DATA PROTECTION INSIGHTS · 6 MIN READ

5 Steps to Comprehensive Privacy Compliance

RYAN SPLAIN · NOVEMBER 23, 2021

While universally desired by individuals and enterprises alike, true privacy is nearly unobtainable. On a conceptual level, adhering to privacy may appear straightforward, but the logistical and technological challenges getting there are daunting. To holistically incorporate privacy into an organization, one has to take stock of the challenges that have historically impeded compliance efforts and continuously re-evaluate privacy strategies.

Roadblocks to compliance

Privacy requirements stipulated by the European Union's General Data Protection Regulation (GDPR) are antithetical to how enterprises have traditionally managed data. For decades, data governance has resided in a limited state of managing official corporate records while relegating the bulk of enterprise data to the dark.

In contrast, privacy regulations mandate that organizations remediate sensitive information wherever it resides, in whatever form—requiring a high degree of data control that organizations rarely have.

To find personally identifiable information (PII), enterprises have to explore all their data in place, not just within the confounds of their existing governance framework. A large share of PII resides in employee-created data sources, such as emails, files, and collaboration platforms, that have long been an unchartered corporate dumping ground. In essence, GDPR compliance requires a complete revamp of enterprise data governance, shedding light on all dark data and wrangling control over it at the source.

Early privacy initiatives

With the technical aspects of compliance out of reach, the majority of early privacy initiatives were focused on front-end work: privacy policies, user agreements, and procedures. These endeavors gave the illusion of compliance without providing the core capabilities, and any additional privacy requirements were often met with one-off, patchwork solutions.

A new privacy era, ushered in by recent GDPR violations that demonstrate the severity of non-compliance, is shifting the focus back to the technological infrastructure. No longer are regulators satisfied by surface-level controls and goodwill gestures, leaving organizations scrambling to establish the data governance required for compliance. To assist with compliance efforts, here are five steps to starting the privacy journey.

Step 1: Gather stakeholders

GDPR compliance is daunting, and no one individual or department can achieve it alone. By forming a privacy council and divvying up responsibilities into manageable chunks, organizations can ease the burden of compliance. Notable stakeholders to include in a privacy council are

- Legal and compliance: There is no one better to guide an organization through the ins and outs of GDPR compliance than legal professionals, and they continue to play a crucial role in ensuring that all measures meet regulatory standards.
- IT/IS: Most GDPR obligations require control over data; it is up to IT departments to be capable of finding, managing, and remediating PII.
- HR: Non-compliant acts often originate from accidental employee actions, and it is HR's responsibility to educate employees and set policies to limit the unnecessary collection of PII. For example, limiting personal use on work devices can drastically reduce the amount of sensitive information a company ingests.
- Project Management: Companies are not only held responsible for their own actions, but also for the vendors with whom they share sensitive information. It often falls on project managers to ensure that all data processors and applications also facilitate GDPR compliance.

Collectively, the committee should have a complete understanding of how sensitive information is collected, managed, and used throughout the enterprise.

Steps 2: Assess existing capabilities

To assess whether the organization has the capability to meet GDPR's requirements, organizations should ask themselves a series of questions regarding their existing data collection, security, and control practices.

Data collection

GDPR provides users the right to be informed about what sensitive information is collected and how it is used. For a company to properly disclose this information, it requires a solid understanding of

- What user information is being actively and passively collected?
- How PII is being used, and what is its journey from ingestion to deletion?
- How are data processors using the information shared with them?

Data security

Once ingested, GDPR requires organizations handle PII with a high degree of data security. To assess whether your organization can sufficiently meet these requirements, organizations need to know

- Is enterprise data—especially PII—encrypted in transit and rest?
- Is there data loss protection, such as high data redundancy, to recover information that is accidentally destroyed?
- Would the system recognize if it has been breached and information was leaked?

Data control

GDPR gives users a host of remediation options they can request an organization take: PII deletion, rectification, portability, and restricted processing and collection. To complete these remediation requests, organizations need to know if they can:

- Find PII across data sources?
- Send this information to the user?
- Delete user data?
- Correct false information?
- Selectively stop collecting information from specific users?
- Restrict processing on already ingested PII?

Step 3: Bridge the gaps with technology

If, while going through this checklist, the privacy council determines that it is capable of answering all these questions and meeting GDPR requirements without assistance, great! Go ahead to steps four and five.

However, if these questions pose challenges, companies will have to bridge the gap with technology. For example, the company may require a governance solution to assist in data control, a protection solution to increase data security, or new expert hires to increase internal manpower when conducting in-house efforts.

Step 4: Create a privacy heat map

Once equipped with the right tools and capabilities, organizations can begin the compliance process by locating PII. While PII is scattered across the enterprise, some data sources are prone to containing more sensitive information than others. Notably, textual, unstructured data sources, such as emails, files, and collaboration platforms, tend to have far more PII than their structured counterparts. Organizations should start by mapping out these data sources and creating a privacy heat map that highlights areas with the most unmanaged PII.

To create a privacy heat map, organizations need a systematic means of isolating PII as it enters the system. This tends to require analysis into documents' metadata and content as it is ingested. For example, pattern recognition can notice that any 3-2-4-digit sequence is a social security number, and a 2-2-4-digit sequence is a birthday. However, it is not enough to simply identify PII. Compliance requires organizations know who the PII belongs to were they to request remediation actions, typically ascertained and retrieved through ad hoc searches. Only once sensitive data has been identified can organizations start the active work of compliance: remediation.

Step 5: Establish the technological infrastructure

To remediate PII, organizations have to sift through documents and sort between the more inconsequential data they can delete and the records they must preserve. While destroying all documents with PII would be the quickest way to achieve GDPR compliance, there are countless instances where PII is integral to operations. That said, the vast majority of sensitive information resides in redundant, obsolete, and trivial (ROT) data that can be defensibly discarded. The good news is that the data control required to isolate PII can also be used to identify ROT, easing the deletion process.

For the PII that must be maintained, organizations are responsible for governing it. Accordingly, organizations have to apply lifecycle and security policies to ensure that their data is safely retained and deleted in a timely manner. When determining how to preserve sensitive records, look to the user privacy agreement as a beacon

to guide all compliance actions. In fact, deviating from that agreement is one of the most frequent causes of penalty.

> #Privacy compliance requires a complete revamp of enterprise #datagovernance, shedding light on all dark data and wrangling control over it at the source. #respectdata
>
> Click to Tweet

Remain accountable

Information is one of the most powerful weapons known to man, in the wrong hands it can be easily wielded to coerce, exploit, and subjugate both users and organizations. As legislators continue to wake up to the world of data stored in corporate servers and the ways that information can be exploited, more privacy regulations are bound to crop up. GDPR may have been the first major call for data privacy, but it will not be the last, nor the most stringent. It is up to organizations to explore their dark data and establish control—before it is too late.

TAGS #PRIVACY COMPLIANCE

Ryan Splain

Director of Global Partnerships at ZL Tech

Ryan Splain is the director of global partnerships at ZL Tech, a leader in information management. Having consulted enterprise leaders for just short of a decade, Splain works directly with Fortune 500 companies as they begin and continue their governance journeys—leveraging unstructured, human-created data for workforce analytics, compliance, and legal needs.

in