PrivacyCheq

DPO's Guide to Working with IT to Operationalize GDPR Compliance

Introduction

The purpose of this guide is to inform Data Privacy Officers (DPO) about the notice and consent requirements of the EU's General Data Protection Regulation (GDPR) and provide an overview of what technical changes an organization needs to put in place to operationalize compliance. This document will help you understand the challenges involved with implementing these changes and discuss choices you and your IT team will have to tackle.

What is GDPR Operationalization?

There are many aspects of operationalizing GDPR compliance, which include identifying gaps and risks, updating privacy policies to cover different situations, updating data security protocols and processes, defining internal teams and roles, and determining how to systematize data subject notice and consent. One can think of operationalization as the "rubber on the road" moment where steps are taken both organizationally and procedurally in the organization to modify data practices and user interactions to achieve compliance. In general terms, operationalization will include:

- Capturing data subjects' explicit consent
- Providing explicit, concise, intelligible notice in plain language that specifies data collection purpose and discloses third parties with whom such data may be shared
- Internally checking against data subjects' consent choices each time their personal data is processed
- Giving data subjects the power to manage their consent by exercising their rights – such as the Right to Withdraw Consent, the Right to be Informed, the Right of Access, the Right to Rectification, the Right to Erasure, the Right to Restrict, the Right to Data Portability, the Right to Object to Direct Marketing Processing, and Rights Regarding Response to Auto Profiling
- Creating and maintaining logs and reports to prove to the appropriate supervisory authorities that a data controller has a data subject's consent at the time that data processing occurred
- Providing a secure channel of communication to data subjects to share personal data and publish notice in case of a breach

What is the role of the DPO with respect to operationalization technology decisions?

The DPO is generally responsible for developing the GDPR compliance strategy for an organization. They are very familiar with the data protection responsibilities within an organization and liaise with internal teams to develop and implement internal and external policies around data protection. However, the DPO is often not in the best position to understand the best ways to achieve the technological requirements to implement user flows and retention practices around user data and often works closely with IT teams to achieve implementation. The DPO's role in operationalization is that of a project

manager who breaks operationalization into technical requirements that IT can either develop in-house or outsource by licensing third party software.

Why not operationalize GDPR yourself?

You may consider if your organization could build adequate GDPR compliance technology without help from external technology providers. At a high level, it looks like a simple engineering project and you may question how hard it could it be. Before you and your IT team decide to go it alone, ask yourself these questions:

- **Who will build it?**

  Building software isn't free. You and your IT resources will have to spend time and resources taking on this task. Implementing compliance may not be groundbreaking engineering, but as you may have learned from other internal privacy technology projects, prioritizing internal engineering resources to focus on implementing compliance can be a challenge. Is your organization equipped and prepared to invest the appropriate internal resources?

- **Will your technology scale along with your software?**

  Organizations grow and change. Compliance technology should scale right along with your organization. If your organization builds software to manage privacy compliance, how will that software be incorporated into future projects and business initiatives? Would your homegrown technology be able to scale as necessary over time?

- **What is the ROI?**

  A CTO trying to decide whether to develop compliance technology in-house or work with an external provider may view this challenge from a "return on investment" angle. Most IT budgets are roughly 5% of the overall company budget and at any given moment, certain projects are prioritized over others. An accounting of the effort involved for compliance should take place before any IT work is done. Don't forget that any compliance implementation project also requires extensive testing as well as maintenance work and resources, as well.

- **How well do does your privacy team liaise with your engineers?**

  Data Privacy Officers have an intimate knowledge of their organization's compliance needs, but chances are your organization's engineers do not. How challenging were gathering requirements for and having your IT teams implement previous privacy technology projects?

Questions Worth Asking

Implementing GDPR compliance can be challenging. If you've decided to review external technology providers, choosing the best compliance automation service can be doubly so. When working with an external company to operationalize GDPR compliance, there are some features that will separate one service from the others. Here are a few questions you might ask when assessing external services.

How do data subjects interact with the service?

Under the GDPR, data subjects must be able to exercise various rights with respect to their consent choices. You'll want to make sure data subjects can easily exercise those privacy rights in a straightforward and secure manner. PrivacyCheq's ConsentCheq Dashboard gives you an out-of-the-box solution to empower customers to manage their own consent choices on any platform and in various languages. When looking any external GDPR consent management solution, we encourage you to consider the ease of use from the perspective of the data subject.

How do I administer the service?

Unless you want to always be on the phone with a customer "ninja" or "jedi" or constantly be updating and sending Excel spreadsheets, you'll want some sort of online dashboard to automate many of the administrative tasks associated with compliance technology. Does the dashboard for your chosen service include analytics to track how your customers are using the tool and progressing through the consent lifecycle? Can you track how many unique devices are making requests? Are you easily able to export an auditable and updated consent log to prove to supervisory authorities that your organization was processing data subjects' data appropriately?

How reliable is the service?

Any time your organization is going to process a data subject's personal data, your organization should find out the real-time status of a data subject's consent. This could mean that queries are made frequently depending on the nature of your organization's business. How many requests can this service handle? What sort of hardware does the service run on? Can more resources be added so that it can scale up smoothly if the rate of queries increases?

How easy is it to integrate the service?

Whatever choice your organization makes, an external compliance service should be simple and straightforward for your company to integrate and obviously save internal resources time and energy compared to developing a solution internally. Organizations should have few technical troubles understanding how to use a quality compliance technology to record and confirm a data subjects' consent to processing and integrating it with company websites and apps.

