How to Evolve Your Privacy & Data Protection Program

CHECKLIST PART II: MATURING THE PROGRAM

As technology companies continue on their data privacy compliance journeys, it is important that they iterate on the basics of their program to enhance data privacy and protection practices, maintain compliance, and earn customers' trust.

In Part I of our checklist, **Building the Foundation**, we addressed a number of imperative baseline practices that tech companies should implement. This included securing executive buy-in, weaving in data privacy as part of the corporate strategy, and establishing a breach response program. After organizations have successfully worked through Part I of the checklist, it's time to focus on maturing the program.

Using a Data Protection 'by Design' and 'by Default' approach remains critical, no matter the status of your company's program. Integrating privacy and data protection practices into processing activities at the onset of product or service development, IT development methodologies, and into vendor procurement policies helps proactively mitigate risk and close compliance gaps. While many regulations already require organizations to implement robust and stringent measures to avoid financial fines, adopting a Data Protection 'by Design' approach allows organizations to go past compliance and toward proactivity. What more can you be doing to minimize data collection? Are there strong security measures built into every product design? Asking these questions — and working to find the answers — helps to build trust with customers.

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 We regularly see companies fined for improperly using outdated tracking technologies, writing code that leaks data, and violating regulations.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 as the hiring company. 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 tech companies to continuously reassess and update their privacy policies and practices to promote compliance and protect users' personal data.

Now that you have established an understanding of potential gaps and used Part I of our Privacy & Data Protection Checklist, consider moving on to Part II of our three-part series. The below checklist can help you determine your next steps for upgrading your program. Keep in mind that as programs evolve, the steps in the foundational stage progress.

Maturing the Program

□ **Has your company implemented a Data Protection Committee?**
It is impossible for privacy leaders to do their jobs without help from others. A Data Protection Committee offers an opportunity for a group to become responsible for overseeing and ensuring compliance with privacy and data protection regulations. The committee typically consists of individuals from privacy, legal, risk management, Information Technology (IT), security, marketing, sales, and business operations. Participation from this team will increase your company's likelihood of advancing their privacy compliance program and establishing a culture of compliance.

□ **Do you have a dedicated privacy and data protection team?**
In addition to the Data Protection Committee, building a multidisciplinary team is a cornerstone of a mature approach. With a dedicated team, your company can better develop and institute a comprehensive privacy and data protection governance framework.

□ **Have you established Privacy Impact Assessments?**
To identify and remediate potential privacy risks associated with a project, system, or process, steps must be taken to implement Privacy Impact Assessments (PIAs). PIAs should ask users about the project definition and the types of data that will be collected, where data will flow, and how data will be used. During the assessment, the privacy team should identify potential privacy risks, evaluate whether data collection and use is proportionate, and define mitigation strategies. If the team determines that sensitive data will be collected, a Data Protection Impact Assessment (DPIA) may be required, and it could be necessary for the Data Protection Officer (DPO) to review and sign off on the DPIA to comply with regulations. Establish a process that engages the business and holds them accountable for complying with the organization's obligations and policies.

□ **Do you have a defined data subject request and monitoring process?**
Prior to 2018, it was an uncommon practice to respond to data subject requests. Companies in Europe established early processes to comply with local laws, but until the EU's enforcement of the General Data Protection Regulation (GDPR) began, companies addressed these requests on an ad hoc basis. In 2023, companies maintain Privacy Business Process Outsourcing (BPO) and customer support teams to constantly monitor and manage data subject requests. Technology companies often integrate features for data subject access requests into their apps. However, there are several additional steps that should be considered beyond having these features available in apps: (1) monitor applicable regulations for changes in handling data subject requests, (2) audit the types of requests you receive to identify gaps, (3) designate points of contact and escalation points, (4) standardize processes and workflows, (5) define how individuals can submit data subject requests, (6) revisit identity authentication practices, (7) review acknowledgement, standard, and automated messages to match the current environment, (8) review timelines and data outputs to recipients, (9) revisit response formats and whether system changes impact the formats, (10) evaluate potential risks with large data requests and conduct PIAs when necessary, (11) revisit data portability formats and record keeping, (12) define a process for handling appeals, and (13) review employee and software developer training to match the current regulatory needs.

□ Have you revisited your training program?

Marketing and software developers require distinct privacy and data protection training that you would not typically offer to other employees. Consider reviewing the types of advanced training that you offer to select employee groups to tailor it to enhance product development and marketing activities.

□ Does your technology company conduct data transfer impact assessments (DTIAs)?

DTIAs are important for technology companies due to the increasing complexity of data flow across borders. Technology companies often operate on a global scale, with data moving across authorities. DTIAs help assess the risks and compliance requirements associated with transferring data to different countries. DTIAs also demonstrate a commitment to protecting personal data and can enhance consumer trust, particularly as regulators continue to scrutinize data sharing practices.

