Top 10 Operational Responses to the GDPR – Part 3: Build and maintain a data governance system

Feb 14, 2018 Save This

Rita Heimes, CIPP/E, CIPP/US, CIPM

In 2016, the Westin Research Center published a series of articles identifying our analysis of the top 10 operational impacts (https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/) of the European Union's General Data Protection Regulation. Now, with the May 25, 2018,GDPR implementation deadline looming, the IAPP is releasing a companion series discussing the common practical organizational responses that our members report they are undertaking in anticipation of GDPR implementation.

This third installment in the 10-part series addresses data protection governance, from appointing privacy leadership — including a data protection officer, when necessary — to developing policies and procedures for data management, and training personnel on best privacy practices. The first two installments of the series on data mapping and inventory and on identifying legitimate bases for processing can be found here (https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-2-lawful-bases-for-processing/).

Leadership

While data mapping and inventory, and establishing a lawful basis for processing, are logically the first two steps on the road to GDPR compliance, these activities require coordination among many people throughout the organization to be performed by at least one person who is both knowledgeable about the GDPR and capable of

project management. Whether that person's title is DPO or not will depend on additional analysis of the relevant GDPR provisions.

Organizations may engage (https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf) a consulting firm for data mapping and inventory assistance, and may seek legal counsel for help understanding which lawful basis applies to each processing activity. Indeed, companies can outsource even some privacy leadership functions in the form of an external DPO. But many organizations either do the work entirely in-house with their own privacy staff (https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf) or take a blended approach, with in-house privacy professionals who draw on assistance from outside experts where necessary.

Regardless, projects as important as building GDPR-compliant systems and processes do not happen without leadership.

According to the 2017 IAPP-EY Privacy Governance Report (https://iapp.org/resources/article/iapp-ey-annual-governance-report-2017/), legal training is the most common background (https://iapp.org/media/pdf/resource_center/2017-IAPP-Salary-Survey-FINAL.pdf) for a privacy lead. The most common corporate rank for a privacy leader is "manager," although many are more senior with a title of "director," "associate general counsel," or even — 7 percent of the time — "Chief Privacy Officer." According to the report, moreover, three out of 10 organizations have promoted their privacy leader within the organization due to GDPR compliance concerns. Privacy leaders also earn, on average, nearly U.S. $130,000 annually, and as much as $170,000 for those whose title is chief privacy officer.

The DPO

Although not all privacy leaders serve in the role of DPO, most professionals with DPO responsibilities — 74 percent (https://iapp.org/media/pdf/resource_center/2017-IAPP-Salary-Survey-FINAL.pdf) — serve as their employer's privacy lead.

Article 37 (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A37) of the GDPR requires certain organizations to appoint a DPO. Much has already been written (https://iapp.org/resources/topics/eu-gdpr/#the-mandatory-dpo) about the DPO role, and the IAPP's Resource Center has a DPO toolkit (https://iapp.org/resources/topics/dpo-toolkit/), job description (https://iapp.org/resources/article/dpo-job-description/), and other information to help organizations and their DPO understand and manage the position. According to IAPP research, this mandatory role will lead to the creation of at least 75,000 new DPO (https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/) appointments globally.

In short, an organization must designate a DPO when one of the following is true:

- It is a public authority or body.
- It conducts regular and systematic monitoring of data subjects on a large scale.
- Its core activities consist of processing on a large scale of special categories (https://iapp.org/resources/article/the-eu-

general-data-protection-regulation/#A9) of data or of personal data relating to criminal cases (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A10).

- It is required to do so by member state law.

The DPO must be knowledgeable with the GDPR (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A38) and able to guide the organization's GDPR compliance. At the same time, the DPO is to serve as a point of contact for data subjects, ever vigilant to their rights and interests, and able to cooperate (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A39) with data protection authorities during investigations of consumer complaints or on routine compliance matters. DPOs must be consulted (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A38), for example, in the event of a suspected data breach, or when conducting a data protection impact assessment (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A35), the subject of the next installment in this series.