Is this technology approved by the EU-U.S. Privacy Shield Framework?

The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. If you are a U.S. company doing business both inside and outside of the European Union, you'll need to make sure that your operationalization technologies are compliant with the Privacy Shield Framework.

How does your compliance service integrate with mobile apps?

For many organizations, it is critical for a compliance technology to work seamlessly across both web and mobile platforms. What steps would you need to include a service in a mobile app or game that are different from a Website? Will a service scale across apps and websites across a variety of device sizes? How would any maintenance websites look on a mobile device or tablet?

Are there mechanisms within the service to handle parental consent to collect personal data from children?

Obtaining a parent's consent to collect personal data about a child is a daunting task. To do so, your organization will need to identify children, identify and verify a responsible adult for the child, and collect that adult's consent in order to process a child's personal data. Does the service you're evaluating give you the capability to manage parental consent? Does the service have any provisions for easing the burden of integrating an existing user base? Are any analytics available from the service that could help developers get a sense of how much friction these user flows may add?

May I see your developer documents?

Be wary of compliance automation services that don't want to share their technical documentation with you. Often, these "technologies" are aimed at providing a steady stream of consulting hours for their developers. Instead, have your IT department ask for and review the technical documentation for any service. This request can save your organization considerable time and money in the long run.

Getting Started

Taking the first step toward operationalization is always the hardest. Here are some tips on how to get started making your operation compliant.

How should you decide with your CTO how to operationalize GDPR?

Once the vendor assessment has been done, there will come a point where the Chief Technology Officer of your organization will need to be involved, whether you decide to work with a service provider or not. Perhaps the best way to approach operationalization is to describe where the modifications in the current technology framework will change with a prototype or model of a fully compliant operation. You could meet with your organization's CTO and build prototypes internally, or consider working with a compliance service to build an early prototype. Compliance-as-a-service technologies should come with documentation, sample code, and working models to efficiently describe what needs to be done by the IT department. Later, once the CTO can grasp the scope of the project they may decide to accept the help of a compliance service and re-purpose portions of a prototype rather than build everything by scratch themselves.

What reporting should be automated for your GDPR program?

Reporting needs of your GDPR compliance program will vary depend on the stakeholders within your organization. Depending on the stakeholder, consider developing the following types of automated reports:

- **IT Department**

  Technologists should have reports that track how many data subjects are viewing privacy policies and altering their consent choices. It is important for them to make sure that the operationalization program they've put in place is minimizing friction for your organization's customers.

- **C-Suite**

  Reports to the C-level executives of the company should be brief and demonstrate the level of compliance with the GDPR. They should show how much personal data the organization controls and that unused personal data is being regularly destroyed. These reports should demonstrate how many data subjects have exercised their rights under the regulation, how they have exercised their rights, and how these choices change over time.

- **Data Privacy Officer**

  Data privacy officers and their privacy teams should have access to the most detailed data and have the ability to readily access to the data itself in case a data subject asks to exercise their rights through an unusual channel such as through the mail or through social media. The DPO

should be informed about any unusual activity that could indicate a breach or that the operationalization has failed in any way and opened the organization to litigation risk or possible penalty by a supervisory authority.

What might "Phase 1" of operationalization look like?

- **Locate and identify all the personal data your organization processes**

  The first step in getting consent to process personal data is identifying where your organization may be storing data subjects' personal data and what data is stored.

- **Decide where to store proof of data subjects' notice and consent**

  Recording a data subjects' explicit consent for later is fairly straightforward. Make sure to also record the date and time that this consent was given as well as a record of which version of your organization's privacy notice data subjects agreed to. For added measure, your organization may also want to record whether they chose to view the notice and how much time they spent on the page reading it. Once the first phase of your operationalization is complete, consider drafting a "layered" privacy policy with varying levels of detail to comply with the GDPR's requirements in **Article 12** that notice be "explicit," "intelligible," "concise," and "transparent."

- **Give data subjects the ability to manage their consent choices**

  Article 7 of the GDPR states that data subjects should be able to revoke their consent just as easily as they give consent. Whether that consent may be revoked by clicking a link in an e-mail message, pushing a button on the companion app of an IoT device, or within a mobile app, this process should be simple and straightforward for data subjects. The data subject should be able to prove their identity, perhaps by logging onto a portal, and then clicking a button or selecting from a dropdown menu to update their consent wishes. Although providing an alias for a privacy team's email address or phone number may work in the short term, be sure to consider how your organization will to handle requests to exercise all rights provided by the GDPR such as the "Right to Rectification," the "Right to Be Informed," and the "Right to Be Forgotten."

- **Create a service to test against that consent**

  Just recording a data subject's consent isn't sufficient under the GDPR. Data controllers need to also be able to check that consent status each time they process a data subject's personal data. In later phases, consider any of your organization's vendors who might have access to personal data and how they will check against a data subjects' consent before processing.

- **Provide a reporting mechanism**

In case an executive has a question about the state of compliance operationalization, or a supervisory authority requests proof that your organization processed personal data appropriately, your organization should have some means to easily create logs and reports.

Conclusion

Operationalizing GDPR compliance requires privacy and IT teams to make important decisions about how to design user flows and make compliance as seamless and frictionless as possible both with respect to data subjects and within your organization. Once you assess your internal needs, conduct a detailed review of external compliance technology providers to determine whether an external or homegrown technology solution will best fit your needs.