poorly understood, but there may be no actual activities taking place to mitigate vendor risk. If regulatory requirements *are* understood, they may be met according to the letter of the law but not its spirit. Contractual language may be put into place, but there will be little or inconsistent auditing for compliance. Likewise, there will be inconsistent or absent reviews of privacy risk in vendors prior to onboarding. When a privacy breach or privacy incident occurs relating to vendors, there may be little to no remediation. **More Mature** Mature vendor risk management involves an established and continuously improved process for assessing vendors for privacy risk. That starts before vendor selection occurs by using candidate vendors' privacy practices to establish a short list of acceptable candidates and continues on through onboarding, ongoing review, the establishment of risk mitigation strategies, implementation of risk mitigation plans should vendor practices change, and regular communication with vendors to ensure compliance with privacy and security requirements.

12. Vendor Risk Management

RECOMMENDED NEXT STEPS

Privacy professionals interested in improving their vendor risk management process should:

- Identify a means of evaluating vendors' privacy practices prior to onboarding, including vendor assessments. Ideally, these assessments should be tailored based on the likely risk that the vendor poses to individuals' data privacy, the vendor's criticality to the organization's operations, the sensitivity of the data that will be shared with the vendor, and the level of oversight needed to manage the risks introduced by the vendor.
- Take these factors into account during post-onboarding vendor risk management activities as well.
- Implement a vendor privacy risk management solution to provide capacity to adequately assess vendor risk.

13 Security

Considering all the trouble privacy professionals go through to ensure individuals' personal data is treated respectfully, it should come as no surprise that taking adequate and reasonable security measures is an essential element of a privacy program. Most privacy regulations do not specify what exactly constitutes "reasonable security," so it is important that organizations take steps to review their technical, administrative, and organizational security controls and their effectiveness in protecting the confidentiality, integrity, availability, and resilience of data. While privacy and security have significant overlap, each discipline benefits from specialist expertise; therefore, a best practice is to have distinct personnel focused on privacy and security, respectively, but for both team members to work closely with one another.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** In an organization with immature security as it pertains to data privacy, there will be little coordination between privacy professionals and security and/or IT professionals. Stores of personal data will not be identified as being high risk, and personal data may be stored without encryption or access controls. Even if there is a secure location where personal data is stored, it may be copied or stored in other locations without security. **More Mature** For an organization with mature security standards, privacy factors will be taken into consideration in the overall security framework from the very beginning. There will be regular risk assessments, documented policies and procedures, continuous monitoring and improvement, and employee training. Privacy and security professionals will work closely with one another to ensure high-risk data is kept secure, and they'll collaborate to train their colleagues on best practices. There will also be robust access controls and identity management processes in place to prevent undue access to personal data. Furthermore, the security framework will be regularly reviewed and updated to adapt to the evolving threat landscape.

13. Security

RECOMMENDED NEXT STEPS

To improve the maturity of security practices as they pertain to privacy, privacy professionals should:

- Establish ongoing collaboration with their colleagues in security.
- Consider security factors in privacy awareness and training.
- Determine baseline controls with security teams that correspond to data classifications. For example, is encryption, multifactor authentication, and/or the use of virtual private networks required for all company confidential information and personal data
- Develop robust identity management, authentication, and access controls.
- Create written policies that specify security procedures.
- Establish a remediation plan for security incidents as part of their privacy breach response protocols.
- Regularly test and review the efficacy of security measures, including the resiliency of data from backup and disaster recovery.

14 Privacy by Design

When developing new products, services, or anything that may process data subjects' PI, it is tempting to consider factors like privacy at the very end of the process. While this impulse is understandable, it guarantees that PI is receiving less protection than it would otherwise receive at best; at worst, privacy factors are never considered during the design process due to lack of attention or time, and PI is left unprotected.

Privacy by design ensures privacy factors are considered early in the development process. While the onus of implementing privacy-by-design principles lies with the developers, strategists, and project managers who work on the various initiatives that may involve PI, privacy professionals can take certain steps to encourage privacy by design.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** An immature privacy-by-design process might involve privacy considerations being an afterthought or only considered in the later stages of product development. When project timelines are short, privacy may not be considered at all. There will likely be no standardized steps for project leads to consider when implementing privacy by design, and project leads may not realize their initiative poses privacy risks at all. **More Mature** A mature privacy-by-design process would involve privacy considerations being integrated into every stage of product development, from ideation to retirement. Project leads are educated on what constitutes privacy risk and how minimizing those risks can inform the design of their system, tool, or process. Privacy professionals are consulted early and often throughout the process, and each project serves as a learning experience to improve privacy-by-design practices for the next project.