Because of the high public visibility of the DPO role, many organizations may decide to appoint one even if they can make the argument that their processing activities don't fall under the scope of Article 37. The Article 29 Working Party (https://iapp.org/media/pdf/resource_center/WP29-2017-04-DPO-Guidance.pdf) has encouraged erring on the side of appointing a DPO when in doubt. Whereas data mapping, privacy risk assessments, recordkeeping, and the like are entirely internal processes of which consumers and regulators may never be made aware, a DPO's appointment may visibly demonstrate that a company is aware of and seeking to comply with the GDPR especially if that information is shared with consumers through privacy statements and otherwise in consumer communications.

That said, because the term "DPO" has legal significance triggering obligations and responsibilities under the GDPR, some argue that the term should not be used casually (https://iapp.org/news/a/where-should-the-new-mandatory-dpo-sit/?) to refer to any privacy leader but instead only to the person who is fulfilling the unique statutory role of the DPO. This may be someone within the organization who is consulted only at specific times as set forth in the GDPR. Alternatively, the role could be outsourced (https://iapp.org/news/a/outsourcing-your-organizations-dpo-duties-consider-this/) to a firm that specializes in DPO fulfillment.

Privacy policies

Each year, privacy professionals report that their number one activity is drafting internal privacy policies (https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf) and procedures. The Privacy or Data Protection Policies set forth the organization's intentions and practices regarding the processing of personal data. They should not to be confused with the public-facing Privacy Notice (https://iapp.org/resources/topics/crafting-a-privacy-notice/) or Privacy Statement that typically lives on an organization's website for transparency purposes.

Many organizations create an overarching general privacy policy and use other documents to drill down into specific processes and procedures, such as those concerning the data of employees collected in an investigation, as these may differ from one department to the next. If the organization already has a privacy policy in place, it's best to start with it and revise it for GDPR compliance rather than begin again from scratch.

Examples of general internal privacy policies (https://iapp.org/resources/topics/organizational-privacy-policies/) are hard to come by because they are often considered proprietary, but some (https://www.daimler.com/documents/company/other/daimler-dataprotectionpolicy-en.pdf) have been posted online and can provide a place to start.

An example of an outline for a GDPR-focused privacy policy may look something like this:

- **Purpose or Privacy Mission Statement**. This is a broad-based statement of commitment to data protection and privacy principles by the organization.

- **Definitions**. Some key words to be used in the document require definition, especially if they have legal significance. Examples include: personal data, data subject, data processing, data processor and data controller, third parties and vendors, consent, profiling, special categories of data, and anonymization. Other terms may be applicable to different organizations depending on the scope of their data processing activities.

- **Responsibilities/Accountability**. Here is the place to make it clear where responsibility lies within the organization (e.g., privacy lead, DPO, chief executives, staff). This may also be a good place to prominently place the DPO's and/or privacy leader's contact information.

- **Principles for Processing Data**. Many policies use the Fair Information Practice (https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/) principles, restated in the GDPR, to organize and explain internal organizational data protection and privacy policies.

- **Reliable, Lawful and Fair Data Processing.** Here is where lawful bases (https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-lawful-bases-for-processing/) may be broadly described for different data processing activities, tracking against the data inventory and map. For example, data processing to fulfill contractual relationships, data processing pursuant to legitimate interests. consent-based processing, processing to satisfy a legal obligation, and the general category of direct marketing may be appropriate headings.

- **Transferring Data to Non-EU Countries:** This section can serve as a place to list the organization's plans for complying with Chapter V of the GDPR (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A44).

- **Data Retention**:The GDPR makes explicit that personal data should be stored no longer than necessary (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A5), unless maintained for historical, archival, research, or statistical purposes. For each processing activity and lawful basis of processing, then, a retention plan must be in place. This will likely require detail beyond the scope of the broad-based privacy policy, but reference to a detailed data retention policy and to the storage limitation principle is appropriate in a privacy policy.

