SafeGuard Privacy

The Privacy Success Playbook

The Ultimate 30/60/90-Day Action Plan for People in a New Privacy Role

July 2025 | safeguardprivacy.com

Introduction

Get Privacy Right From Day One

Starting a new privacy role — even for experienced privacy professionals — can feel overwhelming. There are a thousand things that might deserve your attention, and it can be hard to know where to start.

That's why we created this SafeGuard Privacy Three-Phase Action Plan. It was created with the input of top privacy leaders in their field to help you protect your customer's data, get stakeholder buy-in, and effectively manage compliance risks from Day One.

Let's go!

Don't worry. You got this.

Before you start: Set yourself up for success

There are three pillars of management to keep in mind throughout your program:

Managing Yourself	Managing Your Data	Managing Your Organization
Adopt a Privacy by Design mindset Integrate privacy considerations into the design and development of new systems and processes across the entire organization right from the start.	**Data Mapping** Conduct a comprehensive inventory of all personal data held by your organization, including where it originates, how it is used, and where it is stored.	**Create a clearly defined scope, goals, and boundaries** Clearly outline the scope of your privacy program, set specific, measurable goals, and define the boundaries of what your efforts will and will not cover.
Keep up to date with the entire risk landscape Keep up to date with all applicable privacy regulations (such as GDPR, CCPA and other US states, and HIPAA) and all the types of personal data your organization collects and processes.	**Transparency and accountability** Clearly communicate privacy practices to everyone you collect data from, and be prepared to answer questions about how their data is handled.	**Get executive buy-in** Clearly communicate the importance of privacy compliance, including avoiding reputation damage. Customer trust is costly to earn and expensive to lose.

Your First 30 Days: Discovery

List or Whiteboard What Already Exists

☑

List or whiteboard what is already in place. Note weaknesses and gaps to be addressed.

Identify Existing Data Inventories

Determine whether comprehensive data inventories have been done to identify all personal data collected, stored, and processed by the organization, including data sources, usage, and retention periods.
Understand how the inventory is maintained and updated.
Identify the technologies, if any, supporting the data inventory and mapping, including meta data management, data tagging, and unstructured data scanning tools.

Legal and Regulatory Review

Understand relevant privacy laws and determine which laws apply to your organization. This includes regulations like GDPR, CCPA and other US states, GLBA for financial services, or HIPAA for healthcare.

Understand whether your organization has been subject to any investigative demand, enforcement settlement, and/or lawsuit.

Governance Review

Understand whether the company has a privacy framework it uses to manage compliance with privacy laws, and whether it is sufficient.

Analyze existing privacy policies and procedures and identify areas for improvement to ensure transparency and clarity for users.
Prioritize key policies and procedures including your customer-facing Privacy Policy, incident response plan, cybersecurity policies, and processes to respond to consumer data rights requests.

Hold Stakeholder Meetings to Improve Alignment and Communication

☑

Look for allies! They can be essential to the success of your program.

Internal stakeholders

Communication is vital to building and maintaining a successful privacy plan. Meet with key organizational stakeholders to understand data handling practices and identify potential privacy concerns. Learn about stakeholders' business goals and challenges.

- **CISO and Security** (this function may be a part of your IT team): What physical and technical controls are in place? What known gaps exist in data management and security?
- **Legal/Risk/Compliance:** What are the legal team's concerns with privacy in general? What work has been done on privacy to date? What is working/not working?
- **Sales and Marketing:** How are they using data now? What Privacy concerns do they and/or their customers or vendors currently have? How would additional guardrails or privacy processes impact their function and activities (e.g., data minimization, vendor management)?
- **CFO:** What resources exist to fund a privacy program and related technology? What is the budget cycle and process at a high level? What other teams may have a need for privacy tech that can contribute?
- **CEO:** What are their concerns about privacy in general? Why do they want a Privacy program, and what are they worried about? These factors are significant and may include breaches, cyber-attacks, and reputation risks arising from non-compliance.

When your challenges and opportunities align with other stakeholders, try to make them your allies: the more partners you have the better. Discuss how you might partner with them, and be sure to clarify roles and responsibilities.