Moving Forward on Maturity

Using the above checklist can guide you as you iterate on your existing privacy and data protection program. However, it's important to remember that privacy and data protection efforts are never complete. These programs are always evolving as regulations change and implementation deadlines arrive, which means tech companies must continually reassess themselves in accordance with those changes.

In our next checklist, Creating an Optimized Program, we'll provide guidance on how to evolve the steps in this checklist to fully optimize your privacy and data protection program. This checklist will include tactics such as implementing automation capabilities, adopting AI, and assessing the risks associated with marketing technology.

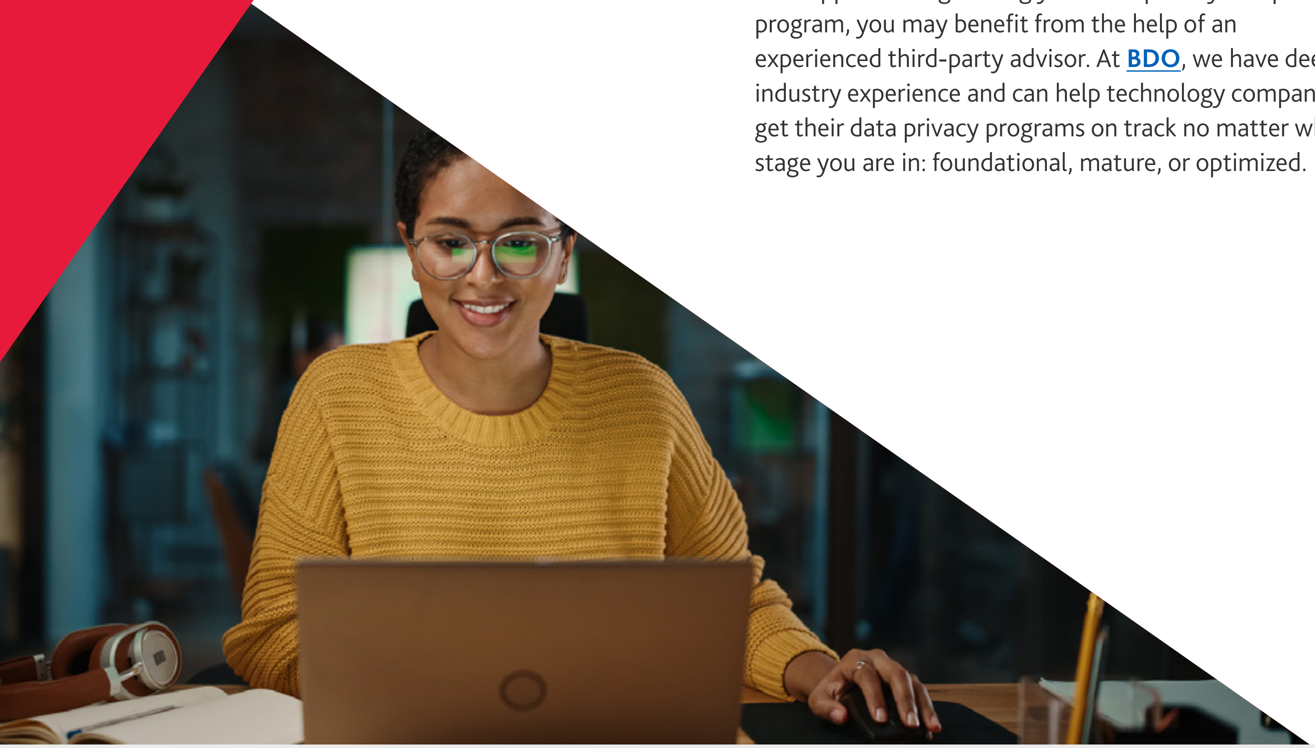
If, after completing this second assessment, you would like support strengthening your data privacy compliance program, you may benefit from the help of an experienced third-party advisor. At BDO, we have deep industry experience and can help technology companies get their data privacy programs on track 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.

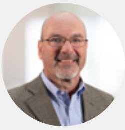
Finally, we use Privacy by Design and by Default and Data Protection by Design and by Default approaches so that you can feel confident in your organization's ability to establish a program — and enhance it — in a way that protects the integrity of the data you collect now and in the future.

Ready to enhance your data privacy program?

CONTACT BDO TODAY



CONTACT US



HANK GALLIGAN
National Technology Industry Leader
hgalligan@bdo.com

KAREN SCHULER
National Privacy & Data Protection Practice Leader
kschuler@bdo.com

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C, a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms: www.bdo.com

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.