Acronis

FREQUENTLY ASKED QUESTIONS (FAQ) ABOUT GDPR

FAQ

Q: What is GDPR?

A: The European Union (EU) General Data Protection Regulation (GDPR) is a new EU law that strengthens the protection of private data belonging to EU residents. It replaces the existing patchwork of national data privacy laws with a single set of rules that are directly enforced by every EU member state.

Q: When does GDPR come into effect?

A: 25 May 2018.

Q: Does GDPR only apply to companies based in the EU?

A: The answer to this common misconception is "No." Any company that has customers in the EU and acquires or otherwise handles any of their personal data is required to comply with GDPR.

Q: What does GDPR mean by "personal data"?

A: "Personal data" refers to any information that can be used to identify a person. This goes well beyond the historical definition of personally-identifiable information to include the person's name, email address, social media posts, physical, physiological, or genetic information, medical information, location, bank details, IP address, cookies, and cultural identity.

Q: What exactly does GDPR regulate?

A: GDPR regulates the collection, storage, transfer, and/or use of all personal data – collectively known as processing – that belongs to residents of the EU. Any organization that processes the personal data of EU residents, including any tracking of their location or activities, e.g., with browser cookies, falls under the purview of the law, even if the processing organization does not physically reside within the EU.

The regulations make a distinction between "controllers" and "processors" as handlers of personal data. The organization that determines what to do with personal data and the reason for doing so is the controller. Any third party that a controller engages for any operation on personal data, e.g., a cloud storage service provider, is a processor.

Q: What effect does GDPR have on privacy rights?

A: GDPR greatly enhances the privacy rights of EU residents and imposes significant obligations to protect those rights on any business, institution or individual that handles their personal data. The new requirements that processors of personal data must honor include:

- **Data subject rights:** EU residents have greater control over their personal data, including the right to request that processors provide them copies of it, correct errors in it, and delete it entirely on request.

- **Proof of compliance:** Processors must implement adequate data security policies and procedures and keep detailed records on their data processing activities.

- **Security breach notifications:** Processors must report data breaches to their local GDPR supervisory authorities, and report severe breaches to the affected data subjects.

- **Penalties for non-compliance:** GDPR regulators can impose hefty fines on organizations caught failing to comply based on the seriousness of the breach and damages incurred.

Q: Does GDPR require personal data to stay within the EU?

A: Not exactly, but moving personal data outside of the EU (referred to as a "cross-border data transfer") while staying compliant with GDPR can be complicated. There are a few rules to consider. First, data transfers are generally allowed to any recipient country that is on the EU's list of destinations with "adequate" security, meaning its data privacy safeguards meet the EU's standards. In some cases, the entire country may not be deemed adequate, but individual territories or sectors within it may be. As of early 2018, the approved list included all EU countries, three non-EU countries that are part of the European Economic Area (Iceland, Lichtenstein and Norway), and a few additional countries and territories (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay).

Data transfers are also allowed to destinations that meet the EU standard for "Binding Corporate Rules (BCRs)". These allow certain legal entities within a corporation, and in some cases, groups of independent companies engaged in some joint economic activity, to transfer personal data. To qualify, the governing BCRs must be approved by an appropriate supervisory authority and meet the EU's consistency standards.

Other data destinations are allowed if they live up to certain "codes of conduct" and "certification schemes", usually drawn up by an industry association or one of its representative bodies, and only with the approval of GDPR regulators.

Still other data transfers are legitimate if they fall under the heading of "specific derogations", i.e., exceptions to the standard rules. Examples include any personal data transfer that:

- The data subject explicitly consents to and understands the associated risks
- The processor needs to fulfil a contractual obligation or satisfy a legal claim
- Is deemed to be in the public interest or the data subject's vital interest
- Is in the '"legitimate interests" of the data controller, as long as those interests do not supersede the rights of the data subject. The data controller must assess the circumstances of the transfer and take reasonable steps to safeguard the personal data.