External stakeholders

Ask all vendors — including those that work with your CTO and IT — how they are helping with your company's data privacy responsibilities. Take notes and be sure to capture what you learn. Get a basic understanding of data handling practices, how long data is kept, where it is stored, and the general costs to manage and store data. Also, remember that these vendors work every day with privacy leaders like you. The best vendors can be an excellent source of information about what is working and not working.
Which vendors have access to your company's or your customer's data? Do you have written contracts in place with these vendors? Who is managing those vendors? Has anyone performed privacy assessments in addition to security assessments?

Get ready for the next phase

Review everything you've learned

Go through your notes, note weaknesses and gaps to be addressed and rank them in order of priority.

Identify quick fixes

Are there any glaring gaps you can address with a quick fix? For example, if there is no privacy policy on the website, draft and implement one ASAP!

Training

Determine what training programs exist for employees, leaders, and vendors. Some laws, including CCPA, require that all employees who touch customer data must be trained.

Stay Relevant

What tools and resources do you as the CPO need to stay current on developments in this rapidly changing area? What conferences might be helpful to you? How will you develop a network of other privacy leaders? Which thought leaders might you follow on LinkedIn or otherwise? There are several organizations, including the IAPP, Future of Privacy Forum, and TeachPrivacy, that you can look to for training, thought leadership, and industry events.

Days 30-60: Planning

Improving Communications and Setting Expectations

☑

Now that you understand your organization's privacy practices, stakeholders, and the critical gaps to fill, it's time to start planning your program. What laws do you need to follow? What assessments and training do you need to put together?

Privacy Program Framework

Develop a privacy program framework outlining key goals, objectives, and metrics to measure progress. Include Privacy by Design concepts in all phases of the program. Metrics to include are:

- **Legal and Regulatory Analysis and Privacy Risk Assessments**
  Assess specific requirements from relevant laws that apply to your business. Conduct a risk assessment to identify high-priority privacy risks based on data sensitivity and potential impact. Use assessments that are written to the entirety of the law (if not done already). A platform like SafeGuard Privacy includes comprehensive standardized assessments and an automated gap analysis tool to make this easier.
- **Privacy Training Plan**
  Design a targeted privacy awareness training program for all employees at all levels, including leaders, vendors, and other third parties who have access to data. CCPA requires employee training for any employee who touches consumer data.
- **Vendor Management Program Review**
  Develop a plan to address any gaps uncovered with regard to vendor management in your first 30 days. Ensure that you are addressing data access and security requirements and that you have current written agreements in place with vendors that address current laws, including various US state laws.

Remember that if you do not ask for a budget, you will not get one!

- **Conduct vendor assessments on your vendors**
  Prioritize your vendors by risk and importance. Using standard assessments and technology to centralize and streamline your vendors can make your team more efficient and speed up deal processes. This may include checking your website's advertising pixels to ensure you know exactly who is touching what consumer data.
- **Data Subject Access Request (DSAR) Process**
  If such a process does not yet exist, develop a plan to establish a streamlined process for handling data subject access requests. You will need to ensure that it is easy for consumers to make the requests and honor them appropriately.
- **Company Alignment and Communication**
  Check in with your stakeholders. Secure buy-in from senior leadership to prioritize privacy initiatives and allocate necessary technology and/or legal resources. You may find you have friends willing to help you with budgets (such as marketing and sales looking to provide vendor management support).

Collaboration is key.

Days 60-90: Implementation and Communication

Time to start implementing your plan.

Review the previous phases and start putting things into action.

- **Establish Privacy Policies and Procedures**
  Develop clear data collection, use, sharing, retention, and disposal guidelines, including data subject rights. Implement necessary updates to privacy policies based on risk assessment and stakeholder feedback.
- **Implement Data Protection Measures**
  Utilize appropriate technical and organizational controls to safeguard personal data, such as encryption, access controls, and data minimization. Your security/IT team should be on board with you.
- **Data Subject Access Request (DSAR) Process**
  Implement a streamlined process for handling data subject access requests.
- **Incident Response Plan**
  Implement a privacy incident response plan to effectively address data breaches and privacy concerns.
- **Testing and Ongoing Monitoring**
  Establish a monitoring and review process to adapt the program. Analyze potential privacy risks associated with your data processing activities, considering factors like data sensitivity, access controls, and potential breaches. Develop a program to conduct periodic risk assessments to test your program. Pay special attention to new products and material changes to existing ones that involve new or modified uses of personal information.

