ROPES & GRAY

ARTICLE

Privacy & Cybersecurity

May 26, 2017

Countdown to compliance: one year to go until GDPR enforcement

Attorneys
Rohan Massey
Heather Sussman
Clare Sellars
Michelle Feldman
Jim Degraw
Doug Meal
Mark Szpak
Seth Harrington
Michelle Visser

This article by partners Rohan Massey and Heather Sussman, counsel Clare Sellars, associate Michelle Feldman and partners Jim Degraw, Doug Meal, Mark Szpak, Seth Harrington and Michelle Visser was published by Law360 on May 26, 2017.

The General Data Protection Regulation (GDPR) is a sweeping privacy and data protection regulation in the European Union (EU) and will be enforced from May 25, 2018, replacing Data Protection Directive 95/46/EC. The GDPR aims to protect both individuals' fundamental rights to protection of data about them and the free flow of such personal data, as well as to harmonize the existing patchwork of EU member state implementations of the Directive. In doing so, the GDPR significantly expands the application of EU data protection law.

The GDPR imposes significant new obligations on organizations that control or process relevant personal data and introduces new rights and protections for EU data subjects. In addition, the GDPR has extended the territorial scope of the EU data protection regime beyond EU based businesses. For example, many organizations who may not have been covered by the Directive previously because they do not have operations in the EU will now be covered by the GDPR by virtue of offering goods and services into the region, or monitoring the behavior of EU based citizens.

Data controllers are organizations that determine the purposes and means of processing personal data, making key decisions about the scope and nature of the processing. Data processors are organizations that handle personal data and carry out technical operations on behalf of data controllers and in accordance with their instructions. Whereas the Directive imposed obligations only on data controllers, under the GDPR, data processors will also be required to comply with certain data protection requirements, including those related to cross-border transfers of personal data, security, appointment of data privacy officers, and recordkeeping of processing activities.

In order to effectively safeguard individuals' data protection rights, the GDPR is "technologically neutral": it governs the processing of personal data by both automated and manual means if the personal data is part of, or is intended to form part of, a filing system—a structured set of personal data that is organized according to specific criteria. The GDPR removes the Data Protection Directive's obligation to report all data processing activities to Data Protection Authorities, which costs businesses around 130 million euros per year. However, controllers now bear the burden of proof for demonstrating that they have procedures in place for dealing with their obligations to data subjects. The GDPR's new recordkeeping requirements are substantial and not something that many organizations currently have in place – for example, the law requires keeping an up to date inventory of personal data processing activities.

The requirements of the GDPR are driven by the following guiding principles for the collection and use of personal data:

- Lawfulness, Fairness, and Transparency – Data must be collected in a lawful, fair, and transparent manner.
- Purpose Limitation – Data can only be collected for specified purposes, and cannot be used in a manner incompatible with those purposes.

- Data Minimization – The amount of data collected must be limited to data that is relevant to, and necessary for, the purpose for which it was collected.
- Accuracy – Efforts must be made to ensure data accuracy and allow for correction of inaccurate data.
- Storage Limitation – Data must not be stored in an identifiable form for longer than necessary to accomplish the purpose for which it was collected.
- Integrity and Confidentiality – Data must be processed in a manner that ensures appropriate security and protects against loss or compromise.
- Accountability – Data controllers are responsible for, and must be able to demonstrate, compliance with the above principles.

This last principle—accountability—is not a new concept in the world of data protection, but is now a formalized requirement under the GDPR. The GDPR lays out a two-pronged approach to compliance with the accountability principle. First, a data controller must ensure that appropriate data protection policies are implemented, executed, and embedded into its corporate structure. These policies and procedures must align with and further the data protection rights and freedoms outlined under the GDPR. Second, a data controller must be able to demonstrate compliance with its internal policies and procedures for the protection of personal data.

Accountability therefore requires that data controllers create and maintain a corporate culture that emphasizes data privacy and security by establishing reliable data protection governance. Complying with the accountability principles will reduce data controllers' risks of suffering potential data breach incidents, bolster individuals' trust in controllers and reduce the likelihood of financial penalties.

What is at stake?

The GDPR establishes an extensive enforcement regime. In comparison to the Directive, the GDPR creates the potential for increased invasive investigations and substantial economic consequences for potential violations. The GDPR grants Supervisory Authorities (SAs) extensive powers and responsibilities, which include broad investigative and corrective powers.

SAs are empowered to impose significant administrative fines on both data controllers and processors that violate the GDPR. For the most serious violations, including those relating to the guiding principles discussed above, obtaining consent, data subject rights, and cross-border data transfers, organizations may face fines of up to 4% of the global annual turnover of the preceding financial year or 20,000,000 EUR, whichever is greater. Unlike the current system, the fines may be calculated using turnover values across a group of linked organizations rather than just that of the non-compliant organization. In determining whether to issue a fine and the amount of any fine, SAs will consider the nature, gravity, and duration of the violation, the type of personal data affected, whether the violation was intentional, remedial measures, previous violations, whether the controller or processor voluntarily reported the violation to the appropriate SA, cooperation with the SA, and any other aggravating or mitigating factors.

Individuals may lodge a complaint with an SA if they believe a data controller or processor has violated their rights under the GDPR. Most notably, the GDPR empowers individuals to seek judicial remedies against data controllers or processors and to recoup compensation for financial or emotional damage that they suffer as a result of GDPR violations. Consumer bodies may also lodge complaints with SAs, seek judicial remedies, and demand compensation from data controllers or processors on behalf of data subjects.

