ACCESSDATA

WHITE PAPER

The New EU General Data Protection Regulation: A Strict Legal Framework for Digital Privacy

After nearly four years of negotiations, European Union officials have finally reached agreement on a pan-European digital privacy law that, once approved by the European Parliament and EU governments, will go into effect in 2018. This new General Data Protection Regulation (GDPR) creates a strict legal framework for how companies can use personal information collected online.

This is serious business for any organisation that collects personal data in the EU. The GDPR substantially increases penalties for privacy violations to as much as 4% of a company's global revenue.

With stakes this high, it's important for corporate executives whose companies collect and store personal information within the EU to make sure they are apprised of the key elements of this new law so they are prepared to be fully compliant as soon as the GDPR takes effect.

There are a number of data management steps that should be followed, each of which is made much easier for EU companies by leading-edge software tools that can be put to work in this effort.

A GDPR Overview

The new law will replace a patchwork of 28 different sets of national privacy laws by creating a single set of rules for the protection of data within the EU. This consolidation to one national privacy regulator should lighten the administrative burden on companies as they'll be able to conduct business across the entire EU without having to monitor compliance with multiple autonomous privacy laws.

At the same time, the GDPR sets the privacy bar quite high, placing extensive limits around how businesses must treat personal data and requiring consistent privacy monitoring controls. The goal of EU regulators is to become a model for the rest of the world by creating a regulatory environment in which businesses can flourish while fiercely protecting individual privacy.

There are six key components of the GDPR that European corporate executives need to understand:

1. Broader concept of "personal data"

The definition of "personal data" has been widely expanded to include information related to a data subject's physical, physiological, genetic, mental, economic, cultural or social identity. This is going to require a rethink of most organisations' previous data privacy policies.

2. Notifications for data breaches

The GDPR establishes a uniform data breach notification requirement: in the event of a data breach leading to the loss, access or disclosure of personal data, organisations must notify regulators "without undue delay" and—unless the data is encrypted or the individuals involved will be harmed—they must do so within 72 hours.

3. Data transfer rules

Data transfer out of the EU will only be allowed if the European Commission has evaluated the level of data protection in the country where the data is being transferred and has affirmed that it is acceptable.

4. Consent rules

Under the GDPR, consent must be freely given, specific and informed. Any organisation collecting personal data must be clear that the individual providing that information is making a clear and unambiguous decision that they're entering into an agreement for the organisation to collect and process that data.

5. Data Protection Officer

If a company consistently monitors or processes sensitive personal data—regardless of where that data is processed in the world—they will have to appoint a Data Protection Officer who has appropriate data protection law expertise. The data protection officer may be employed by the company or be engaged with a service contract, but either way that professional's tasks must include advising the company on data protection issues, monitoring compliance with the GDPR and acting as the point of contact for regulators.

6. Enforcement

The GDPR gives individual consumers a private right of action in EU courts, which means they have a right to seek financial damages for any harm caused by the processing of personal data. Meanwhile, regulators have been empowered to issue opinions, adopt binding decisions and otherwise oversee data protection processes to ensure compliance by organisations. The power to assess fines is alarming—up to 4% of worldwide corporate revenues is astounding—although the GDPR makes it clear that the amount of the fine will depend on several factors such as the nature, gravity and duration of the infringement.

Data Management Steps to Prepare for GDPR

In the months leading up to the implementation of the GDPR, corporate executives will have a lengthy list of operational, staffing and cultural changes to make in order for them to be compliant with the new regulations. Those compliance steps are already being well documented and there will no doubt be many professionals rushing to assist companies with these important organisational changes.

Meanwhile, the implementation of the new regulation will also require companies to take some important actions with respect to how data is managed in their organisations. In fact, as industry experts such as Marcus Evans have noted, most businesses will need to make at least modest changes to their data processing practices to meet the requirements of the GDPR; many will have to make extensive changes to be in compliance.