Leverage your information security team's work. For example, use their Security Incident Response Plan as a guide for privacy incident response.

- **Customer Communication**
  Depending on your organization, you may need to communicate privacy policy changes with customers and consumers. That could include an email to subscribers or a website notification that it has changed and they should read the latest version.
- **Company Alignment and Communication**
  Communicate privacy initiatives to employees and relevant stakeholders. Now that you are implementing, ensure your stakeholders understand your privacy KPIs.

Privacy is an ongoing process and continues to evolve. Your plan will, too.

The plan is in place, but the work continues.

You made it! You've got a great plan. But that's just the beginning. Privacy regulation continues to evolve in the US and around the globe and you will need to be diligent in sticking to your plan and shifting gears as business and regulatory needs change. But now that you've built your program on a solid foundation, you should find it easier to keep up and adjust.

The Ultimate Privacy Program Checklist

The handy checklist on the next two pages will help keep you on track as you build out your program. Additionally, you can **download a spreadsheet** version here.

Ultimate Privacy Program Checklist

Area	Information Gathering Checklist	Phase 1 30-Day Action Plan	Phase 2 60-Day Action Plan	Phase 3 90-Day Action Plan
Organizational Understanding Understand the organization's mission, objectives, stakeholders, and activities.	✓ **Mission Vision and Culture**. Understand and prioritize to inform the program design assumption, risk tolerance and approaches for its privacy program. ✓ **Roles in the Ecosystem**. Understand the organization's role in the data-processing ecosystem (e.g., business, service provider, third parties, B2B, business associate, etc.). ✓ **Types of Data**. At a high level, understand the key types of PI processed by the organization. ✓ **Industry**. Understand the desired maturity level for the industry. ✓ **Key Stakeholders.** Identify key stakeholders (e.g., Legal, Privacy, Info Sec, Data Governance, IT, Marketing, HR, Internal Audit) both vertically and horizontally throughout the organization. ✓ **Organizational Collaboration.** Who are the privacy team members (if any) and key business stakeholders for each area? ✓ **Public Disclosures**. Review public privacy disclosures and data collection interfaces. ✓ **Program Maturity**. Review the previous program maturity assessment(s), if any.	**Meet with key stakeholders** both vertically (e.g., executive sponsor, mid-level) and horizontally throughout the organization. **Strategize on gathering information** in the checklist most efficiently without overwhelming the business or obtaining insufficient information. **Understand the budget** and its allocation for the privacy team and other functions supporting privacy and the budgeting processes. **Gain a preliminary understanding of risks,** including legal risks, processes, governance, and technology, to inform the preliminary risk assessment. **Identify the privacy technology stack**, including privacy impact assessment platform, vendor due diligence platform, online tracking technology scanning tools, metadata management and tagging, auditing, and documentation tools.	**Continue to gather information** and identify prioritized areas for follow-ups. **Identify preliminary risks impressions,** including major areas with problematic data processing, missing governance controls, lacking privacy technologies, or areas of improvement for team competency **Categorize risk factors** based on priority and efforts (e.g., high risk-high effort, high risk-low effort, low risk-high effort, and low risk-low effort). **Address those in high-priority and low efforts** (e.g., updating privacy disclosure if outdated) **Identify missing controls and technologies** at a high-level, such as missing vendor due diligence processes and tools.	**Continue to gather information** and identify prioritized areas for follow-ups. **Prioritize items** to build or enhance the maturity of the program for the first year focused on high-risk items (e.g., targeted advertising privacy impact assessment and vendor due diligence). **Compose budget recommendations** based on risk exposure, enterprise risk tolerance, and current maturity level. **Address high-priority efforts as resource permit**, such as making necessary updates to the internal policies and processes. **Communicate the program improvement plan** with the relevant stakeholders and strategize on change management.