- **Data Subjects' Rights**: These rights will help define data protection processing within an organization and understanding them will help employees comply with the GDPR. By outlining them in the policy, moreover, a privacy leader can help focus attention during training on these core rights: information access, rectification and supplementation, objection to processing, data erasure, objection to profiling, restriction of processing, and data portability

- **Confidentiality and Access Controls**: Akin to but slightly separate from technical security measures are principles of maintaining confidentiality of not only personal data but also other corporate information. This section encourages the organization to establish and maintain access controls to limit those within the organization who can access, modify, process, and transfer personal and confidential information.

- **Security:** Separate written security and incident response plans are crucial, but because security is a feature of privacy, it's important to mention that physical, technical and administrative security are core operational values. Here is one place to alert employees to the Chief Information Security Officer or equivalent role.

- **Data Incidents**: The privacy policy may also mention what to do in the event of a privacy incident, including a reminder to inform and consult the DPO

(https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A33), and should also point to the company's incident response plan for additional information.

- **Key Contacts (e.g., privacy leader, DPO, CISO, etc.)**. This information should appear prominently in the policy.

Of course, this high-level explanation of privacy's importance to an organization does not necessarily tell employees precisely what to do in all situations. Accordingly, more detailed guidelines may be required depending on the type of data the organization processes and the size and complexity of the organization.

Once a policy is in place, training can begin, since training to the law is not nearly as effective as training to an organizational policy.

Training

The GDPR rather subtly requires training. Under Article 39 (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A39), the DPO is obliged to monitor the organization's compliance with the GDPR, including keeping track of "awareness-raising and training of staff involved in processing operations."

Training and awareness-raising is an age-old responsibility of privacy professionals, especially privacy leadership. Nonetheless, only in last year's Privacy Governance Report did privacy professionals for the first time cite investing in training (https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf) as their number one tactic for GDPR compliance. In a separate study, they listed training staff (https://iapp.org/resources/article/getting-to-gdpr-compliance-risk-evaluation-and-strategies-for-mitigation/) on data protection and privacy as the top mitigation tool for 10 out of 11 perceived GDPR-compliance risks.

Engaging staff at least annually in privacy training (https://iapp.org/train/make-your-case/) can help reduce the risk of data breach, enhance consumer trust through more overt attention to privacy company-wide, increase the likelihood that new data processing activities — including the use of new technical tools — are brought to the DPO's attention in a timely manner for risk assessment and record keeping, and enhance the potential for privacy by design and default (https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A25) in new products, services, and systems.

For many privacy professionals, translating the GDPR (https://iapp.org/news/a/explaining-the-gdpr-to-an-american/) into human-readable language is a tall order — especially for U.S. privacy professionals, who cited the law's complexity (https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf) as the top reason for not complying by the May 25 deadline. A good privacy policy can launch training off on the right foot, however, and, regardless of friction, training employees to understand the vocabulary and main requirements of the GDPR is a task that must be accomplished as part of any compliance program.

Conclusion

GDPR compliance – like any privacy program – will not happen without privacy leadership, appropriate internal policies, and data protection training and awareness throughout the enterprise. Privacy professionals have long known that these tasks are core to sound data governance and to privacy "on the ground (https://iapp.org/news/a/digging-deeper-into-privacy-on-the-ground/)." GDPR's expansive scope and complex language merely makes these responsibilities explicit for many organizations.

photo credit: Stuck in Customs Supplies For The Long Winter (http://www.flickr.com/photos/95572727@N00/27476816714) via photopin (http://photopin.com) (license) (https://creativecommons.org/licenses/by-nc-sa/2.0/)

Author

Rita Heimes, CIPP/E, CIPP/US, CIPM

Share This

Tags

EU (/tag/eu) Privacy Law (/tag/privacy-law)

Security Operations Management (/tag/security-operations-management)

Pease International Tradeport, 75 Rochester Ave, Suite 4
Portsmouth, NH 03801 USA • +1 603.427.9200