There are a number of data management steps that should be followed, each of which is made much easier for EU companies by leading-edge software tools that can be put to work in this effort.

Locate the Data

Identifying electronically stored information of relevance within an enterprise is nothing new, but being confident that you understand where data is has never been more important. Therefore, searching for and locating data of relevance against a backdrop of information governance is a good place to focus. For example, it's important to understand the data within the organisation by knowing the range of data formats that contain personal information (e.g., multimedia files, metadata associated with image files, etc.). Moreover, in order to keep pace with this expanded range of data structure, search capabilities need to be advanced in order to accurately find the data that falls within the scope of the GDPR.

Define Access

One of the key attributes of the GDPR is to encourage a "high standard of protection" for personal data and for this standard to be maintained across the enterprise, which includes third parties and operations in other countries. With respect to the GDPR, these points of access are defined by their physical location, rather than virtual data locations. This includes third-party data controllers as well as third parties that are merely processors of data. It's also important to consider that the rise in mobility and mobile applications is becoming more predominant in Internet usage, so understanding and defining access requires a special consideration of mobile technology. A structured data audit plan—together with good compliance monitoring—will allow the organisation to clearly define and visualize access.

Understand the Framework

It's crucial to understand the legal framework in order to shape data management policy. The GDPR is essentially the final regulation that formalizes an earlier EU data protection directive. One key aspect of this is that the GDPR aims to introduce Binding Corporate Rules. These can be repeatedly used for the exchange and control of data across different jurisdictions within the EU and externally, enabling governance and policies to be written once and assessed within a single country of residence. For example, data must be collected in a forensically sound manner with best practices and reliable software tools. Also, in the event of a litigation review, data must be properly shared with individuals, critical staff members, attorneys and appropriate regulators.

Know the Security Risks

Any organisation that has been victimized by a data breach or other cybersecurity problem can point to at least two major security risks related to their management of personal data: liability associated with loss of that data and damage to the corporate brand as a result. When we talk about knowing the security risks, what EU companies really need to understand are the threats associated with these risks versus how their controls and measures are performing; the combination of these two factors gives the ability to quantify risk and identify areas for improvement and investment. A thorough data compliance audit is the first step toward quantifying that risk and building a proactive security culture within the business.

Assess the Future

Keeping pace and planning for the future in a world that is rapidly evolving—such as the migration to storing data in the cloud—drives a different level of interaction between executives, internal data management teams and outside service providers. An effective plan for data management under the GDPR needs to anticipate what is around the corner by considering what the future of personal data will entail. Technology is also changing rapidly, so it's important to choose IT partners very wisely and work with them to provide guidance on product roadmaps that will meet the needs of the future. Also, start data mapping as soon as possible so that flowchart can be used to guide a long-term data management strategy that is fully compliant with the GDPR.

Conclusion

The new GDPR was four long years in the making, but it appears that EU officials have now settled on the final language for a sweeping digital privacy law that will be in place in 2018. For all organisations collecting personal data online from individuals within the EU, the new legal framework will be strict and failure to comply will expose a company to draconian financial consequences.

It's important that EU corporate executives begin the important preparatory work now to make sure their companies are ready for this landmark regulation to go into effect.

ACCESSDATA®

AccessData Group has pioneered digital forensics and e-discovery software development for more than 25 years. Over that time, the company has grown to provide both stand-alone and enterprise-class solutions that can synergistically work together to enable both criminal and civil e-discovery of any kind, including digital investigations, computer forensics, legal review, compliance, auditing and information assurance. More than 130,000 customers in law enforcement, government agencies, corporations and law firms around the world rely on AccessData® software solutions, and its premier digital investigations products and services. AccessData Group is also a leading provider of digital forensics training and certification, with its AccessData Certified Examiner® (ACE®) and Mobile Phone Examiner Certification AME programs. For more information, please go to www.accessdata.com.

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com

LEARN MORE

www.AccessData.com