Ultimate Privacy Program Checklist

Area	Information Gathering Checklist	Phase 1 30-Day Action Plan	Phase 2 60-Day Action Plan	Phase 3 90-Day Action Plan
Inventory and Mapping Data processing by systems, products, or services is understood and informs the management of privacy risk.	✓ **Systems/products/services.** Understand whether, how, and where systems, products, or services that process data are inventoried. ✓ **Identify owners or operators** and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. ✓ **Understand the categories of individuals** (e.g., customers, employees or prospective employees, consumers) whose data are being processed and inventoried. ✓ **Understand data processing activities,** including how data processing activities of the systems/products/services are inventoried, what data elements are processed and shared, purpose of processing, sources, processing environment, geographic location, roles of the component owners/operators; and interactions of individuals or third parties.	**Consider engaging vendors** to facilitate the privacy risk and program maturity assessment.	**Start implementation or update of consent and DSAR** tools where necessary.	**Start protection implementation** for technologies where necessary, including data inventory, mapping and governance. **Engage IT/Security** teams to ensure buy-in and success.
Legal Risks Regulatory	✓ **Legal Requirements.** Understand and Analyze relevant privacy laws (GDPR, CCPA, etc.) applicable to the enterprise. ✓ **Enforcement Actions.** Understand whether the enterprise has been subject to any investigative demand and settlement agreement in force. ✓ **Litigations.** Understand the past, ongoing, and potential privacy lawsuits.	**Stay relevant**. Choose tools that help you stay current with privacy legislation and regulation. **Quick fix glaring gaps**, such as a non-existent or inadequate privacy policy.	**Conduct Risk Assessments** to identify high-priority privacy risks based on data sensitivity and potential impact. **Implement Employee Training** where required (e.g. CCPA, GDPR)	**Continue to monitor regulatory landscape** to inform your program.

The Most Successful Privacy Leaders Choose SafeGuard Privacy

This Ultimate Privacy Program Checklist was created for people in a new privacy role, and is just the beginning of how SafeGuard Privacy can help you succeed. SafeGuard Privacy the only privacy compliance solution purpose-built for companies like yours that use consumer data.

We're the first legal assessment and vendor management platform for advertisers, publishers, and AdTech. We answer what other platforms don't.

10X

Speed to Compliance
Versus months of work. Get it done in hours.

1,000+

Hours Saved
Versus starting from scratch or using a framework

Up to 80%

Cost Savings
Versus doing it yourself with internal and external resources

If you're starting a new job, SafeGuard Privacy means knowing that one part of your very lengthy task list is completely under control.

Good luck in your new position and let's talk about how we can help!

Email: hello@safeguardprivacy.com **Demo:** safeguardprivacy.com

SafeGuard Privacy Features

YOUR COMPLIANCE

Assessing

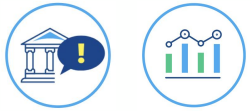
- Pre-written Comprehensive Assessments with multiple choice questions
  - US Multistate Substantial Compliance and Sensitive Data Assessments
  - Individual US State Assessments
  - IAB industry vertical specific questionnaires (for Advertiser & Agency, SSPs, DSP, Publisher, etc)
  - NAI Code of Conduct, COPPA, HIPAA, and BBB National Programs Verifications
- SafeGuard Simplified Commentary with each question
- DPIA Tools

Remediation

- Business continuity: all of your compliance information in one place
- Automated gap analysis: Find gaps and remediate while answering questions
- Remote team collaboration
- Real-time reporting
- Policy, Contract, & Document Wizards & Templates
- Kanban style project board for to manage remediation tasks
- Assign tasks to teammates, prioritize, and track progress
- In-depth virtual training to educate employees with handbooks and quizzes

Assessment Sharing

- Complete an assessment and share your answers and supporting evidence with your all of your partners on the platform
- No spreadsheets or email chasing
- It's your secure workspace, you control what you share & with whom
- Third party review features include dynamic updates and communication with your partners
- Event logging and history keep your ongoing audit trail intact
- Quickly export compliance summary reports for stakeholders



VENDOR COMPLIANCE

Vendor Compliance Hub

- Streamline required vendor diligence with standardized US and global law assessments
- Vendor Dashboard: your vendors assessments, risk scores, and compliance information in one place
- Deep dive into shared assessments and review every answer
- No spreadsheets or email chasing
- Contract addendum wizards can quickly create required counterparty agreements
- Real-time vendor reporting and vendor export
- Benchmark your vendors