14. Privacy by Design

RECOMMENDED NEXT STEPS

To encourage the adoption of privacy-by-design principles, privacy professionals should:

- Advocate for privacy to be included in product development from the outset.
- Create and implement privacy-by-design frameworks.
- Provide training and resources to staff on privacy-by-design principles and best practices.
- Collaborate with product development teams to ensure that privacy is considered throughout the product development process.
- Conduct privacy impact assessments at the outset of new projects and initiatives.
- Foster a culture of privacy and data protection to encourage project leads to consider privacy and/or consult with the privacy professionals in their organization.

15 Governance and Accountability

Governance and accountability refers to the policies, procedures, and processes that an organization puts in place to ensure that its data privacy program is effective and compliant with relevant laws and regulations. It also includes the mechanisms for ensuring that individuals and teams within the organization are held accountable for meeting the organization's privacy obligations. Without such a system in place, proving compliance, ensuring follow-through, and identifying compliance gaps are significantly more challenging.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** A privacy program with immature governance and accountability practices has little or no formal structure for overseeing data privacy at the organization, and the individuals who are accountable for data privacy at the organization and team level is unclear or undefined. There Is likely no internal auditing of privacy policy adherence, or if there is, it is done in a retroactive manner. When internal noncompliance is identified, there may be no follow-up or remediation efforts. It may be the case that individuals who ought to be accountable for privacy in their domain are unaware of privacy policies and procedures at all. **More Mature** In contrast, mature governance and accountability practices include clear policies and procedures for handling personal data, oversight mechanisms to ensure compliance with those policies, and accountability structures to ensure that individuals and teams within the organization are held accountable for meeting their privacy obligations. The organization regularly assesses its privacy program to identify and address any gaps, and it has mechanisms in place to monitor and report on privacy risks and incidents.

15. Governance and Accountability

RECOMMENDED NEXT STEPS

Establishing strong governance and accountability practices can seem abstract at first, but privacy professionals can mature these practices through the following actions:

- Secure the support of senior management for the privacy program and ensure that privacy is treated as a strategic priority within the organization.
- Establish clear policies and procedures for handling personal data, along with clearly identifying responsible individuals and their responsibilities in the context of data privacy.
- Create a charter for the hierarchy, roles, responsibilities, communication strategies, and overall privacy governance structure.
- Implementing an oversight mechanism to ensure compliance with those policies and procedures, such as regular reviews and/or audits.
- Provide regular training and awareness programs to ensure that all employees are aware of their privacy obligations.
- Regularly assess and test the organization's privacy program to identify and address any gaps.
- Monitor and report on privacy risks and incidents and share the results of that reporting with the broader organization.

16 Program Management

Data privacy program management involves the overall strategy, planning, implementation, and continuous improvement of an organization's data privacy program. Taken together, the individual elements described in this model serve as a good approximation of a data privacy program, but the whole of a privacy program is more than just the sum of its parts. This element represents the holistic, end-to-end management of a data privacy program, inclusive of the elements described in this model and of any other elements unique to your organization. This includes the coordination of the different components and activities that make up the program, as well as the allocation of resources and the management of stakeholders.

MATURITY LEVEL	NOTES
1 Reactive 2 Provisional 3 Formalized 4 Monitored 5 Proactive	**Less Mature** An immature data privacy program management process is characterized by ad hoc, reactive, and disjointed efforts to address privacy risks and compliance requirements. The organization may lack clear ownership and accountability for the program, as well as a comprehensive and cohesive privacy strategy. The program may also be under-resourced, poorly documented, and not regularly evaluated or updated. You may pursue individual activities (such as those described in this model) but struggle to prioritize one over the other or find that as you progress in one area of data privacy, another area suffers. **More Mature** In contrast, a mature data privacy program management process is characterized by a proactive and strategic approach to privacy risk management and compliance. The program is well-defined, well-documented, and regularly evaluated and updated. There is clear ownership and accountability for the program, with dedicated privacy professionals or teams leading the effort. The program is supported by sufficient resources, including personnel, technology, and funding, and has the buy-in and participation of all relevant stakeholders. You'll have identified priorities and established a systematic approach to growing and maturing your privacy program, and you will track its growth over time.