Evaluating your current state and planning your roadmap to compliance

With so much on the line, data controllers and processors will want to take immediate action to prepare for enforcement of the GDPR. The first step is determining whether the GDPR applies to your organization. You can do this by:

- Designating a GDPR compliance team comprising stakeholders from key business units within the organization.
- Mapping your organization's current data handling practices to create an inventory of the types, locations and flows of personal data, and maintaining this data map as a living document to be used as a reference, guidance, and reporting tool. Third-party vendors and software tools specializing in data mapping may be helpful.
- Reviewing your organization's current data handling activities to determine whether they fall within the scope of the GDPR, taking into account the breadth of the definitions in the GDPR.

Next, you can determine how the GDPR applies to your organization and plan a roadmap to compliance that fits your organization's needs. Does your organization function as a data controller or processor, or both? While both data controllers and data processors are now directly subject to the GDPR, there are differences in how each type of organization is required to comply. In general, if your organization is a data controller or processor subject to the GDPR, potential next steps could include:

- Engaging the participation and support of your board of directors, as well as C-level or other senior management, which will be necessary for implementation of a compliance program and will help demonstrate commitment to privacy and accountability to external stakeholders.
- Carefully reviewing your new legal obligations under the GDPR and conducting a gap assessment by reviewing any existing data protection programs. Consider engaging a vendor to conduct the gap assessment in a manner that maximizes privilege protection for the relevant documentation.
- Setting a budget and allocating resources to address the weaknesses identified by the gap assessment and areas of non-compliance with the GDPR.
- Assessing your current liability arrangements and insurance coverage. This can help to reduce heightened regulatory and litigation exposure once the GDPR goes into effect.
- Identifying your Member State of main establishment, which is important under the GDPR because it determines which SA will have the lead in regulating your organization's GDPR compliance. Note that the definition of main establishment differs based on whether your organization is a data controller or processor. Once identified, the business can familiarize itself with its lead SA's typical policies on data protection enforcement, and can implement processes and procedures for dealing with supervisory authorities, potentially in multiple EU Member States.

Follow your roadmap to compliance

Evaluating your current state of compliance and formulating your roadmap lay the groundwork for your organization's compliance program. After assessments, potential next steps for compliance include:

- Develop a governance structure. This includes designing a responsibility structure that fits your existing organization, determining whether to appoint a data protection officer, and, for organizations not established in the EU, appointing a representative in the EU that can act on the organization's behalf on all issues relating to processing.
- Update internally facing policies and procedures. This includes implementing data protection by design and default, satisfying new, more stringent requirements regarding consent and recordkeeping, and conducting data protection impact assessments when developing and using data in a manner likely to create a substantial risk to the rights and freedoms of individuals.
- Implement mechanisms to accommodate data subject rights. The law requires that controllers provide data subjects with information notices regarding the processing of collected personal data, any profiling and following certain data breaches. Controllers must also respond to requests relating to data subject rights under the GDPR, including the rights of access, rectification, objection to processing, restriction on processing, data portability, and erasure or 'the right to be forgotten', among others. These new obligations require the creation of new processes and technical mechanisms to accommodate requests, identify data associated with a data subject request and interface with data subjects.
- Closely manage vendors. Data controllers will want to perform due diligence in respect of its relevant processors and other vendors with access to EU personal data to ensure that there are "sufficient guarantees" that such third parties' technical and organizational processing measures satisfy the requirements of the GDPR and ensure the protection of the rights of the data subject. Existing contracts can then be reviewed to ensure the specific requirements set forth in the GDPR are met. Careful negotiation of liabilities is crucial given that data subjects may seek compensation for GDPR violations from either controllers or processors. Companies may want to develop a standard form addendum for new vendor agreements and consider how to add these new clauses without renegotiating existing provisions, particularly for contracts that will persist in duration beyond the compliance deadline.
- Restrict international data transfers. Transfers of personal data to a third country or international organization outside the EU can only take place if the safeguards set forth by the GDPR are in place. While this was true under the Directive, the list of acceptable safeguards has changed and, as this area of the law is still evolving, data controllers and processors will want to evaluate any existing mechanisms to be sure they continue to serve the intended purpose.
- Implement appropriate data security and incident response measures. Data controllers and processors are required to implement and be capable of demonstrating appropriate and effective technical and organizational security measures to protect personal data they process. These measures must be tailored to the nature and scope of the data collected and therefore reviewed and updated as necessary. The GDPR also imposes an obligation on data controllers to disclose the occurrence of certain personal data breaches to the supervisory authority within 72 hours, therefore organizations must be prepared to respond.
- Abide by seals, certifications, and codes of conduct. The GDPR strongly encourages approved codes of conduct and certifications for the purposes of guiding data controllers and processors on GDPR requirements.
- Set up an ongoing monitoring program. Organizations may want to put in place a mechanism to track regulatory developments and guidance, interpretative decisions, and local requirements relating to the many areas of the GDPR reserved to Member States. Remember that May 2018 is only the beginning of the GDPR.

Conclusion

Compliance with law is not the only, or even the primary, benefit of embracing the principles that underlie the GDPR—reducing the risk of data breaches and developing a reputation for sound data handling practices is good for business. The increased sanctions under the GDPR incentivize compliance with all its aspects, but taking accountability seriously in particular can both help prevent breaches and possibly work to reduce sanctions if an organization can demonstrate the efforts it has taken to protect data.

In addition, the principle of accountability provides an opportunity for organizations to bolster individuals' trust in them by showcasing their robust data protection efforts and for demonstrating transparency and corporate responsibility. Responsible information handling practices can attract customers, investors, and talent. Rather than simply doing the minimum necessary to meet high-risk legal requirements, companies are increasingly leveraging the resources they dedicate to compliance and building out their corporate responsibility programs, integrating these programs into their business strategies, and marketing them as a competitive advantage.