How to Evolve Your Privacy & Data Protection Program

Checklist Part I: Building the Foundation

BDO

Safeguarding consumer trust and your company's integrity requires a proactive journey to privacy and data protection. Each company is the guardian of its customers data, which means each company requires a comprehensive privacy roadmap to maintain compliance and foster a culture of trust. Elevating data privacy standards is more than a legal requirement; a company's privacy and data protection program must be strategic to enhance brand loyalty and customer and employee satisfaction.

However, as privacy and data protection regulations continue to evolve, and customers demand more control over their data, many technology companies struggle to update their privacy and data protection compliance programs accordingly. With cyber threats growing more sophisticated, a well-structured corporate privacy roadmap is the first line of defense in preserving data integrity. Data privacy compliance is a journey — companies must always evolve and iterate on their programs. It is important to understand that 100% compliance is not the goal but rather developing an ongoing, overarching culture of compliance.

As technology companies embark on building a strong program foundation, one critical element to keep in mind — regardless of the maturity level of your current privacy & data protection program — is adopting a Data Protection 'by Design' and 'by Default' approach. Integrating privacy and data protection practices into processing activities at the onset of product or service development, IT development methodologies, and/or into vendor procurement policies helps proactively mitigate risk and close compliance gaps. It builds confidence that the data is managed responsibly and transparently, thereby reducing the risk of privacy breaches and unauthorized data access. Most regulations require organizations to implement robust privacy measures to avoid legal and financial fines, but Data Protection by Design and by Default helps to go beyond that. With this approach, organizations can foster trust with users and consumers by minimizing data collection, incorporating security measures into product or service design, and reducing the likelihood of privacy violations.

Have You Seen Any of These Red Flags?

Before getting started with our checklist, take a moment to think about whether your company has experienced any of the following scenarios, which may be a driver for change.

- Consumers complain about a lack of transparency in the amount of personal data you collect about them, or the ways in which you handle their personal data.
    - More than ever, users are aware of the way their data is being used and protected. Trust between consumers and companies is critical to success, but according to our **2023 Tech CFO Outlook Survey**, that trust is eroding.
- Your company receives a high volume of complaints or regulatory inquiries.
- Your services or products put you in the category of high-risk controllers or processors because of the amount of personal data you collect or process.
- Your company experienced a decline in user engagement, and it is driving a reduction in market share or brand recognition.
- Privacy activists are filing lawsuits against your company or your peers.
- Your industry is on the receiving end of frequent regulatory fines.
    - This is often a tell-tale sign that regulators are scrutinizing tech companies or companies within your industry, so your business should work to shore up data privacy compliance processes sooner than later.
- Your company has incurred a regulatory fine.

COMMON GAPS IN PRIVACY & DATA PROTECTION PROGRAMS

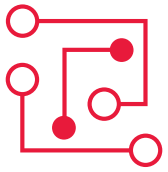
While identifying privacy and/or data protection red flags may be straightforward, companies need to uncover the program gaps that may be leading to potentially problematic scenarios to resolve issues and strengthen their compliance. Here are four common compliance gaps to look for and address within your organization:

1. **Tracking technologies:** Everyone loves a good cookie, but what happens when that cookie stores information about website and mobile app users that does not comply with user preferences or privacy laws? Companies, especially in the tech industry, continue to struggle with tracking technology (pixels, web beacons, and cookies) compliance. We regularly see companies fined for improperly using outdated tracking technologies, writing code that leaks data, and violating regulations. Data leakage can lead to a report of a data breach with regulators.

2. **Data collection and consent:** Companies must balance their need to collect personal data with clear and informed consent. For U.S companies this is a challenge since not all laws have caught up with consumer expectations. However, as data usage becomes more intricate and globalized, user consent is one of the most pivotal areas of privacy compliance programs.

3. **Third-party data sharing:** Regardless of where you operate, third-party data sharing compliance is necessary, and third-party due diligence is more important than ever. Most privacy regulations require companies to determine whether their vendors adhere to the same level of privacy and data protection standards in which the hiring company does. Vendor assessments and an understanding of inward and outward data flows identify potential risks and allow an organization to stop sharing data with a third-party efficiently when they have visibility into these two elements.

4. **Emerging technologies:** Integrating innovative technologies like artificial intelligence (AI), Internet of Things (IoT), blockchain, and biometrics while maintaining privacy standards poses challenges in understanding the potential risks and implementing safeguards. These technologies require the tech industry to continuously reassess and update their privacy policies and practices to promote compliance and protect users' personal data.



Once you establish a baseline of common, potential gaps, it's time to think about how to evaluate your privacy and data protection compliance program. Not sure where to start? Our checklist can help you determine steps you can take to initiate or upgrade your program.

Building the Baseline Program

This first checklist serves as part one of a three-part series to help your technology company develop a privacy & data protection roadmap and prepare for enhanced regulator and stakeholder scrutiny — especially for those in the business-to-consumer category.

The items below represent baseline best practices for privacy and data protection compliance programs. This comprehensive list, while not inclusive of every single tactic your company can or should potentially implement, provides a starting point to build the foundation prior to tackling more complex activities.

- [ ] **Do you have buy-in to build or rebuild your privacy and data protection program?** Privacy requires a plan, budget, and buy-in at the highest levels of the organization. Build your business case, identify an executive sponsor, and get board approval to invest in consumer data protection.