16. Program Management

RECOMMENDED NEXT STEPS

To improve your overall privacy program management, privacy professionals can take several actions, including:

- Develop and implement a comprehensive and cohesive privacy strategy aligned with the organization's overall business strategy and risk appetite.
- Establish clear ownership and accountability for the privacy program, including dedicated privacy professionals or teams, and a governance structure that includes regular reporting to executive management and the board.
- Allocate sufficient resources, including personnel, technology, and funding, to support the privacy program.
- Conduct thorough research and evaluation of potential tools and vendors, including the potential privacy risks they will introduce.
- Provide ongoing training and support for the effective use of selected tools for any stakeholders who may interact with your privacy tech stack.
- Ensure the selected tools integrate with existing systems and processes and can be scaled as needed.
- Develop and maintain comprehensive policies, procedures, and guidelines that are regularly reviewed and updated.
- Conduct regular privacy risk assessments and develop risk management plans to address identified risks.
- Implement appropriate privacy controls and measures, including data protection measures and incident response plans.
- Provide regular privacy training and awareness to all relevant employees, vendors, and contractors.
- Regularly monitor and measure the effectiveness of the privacy program, including the identification and tracking of privacy metrics and key performance indicators.
- Foster a culture of privacy throughout the organization, including the active participation of all relevant stakeholders, such as business units, IT, legal, and compliance.
- Stay up to date on emerging privacy risks, legal and regulatory developments, and industry best practices, and incorporate these into the privacy program as appropriate.
- Regularly assess your privacy program using this model and other frameworks and systems as appropriate.

Score Totals

MATURITY LEVEL	NOTES
	1 16–31 points: **LEVEL ONE, OR REACTIVE MATURITY**
	2 32–47 points: **LEVEL TWO, OR PROVISIONAL MATURITY**
	3 48–63 points: **LEVEL THREE, OR FORMALIZED MATURITY**
	4 64–79 points: **LEVEL FOUR, OR MONITORED MATURITY**
	5 80 points: **LEVEL FIVE, OR PROACTIVE MATURITY**

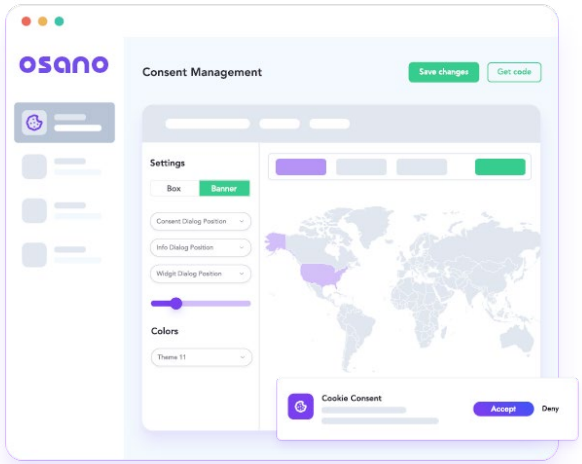
How Osano Can Help You Mature Your Privacy Program

Building, running, and managing an efficient data privacy program can feel overwhelming. If you prioritize maturing one element of your program, other elements may suffer; if you strive to meet a basic standard with all elements of a data privacy program, you may never have the time or resources to increase your program's maturity level as a whole.

The trick lies in automating and streamlining the right tasks.

Broadly, the elements of a data privacy program can be divided into two groups. The first group requires human expertise—yours. Many of the elements of a mature, well-rounded privacy program can only be nurtured by a privacy professional. The second group may require less expertise to mature, less of a human touch, or more expertise that doesn't relate to a privacy professional's core skillset. To gain the time and resources to focus your attention on the first group, you need to automate and streamline the elements contained within the second.

With a data privacy platform like Osano, you can automate and streamline the activities associated with a number of elements in a mature data privacy program, including:



Consent Management

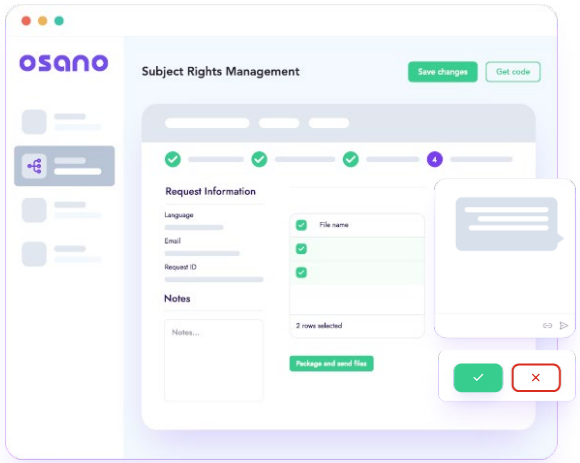
Taking a fully homegrown approach to consent management is asking for trouble. Consider the workload involved:

- Reviewing the tens of thousands of words of legalese in the text of every data privacy regulation covering the various jurisdictions where your customers and website visitors live.
- Translating those into various compliant banners that fire whenever a visitor from a certain jurisdiction accesses your website.
- Configuring the various data trackers on your website to fire or not fire depending on the individual's consent preferences.
- Maintaining this system every time the law or your website changes.

