The Basics of GDPR

Devolutions

GDPR ALSO REGULATES THE TRANSFER OF PERSONAL CUSTOMER DATA OUTSIDE THE EU!

Last year around this time, you may recall getting a flurry of emails from various vendors like Google, Apple, and even your friends here at Devolutions, informing you about their obligations and your rights under the new General Data Protection Regulation (GDPR), which had been adopted by the European parliament in April 2016 and had come into effect in May 2018.

What's more, if you live and work outside of Europe, you may have been scratching your head and wondering if on some sign-up form you mistakenly noted that you live in Paris, France, instead of Paris, Texas; London, England, instead of London, Canada; or Perth, Scotland, instead of Perth, Australia. Rest assured that you did indeed get the right email — and this article will explain why.

What Is GDPR?

GDPR is a regulation that has been implemented across the entire EU and EEA region, and it applies to all organizations that collect, store and use personal customer data about European citizens —regardless of whether the organization itself is located in Europe or not (hence the reason you received all of those emails last year even if you don't live in Europe!). GDPR also regulates the transfer of personal customer data outside the EU.

What Data Is Governed?

GDPR governs a wide range of private customer data, such as:

- Basic information (e.g. name, address, ID number, etc.)
- Web data (e.g. IP address, RFID tags, cookies, etc.)
- Bank details
- Medical information
- Photos
- Updates on social networking sites
- Biometric data
- Racial and ethnic data
- Political opinions
- Sexual orientation

It is also important to note that GDPR makes no distinction between data that derives from a customer's work life and their personal life. For example, if a healthcare organization gleans from a customer's personal Facebook page that they have been diagnosed with diabetes, and if that information is captured and stored by the company (regardless of it being used), then such information is governed by GDPR.

In addition, organizations must be able to prove with a clear time-stamped audit trail that they received opt-in consent from customers to collect, store and use their personal data. Adding a disclaimer or assuming consent and providing customers with an opt-out is not enough.

Customer Rights

Under GDPR, citizens in Europe are granted key rights that include:

- The right to access their personal data and learn how it is being used. Upon request, this information must be provided by organizations for free and in an electronic format.
- The right to be forgotten and have their data deleted.
- The right to data portability, so they can transfer data from one organization to another.
- The right to be informed prior to having their data collected, stored and used.
- The right to have information about them corrected if it is incorrect or incomplete.
- The right to restrict their data from being processed (i.e. they can consent to having their data collected and stored by an organization, but not used).
- The right to prevent their data from being used for direct marketing purposes. This request must be ***accepted and activated upon receipt.***
- The right to be notified within 72 hours if there has been a data breach (more on this below).

Roles & Responsibilities

GDPR also mandates that organizations create and properly support various roles, including:

- A Data Controller, who is responsible for defining how customer personal data is processed. The Data Controller is also tasked with ensuring that all independent contractors comply with GDPR.
- A Data Processor, who is responsible for maintaining and processing personal customer data records. The Data Processor can also be an outsourced firm (e.g. a payroll processing vendor). However, the organization is responsible for ensuring that all third parties are compliant with GDPR.
- A Data Protection Officer, who is responsible for overseeing data security and ensuring ongoing compliance with GDPR (some public organizations are exempt from having a Data Protection Officer).

The 72-Hour Notification Rule

As noted above, one of the most stringent obligations of GDPR is the right for customers to be notified of a data breach within 72 hours. During this short window of time, organizations must do all of the following:

- Conduct a thorough investigation of the breach.
- Inform regulators of the breach.
- Inform individuals who are impacted by the breach.
- Identify what personal data has been impacted, and to what extent.
- Estimate the impact of the breach.
- Create a comprehensive containment plan.

Penalties

Penalties for failing to comply with GDPR are harsh, and can be up to 4% of annual global revenue or 20 million Euros ($22,755,000 USD), whichever is higher. It can also lead to lasting reputation damage that affects an organization's global brand.

From the Desk of Our CSO, Martin Lemay:

"How does GDPR affect information security? Well, the good news is that GDPR should not require a massive

amount of investment in additional security measures. GDPR controls can be securely integrated without any specific toolset, magic appliance or fancy technology. It is all about data hygiene. Knowing what type of data you have (data classification)and where it is (data flow) will be key factors in successfully protecting private information. To help you meet and maintain GDPR requirements faster and at a reasonable cost, leveraging privacy by design can help you integrate privacy into your information security program."

Learn More

To learn more about GDPR, we recommend the excellent articles and videos offered by CSOOnline. We also invite you to access our Privacy Policy, which includes (among other things) our processes and obligations for complying with GDPR. If you have any questions or concerns about our Privacy Policy don't hesitate to email us at privacy@devolutions.net.

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them here.