- [ ] **Do you know where your personal data resides and who has access to it?** Organizing and knowing where personal data resides and who can access it or when it is shared is a hallmark of a foundational, compliant data privacy program. To begin to link data inventory to your organization's privacy program, develop a comprehensive data inventory and then identify what is personal or sensitive data. Key steps to take include: (1) identify data sources, (2) categorize data into personal, sensitive, and other categories to evaluate its privacy significance, (3) map the data flow, (4) determine who owns each data category and is responsible for proper handling, (5) assess data flow, transfer, and other risks associated with each category, (6) record how data is collected, stored, processed, and shared, (7) identify current organizational data practices to align with privacy regulations, (8) define retention periods, (9) understand and update access controls, and (10) establish a timeline to continually review and update the inventory.

- [ ] **Is data protection a priority at the top?** To build a formidable privacy compliance program, data protection must be viewed as a priority. It is also important to educate the board and executive teams to ensure they understand the differences between privacy and security. Privacy and security standards and process make up data protection best practices, and while there is critical overlap, they are inherently different.

  - Security protects data from unauthorized access, breaches, and cyberattacks. It allows an organization to safeguard personal data and information from internal and external threats.
  - Privacy, on the other hand, focuses on the appropriate handling of and use of personal data. Privacy measures focus on minimizing the collection of sensitive and personal data, obtaining consent to use that data, and ensuring that data is used for its intended purposes.

- [ ] **Is the board engaged in privacy and data protection discussions?** The commitment of the board is essential to drive reputation and trust. The board's oversight of privacy practices helps maintain the company's brand and credibility, reduce the risk of data breaches and its fiscal impact, and drive employee engagement to practice good data hygiene and protect personal data. When the board is committed to privacy and data protection, it is a competitive advantage.

- [ ] **Is privacy and data protection part of your corporate strategy?** Privacy considerations can influence strategic decisions, especially for the tech industry, about product development, partnerships, and data sharing practices. Building internal and external support channels to evaluate ways to promote privacy and data protection as a differentiator helps to build the program's business case. Once you integrate privacy and data protection as part of the organization's strategy, it will become apparent to users and consumers that the company is serious about protecting their data.

- [ ] **Are you transparent and do you share data practices with the public?** Your policies around data collection and processing should be highly transparent. This means proactively sharing those polices and privacy notices with customers. Studies have shown that companies that are transparent with the public about how data is collected, processed, and shared are held in higher regard by customers and regulators.

- [ ] **Do you destroy outdated and unnecessary data?** Data retention is a critical component of every privacy program because it demonstrates that you are trying to reduce the risk of data leaks and unauthorized use. Establish retention schedules and policies to guide employees for how long distinct categories should be retained and destroyed.

- [ ] **Has your company established a breach response program and evaluated it?** Data breach and incident response programs are required under every privacy law regardless of your location. Companies must abide by regulations that dictate how to craft a data breach response program, from the detection of a potential breach to how long the organization must notify board members, employees, and customers after one has occurred. Having a data breach or incident response program as part of your privacy and data protection program is no longer "nice to have" — it is an absolute must.

- [ ] **Have you appointed a Data Protection Officer?** It is likely that a DPO (Data Protection Officer) is required in regions where you sell or operate. Review regulations to determine locations where you are required to have a DPO and identify regional or local in - country appointments. A common approach our clients find useful is to appoint a Global DPO with in country or regional appointments to offset time zone, language, and cultural challenges.

- [ ] **Are employees required to complete privacy, security, and data protection training at regular intervals?** At this stage, it is critical that companies establish data privacy awareness and training for employees. Guarding customer data is the responsibility of everyone at the organization so it should be part of regular training, awareness campaigns, and individual goals.

Going Beyond the Groundwork

Using this first checklist can guide you as you build an optimized privacy and data protection program that helps restore trust with your stakeholders, employees, and customers. That trust is paramount for building organizational resiliency.

In our next checklist, Maturing the Program, we'll provide guidance on how to evolve the steps from the foundational stage, looking at tactics such as establishing a Data Protection Committee and finetuning employee training programs. We'll also share more insights around ongoing compliance monitoring because assessing compliance holistically across the organization on a regular basis is critical for developing and maintaining a resilient program.

If, after completing this first assessment, you would like support strengthening your data privacy compliance program, you may benefit from the help of an experienced third-party advisor. At BDO, we have deep industry experience and can help technology companies get their data privacy programs on track no matter what stage you are in: foundational, mature, or optimized.

With a scalable and customized approach, we will work with your organization to assess your current program based on our 12-step modular framework. Our integrated suite of solutions can help you address every element of privacy, data governance, analytics, crisis management, insurance response, cybersecurity, and risk management, thereby strengthening your company's compliance posture.

Finally, we use Privacy by Design and by Default and Data Protection by Design and by Default approaches so that you can feel confident in your organization's ability to establish a program — and enhance it — in a way that protects the integrity of the data you collect now and in the future.

Ready to learn more about building a data privacy program? Contact BDO today ▶

CONTACT US

HANK GALLIGAN
National Technology Industry Leader
hgalligan@bdo.com

KAREN SCHULER
Principal, Global Privacy & Data Protection Chair
kschuler@bdo.com