This approach, however, is a clearly inefficient use of your time as a privacy professional and the time of your colleagues in development, IT, legal, and operations.

Osano Cookie Consent manages this process for you. Unlike other consent management platforms (CMPs), Osano is fast and simple to implement—you can get started by just adding one line to your website and start managing consent within hours or days, not weeks or months. Then, Osano automatically scans your website or websites and auto-discovers your tags like cookies, scripts, and iframes that collect visitor data. Osano automatically categorizes these tags based on best practices, ensuring they fire or are blocked based on consent preferences.

Osano provides out-of-the-box banner templates that comply with the regulations of over 50 countries and disclose legally required information in your visitors' preferred language. And if you use Osano Cookie Consent but still receive a fine from an authority related to the use of Osano, we pay the first $250,000 with our "No Fines. No Penalties." pledge.

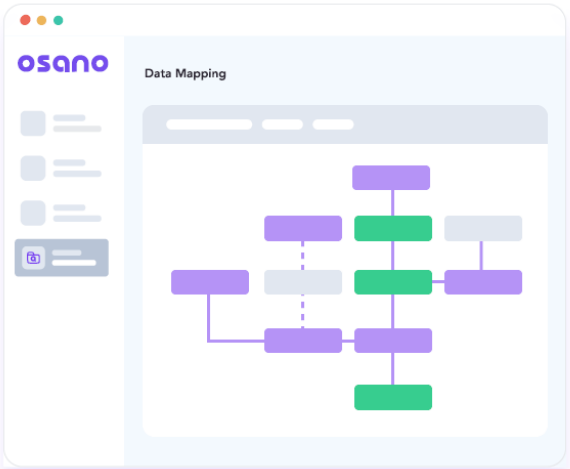


Subject Rights Request Management

Osano provides a comprehensive solution for capturing and processing subject rights requests, including:

- Auto-generated request forms and/or email addresses for accepting subject rights requests. You can then communicate with data subjects via a secure messaging portal in the Osano platform.
- Automated request task assignment so that different stakeholders who own the various stores of personal information across your organization have a clear understanding of the tasks they must complete. You'll be able to review which tasks have been completed, which are ongoing, and which are at risk right within the app.
- Automated third-party vendor notification, which ensures that data subjects can make requests in regard to their personal information that has been transferred outside of your organization to your vendors.
- Automated data summary and deletion, which saves you from having to track down each and every item of data associated with a data subject across the various data stores in your organization. Osano identifies a data subject's personal information and, pending your verification, deletes or summarizes the data depending on the request type.
- Automated data packaging, which provides data subjects their personal information in a portable format as required by law.

Using Osano to manage subject rights requests centralizes the DSAR workflow, reducing your reliance on multiple tools and data stores to fulfill requests. Moreover, Osano provides a transparent experience for your data subjects; you can communicate with requesters in a secure messaging portal in real time and automatically send emails (from templates that come pre-built within the platform) to keep requesters informed at each step of the process.



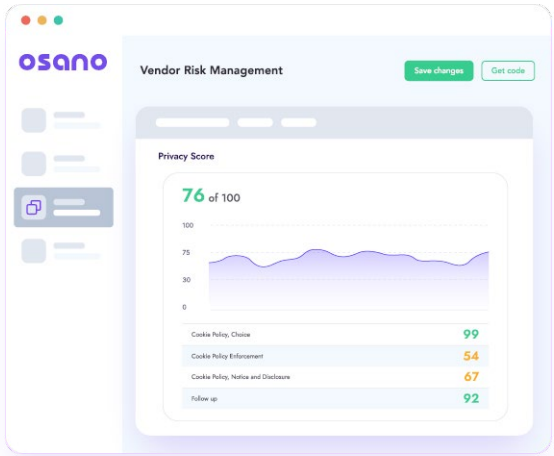
Data Mapping

Whether it's filling out a RoPA or data inventory, quickly responding to DSARs, or identifying data privacy risk across your organization, the first step is to understand where your organization stores personal data. If you don't know where personal data is being collected, where it lives, where it flows, and what's happening to it along the way, you'll have little insight into your organization's overall compliance posture.

