DAVIS GILBERT

T Minus 1 Year Until GDPR: Are You Ready for Take Off?

The Bottom Line

- *It remains to be seen what will happen after the GDPR becomes effective on May 25, 2018. The GDPR compliance roadmap can be helpful for any organization that collects or processes personal data, whether or not an organization in or outside of the EU believes it is subject to the GDPR.*
- *With just one year of the two-year implementation period left, organizations should be well on their way to preparing for the impact of the new regulation.*

The adoption of the European Union (EU) General Data Protection Regulation (GDPR) in April 2016 was one of the biggest changes in European privacy law in decades. It promises significant changes to the way organizations are expected to collect and use information. Further, the extra-territorial reach of the GDPR means organizations outside of the EU may be affected. With the threat of penalties of up to 4% of annual worldwide turnover or €20 million, organizations should take a serious look at their data collection and use practices to ensure compliance with the GDPR before it comes into effect on May 25, 2018.

Reaching Beyond The EU Borders

One of the most significant changes in the regulation is that the GDPR transcends the geographical borders of the EU. In particular, the GDPR applies to the processing of personal data of data subjects who are in the EU, including by organizations that are not established in the EU, provided the data processing is related to either:

- the offering of goods and services to the EU data subjects (including both free and paid goods and services), or
- the monitoring of their behavior in the EU (including tracking data subjects online for interest-based marketing).

In effect, *any* company that meets these criteria may be subject to the GDPR. The narrower "long arm" reach of the GDPR's predecessor, the EU Data Protection Directive 95/46/EC (the Directive), only applied to controllers that used processing equipment located in the EU and will no longer apply. Under the GDPR, many non-EU entities, including those that merely act as a processor at the instruction of, as agent for, or on behalf of a controller in the EU, are not beyond the reach of the GDPR.

Of particular note is the applicability of the GDPR to companies engaging in the "monitoring of the behavior of data subjects" – a concept which the Article 29 Working Party has confirmed includes all forms of tracking and profiling on the Internet, including for the purposes of behavioral advertising. Accordingly, all companies engaging in behavioral advertising or other tracking, and/or profiling activities, need to carefully consider the impact of the GDPR on their business.

Designating a Data Protection Officer

Another major change under the GDPR is the requirement that certain controllers and processors designate a data protection officer who has expert knowledge of data protection laws and practices and can help ensure their organization's compliance with the GDPR. The GDPR charges data protection officers with a number of obligations, including:

- advising their colleagues,
- monitoring his or her organization's compliance with applicable privacy laws (including by providing training, raising awareness and conducting audits),
- advising on privacy impact assessments,
- cooperating with supervisory authorities, and
- responding to inquiries from data subjects.

The requirement to designate a data protection officer applies to organizations whose "core activities" (key operations necessary to achieve the controller's or processor's goals) involve "regular and systematic monitoring of data subjects on a large scale" (such as online tracking and profiling) or where the entity conducts "large-scale processing of special categories of personal data" (e.g., voluminous processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs).

Core Rules Remain, But New Details Hold Significant Impact

The GDPR preserves many of the core rules of the Directive, but updates and additions to these rules will have a significant impact on how entities process personal data. Under the GDPR, all processing must comply with all six general principles and satisfy at least one processing condition.

The six general principles are:

1. Personal data should be processed in a lawful, fair and transparent manner.
2. Personal data can only be processed in connection with specified and legitimate purposes.
3. Personal data should be limited and relevant to the processing purpose.
4. Personal data should be accurate and kept up-to-date.
5. Personal data should only be retained for as long as it's needed and should be deleted after it fulfills its purpose.
6. Personal data must be kept confidential and secure, and its integrity preserved.

Under the GDPR, some of the processing conditions have been enhanced and will be quite burdensome to satisfy. Consent is one example.

Valid consent under the GDPR requires that:

- consent must be freely (i.e., no detriment if consent is refused or withdrawn) and affirmatively given (i.e., no pre-checked boxes) for each processing activity,
- the request must be in plain language,

- consent cannot be bundled with other requests,
- consent is not conditional,
- there is no power imbalance between the individual and the consent-seeker (i.e., such as an employer-employee relationship), and
- the consent can be withdrawn at any time

Consent that has been obtained prior to the GDPR's effective date may be valid if all of the above requirements were met.

It's also important to note that while many of the Directive's definitions, including "personal data," remain the same under the GDPR, "sensitive personal data" has two new additions: genetic and biometric data. Information about criminal convictions and offenses is also carved out and treated separately with more restrictive controls.

