How to Evolve Your Privacy & Data Protection Program

Checklist Part III: Optimizing the Program

Building and maturing a robust privacy and data protection program brings technology companies closer to compliance with each improvement. But in today's highly regulated landscape where new rulings and updates are released from different regulatory bodies all the time, it is often difficult for tech companies to achieve 100% compliance.

That's why the goal of any privacy and data protection program is to foster a culture of compliance that builds trust with stakeholders. Because privacy and data protection programs are always evolving as regulations change and implementation deadlines arrive, it is critical that tech companies continually reassess and iterate on their processes and policies.

That is why Part III — the final part — of our Checklist Series is not focused on completing a privacy and data protection program, but rather encouraging technology companies to continually enhance their existing program. This checklist, Optimizing the Program, will focus on implementing automation, remaining agile, and carefully assessing marketing technology, among other elements.

If you missed Part I or Part II of our checklist, take a moment to go back and work through those steps first before exploring how you can optimize your program.

Finally, remember that 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 helps 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.

For more on Data Protection 'by Design,' check out Part I of our Checklist Series ▶

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:

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.

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.

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.

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 checked the boxes from Part I and Part II of our Privacy & Data Protection Checklist, it's time to consider how you can optimize your program. Even if your company has implemented a sophisticated privacy and data protection program, there are still ways to improve the organization's posture. The below checklist can help you determine your next steps for strategically optimizing your program.

Optimizing the Program

□ **Has your technology company automated privacy and data protection processes?** Although it is helpful to start by handling processes manually, there are benefits to automating processes over time, including improving efficiency and reducing timelines and manual errors. Automation can be applied across multiple functions, including the customer data deletion process, acknowledging receipt of a request, identifying and mapping data sources, implementing tools to provide and withdraw consent for online data processing, using software to improve the Privacy Impact Assessment (PIA) and vendor assessment programs, automating the data subject request process, and more. Your company should also consider innovative ways that implementing AI for privacy compliance can advance the program and positioning.

□ **How well do your teams and systems work together?** By this time, you should have formed a Data Protection Committee, and a multidisciplinary team focused on privacy and data protection; however, silos may still exist across technology and people. Take steps to integrate different components and disparate systems to work together in an effective manner that promotes transparency and flexibility.

□ **Is your program adaptable and scalable?** When you started your privacy and data protection program, your company may have been a third of the size it is now. You need a program that is designed to serve your company as it exists today and as it may evolve tomorrow. Tech companies that implement overly rigid parameters could hamper the program's ability to adapt to shifts in the regulatory landscape. Your program should be flexible by design since it will need to change as you reassess the organization's compliance posture.

□ **Have you considered the impact of AI laws on internal processes?** AI is essential for tech companies to automate, learn, glean new insights, and improve functionality. However, new laws like the EU Digital Services Act can impact how AI is used within an organization. As another example, some U.S. state laws require companies using AI in the employment process to audit their programs annually to verify that hiring systems or processes using AI are not biased, racist, or sexist. As the regulatory landscape catches up with innovative technologies, tech companies must prepare to review or audit existing processes to maintain compliance.

□ **Is your company taking a risk-based approach to the use of marketing technology and advertising technology?** Consent management, personalization, segmentation, preference management, and efficiency are important considerations when implementing marketing and advertising technologies. Consider implementing a process that requires a Data Protection Impact Assessment (DPIA) before leveraging these technologies. Despite the benefits they can provide, these tools tend to over collect data and leak data from one platform to another. They may also inadvertently promote the violation of a user's ability to opt-out or provide consent, while exposing data to a greater risk of breaches. If you are using third-party vendors for these tools, it is also important to consider whether those companies are holding themselves to the same data privacy and protection standards as your organization. A few key vendor processes to investigate include:

- Protocols for cross-border data transferring and whether the data they are transferring can be done lawfully
- Adherence to identifying and remediating algorithmic biases, which, if not addressed, can lead to discriminatory outcomes
- Policies for data retention periods and whether data can be stored for the length of time that the tools purport

□ **Do you review your program on an annual basis and have internal audit teams review aspects of the program?** Ongoing compliance monitoring is always necessary. This means not only refining internal processes and frameworks, but also educating employees to stay current on regulatory changes that could impact company policies. When the privacy and data protection program has been updated in accordance with best practices, the organization is better prepared to consider and prepare for the implications of applicable laws, industry standards, and key program principles.

Data Privacy Compliance: Progress Over Perfection

An optimized privacy and data protection program achieves one goal above all else: it moves your company from a compliance-based organization to a trust-based organization.

Assessing compliance holistically across the organization on an ongoing basis — and knowing when and where to make improvements — is a key trait of an optimized program. The above checklist can help you develop a program that build trust with your stakeholders, employees, and customers. That trust is paramount for building organizational resilience.

If you're exploring ways to improve your program, consider working with a third-party advisor. At BDO, we have deep industry experience and can help technology companies get their data privacy programs on track.

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 compliance.

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 program to protect the integrity of the data you collect now and in the future.

Ready to optimize your 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

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.