Osano Data Mapping integrates with your Single-Sign On (SSO) provider to discover systems that contain PI. With our library of pre-built integrations, you can easily connect to common systems to automatically classify PI. For niche or proprietary systems, our RESTful APIs and semi-automated workflows make integration and data classification fast, accurate, and easy. As a result, you'll gain a visual, navigable data map that you can use to quickly identify your organization's data landscape at a glance.

Still, some organizations have hundreds or thousands of systems that potentially handle personal data—that's why Osano Data Mapping makes it easy to identify high- and low-priority data stores. Osano scores discovered systems' privacy risk based on the data fields they contain, the vendors they export data to, the identities they handle, and other factors, enabling you to quickly determine which data stores create the greatest risk and which require the greatest effort. Similarly, you'll be able to flag irrelevant or deprecated data stores, cutting down on the amount of review you need to conduct on your data map. You can always return to review flagged data stores just in case you change your mind.

Managing manual spreadsheets and tables to serve as your data map can be a full-time job; even if your organization has data analytics specialists and systems, data privacy compliance needs often are the lowest priority for those in-demand resources. Osano Data Mapping gives privacy professionals a dedicated tool to quickly establish a data map to serve as the foundation for downstream compliance activities.



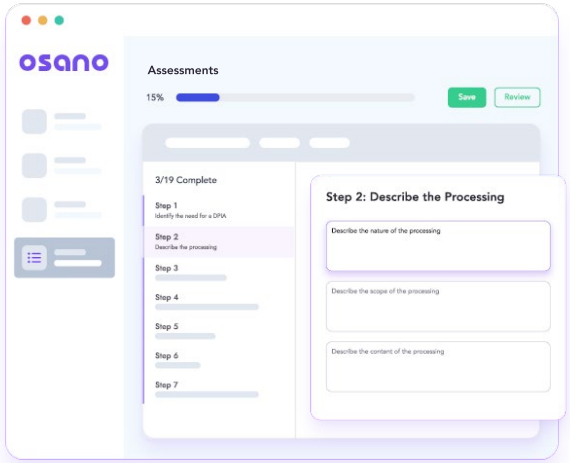
Vendor Risk Management

Vendor risk is especially challenging to manage—after all, you don't have as much insight into your vendors' operations as you do your own. The research and assessment process can be arduous, especially if you find a vendor you like, only to discover their privacy practices are not up to your standards. Your colleagues in development, sales, marketing, and other departments can easily become frustrated if they feel they're being blocked from working with the partners they need to work with to be effective.

Osano enables you to rapidly identify trustworthy partners through our database of over 11,000 vendors, each scored with our Vendor Score. Using a combination of expert review, machine learning, and a proprietary 163-item ontology, Osano generates a Vendor Score that allows you to evaluate vendor privacy practices at a glance. What's more, Osano's other capabilities can help you automatically identify vendors and add them to your organization's vendor privacy list.

- When Osano manages cookie consent on your website, it automatically scans and discovers any cookies or scripts associated with vendors and automatically adds those vendors to your vendor inventory.
- Data stores tracked by Osano for subject rights management are analyzed for vendor associations; if a data store belongs to a vendor, that vendor is automatically added to your inventory.
- And of course, you can manually add vendors to your inventory as well.

When vendors are subject to lawsuits over privacy violations or change their privacy policies, Osano automatically alerts you, ensuring you can quickly keep up with new sources of risk in your vendor ecosystem. We also provide templated vendor assessments so you can launch your own investigations into vendor privacy for regular or as-needed assessments.



Privacy Risk Assessments

Manually performing privacy risk assessments can be highly time-consuming, requiring you to:

- Search for the right assessment to fit your unique circumstances.
- Modify those assessments.
- Track which have been completed, which are at risk, and which are overdue.
- Follow up with stakeholders who have yet to complete a necessary assignment.
- Manage and store completed assessments.

Instead, using Osano to manage the assessment workflow makes this process significantly faster and less arduous. We provide a library of standards-based templates for assessment types like vendor risk assessments, data privacy impact assessments, RoPAs, and more. In Osano, you can quickly view which assessments are in progress, which have been completed, and which are at risk. When deadlines approach, Osano notifies assignees of outstanding assessments they need to complete.

Save Time for the Work Only You Can Complete

With Osano automating the tasks described above and more, you'll have the bandwidth to turn your attention to the critical privacy activities that can take your privacy program to the next level, including privacy-by-design processes, training and awareness, your privacy culture, governance and accountability, and similar elements.

Schedule a demo of Osano today to find out how you can increase the maturity of your data privacy program.

With Osano, building, managing, and scaling your privacy program becomes simple. Schedule a demo today.

Book a Demo

osano