Methods of Data Transfers

Under the GDPR, the core methods of data transfers also remain the same, such as standard contractual clauses, consent, binding corporate rules, transferring to a country that has privacy laws deemed adequate by the EU, and with respect to the United States, transferring the data to an entity registered with the EU-U.S. Privacy Shield Framework.

The GDPR adds two more methods. One method allows data transfers to inadequate jurisdictions if the importer has signed up to a GDPR approved code of conduct or certification scheme. The other new method is really an exemption that allows for one-time minor transfers that only affect a limited number of data subjects, where the risks have been assessed, safeguards applied and the supervisory authority and data subjects are informed of the minor transfer. The transfer can be done provided there is a compelling interest that is greater than the individual's privacy interest.

Increased Data Subject Rights

In addition to their existing rights under the Directive, data subjects under the GDPR will have additional rights, such as the right to be forgotten, the right to restrict processing, the right to object and the right to data portability.

The right to be forgotten (also known as the right to erasure) is an individual's right to have personal data erased or to prevent processing in specific circumstances. Note that children are given an enhanced right to erasure under the GDPR and there are extra requirements when the request for erasure relates to a child's personal data.

The right to restrict processing allows individuals to have a right to block or suppress processing of personal data under certain circumstances. If an entity receives a suppression or restriction request but personal data has already been disclosed to third parties, the entity has an obligation to inform the third party about the restriction on processing.

The right to object allows individuals to object to certain types of processing, including direct marketing, profiling and providing for purposes of scientific or historical research and statistics.

The right to data portability allows individuals to move, copy or transfer personal data from one place to another in a secure manner without interrupting the integrity and usability of the information.

Mandatory Breach Notification

Unlike the Directive, the GDPR provides a definition of "personal data breach" and requires that data controllers notify the relevant supervisory authority of a breach within 72 hours of discovery or provide reasoned justification for a delay. It also sets out the required content of the notification and exceptions to notification. Under the GDPR, entities may also have to report breaches to an individual in some cases.

Consequences of Noncompliance

Supervisory authorities under the GDPR have the power to impose fines on noncomplying entities. Sanctions can total up to the greater of €20 million or 4% of the entity's annual worldwide turnover. These fines apply to the noncompliance of most GDPR provisions, including failure to comply with the six general principles or inadequate consent for processing. There is a less onerous second tier of sanctions that apply to certain noncomplying activities that can result in sanctions of up to the greater of €10 million or 2% of the entity's annual worldwide turnover. Additionally, individuals also have a right to recover damages from a controller or processor in court.

Age Of Consent – 13 or 16

While the GDPR aims for more standardization among the Member States, there will still be differences in the way the GDPR is implemented and enforced in each Member State. Member States can modify certain details of the GDPR through derogations. For instance, they can lower the age of children's consent from 16 to 13, determine whether it is mandatory to appoint a data protection officer or introduce additional restrictions on the processing of employee data.

Action Items

Organizations should be actively preparing for the GDPR in the coming year to bring their businesses into compliance. Below are some action items organizations should consider after determining they fall under the purview of the GDPR:

- Determine whether it's suitable to take steps to avoid being subject to the GDPR.
- Confirm whether the organization's existing processes to obtain consent is in line with the new GDPR requirements.
- Where applicable, appoint a data protection officer.
- Re-approach existing users to obtain GDPR-compliant consent.
- Put in place a mechanism to honor consent withdrawal requests.
- Ensure requests from data subjects exercising their rights can be processed and fulfilled.
- Update internal policies, external facing policies and vendor agreements.
- Review and/or update existing contracts to ensure that any data processing, security and compliance obligations are appropriately addressed.
- Review security and privacy programs in light of enhanced requirements.

- Follow Member State laws that may apply as their requirements may vary from the obligations under the GDPR.
- Ensure that your organization can demonstrate compliance with the GDPR. By way of example, consider taking the following steps:
  - Establish a comprehensive data protection and security program, including appropriate technical, physical, administrative and organizational measures that are consistent with the requirements of the GDPR.
  - Create and implement internal data protection policies (and any external facing policies, including online privacy notices) that are periodically reviewed, tested and updated.
  - Conduct regular internal audits of the organization's practices to ensure compliance with its policies.
  - Provide employees with regular, up-to-date training on data protection and security principles.
  - Require and document any necessary data protection impact assessments.

Related People

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com