In short, it's generally simpler, safer and cheaper for most companies not to move personal data outside of the EU and its short list of approved countries. Be prepared for some extra expense and work to move personal data elsewhere, and be prepared to prove to GDPR supervisory authorities everything you have done to protect it. Be sure you have good legal advice if you decide to rely on BCRs, codes of conduct, certification schemes, and/or specific derogations to justify other types of cross-border data transfers.

Q: How does GDPR affect our responses to security breaches?

A: GDPR requires both controllers and processors to deploy systems to defend against, monitor for, and report on potential security breaches, and to implement and document technology, policies and procedures to support breach prevention, detection, reporting and notification. Stricter new disclosure requirements apply to any incident that causes personal data to be accessed, transferred, altered or destroyed by unauthorized parties, whether by accident or intent.

Privacy protection incidents can be caused by technology failures (e.g., a hard drive crash), accidental human error (e.g., an IT staffer accidentally deleting or corrupting user files), or an intentional, malicious breach (e.g., a ransomware attack by cybercriminals that encrypts personal data and seeks payment for the key to unlock it).

In the most basic terms, controllers and processors must work harder to identify security incidents that affect personal data, report them to supervisory authorities within 72 hours of detection, and in cases of serious personal data damage, theft or loss, to quickly notify the affected data subjects, too.

Q: What new user rights do controllers have to support?

A: GDPR gives data subjects much more control over and visibility to controllers' use of their personal data. Controllers are obligated to satisfy user requests (at no cost to users), to know what elements of their personal data they have acquired, to provide it to them in an easily-accessible format, to correct any errors that users identify, and to erase personal data on request (the so-called "right to be forgotten").

Q: What is a Data Protection Officer, and do controllers and processors need one?

A: The Data Protection Officer (DPO) is an employee or consultant that many controllers and processors will be required to designate as owning primary responsibility for overseeing GDPR compliance. Public institutions are held to a higher standard: almost all will have to appoint a DPO. Private organizations must appoint a DPO only if they process large amounts of personal data that reveal data subjects' race or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, and/or criminal convictions.

The DPO should be a trained compliance professional with expertise in data protection law and best practices. His or her job is to notify the company's controllers, processors, and employees of their obligations under GDPR, to monitor compliance, and to serve as the liaison to the supervisory authority.

Q: What happens if we as a controller, processor or both are caught failing to comply with GDPR regulations?

A: The penalties for GDPR non-compliance are not trivial. Your local supervisory authority can assess a fine of €10M or 2% of your annual revenue, whichever is greater, for what are considered first-level offenses like failing to maintain written records, or not implementing appropriate technical and organizational measures to meet compliance goals. Fines can climb to €20M or 4% of your annual global revenue, whichever is greater, for more serious offenses like major data breaches and failure to protect personal data from theft, alteration or deletion.

Note that fines can be applied to both controllers and processors. Supervisory authorities may allocate a fine proportionally across a controller and its processors, assessing how much each share responsibility for the violation based on the steps each has taken to be GDPR-compliant.

In addition to these scary financial penalties, companies that deliberately ignore or underestimate their GDPR compliance obligations face potential lasting damage to their corporate reputations, as well as lawsuits from private individuals for "material or non-material" damage if personal data

has been breached. Those same fines and sanctions apply to third-party processors, too, if they handle personal data on behalf of another company. When you consider how data breaches have grown exponentially in recent years.

For example, consider how ransomware attacks increased from a US$800,000/ year illicit business in 2015 to a projected $8B-10B in 2018 -- the potential for non-compliance just on the breach reporting issue is enormous.

Q: The task of achieving GDPR compliance look enormous. Where do we start?

A: As a provider of data protection solutions, Acronis believes that a focus on upgrading your data storage and backup infrastructure is a good foundational step toward GDPR compliance. Being able to specify exactly where your data is stored, preventing breaches like ransomware attacks, and protecting data with strong encryption in motion and at rest are fundamental building blocks with concrete, positive impacts on your GDPR compliance posture.

But you should not rely on us for when deciding how to approach the GDPR challenge. Be sure to get qualified legal and professional advice as well.

Note that this FAQ is for informational purposes only. It is not intended to and should not be relied upon or construed as legal advice. You should not act or refrain from acting on the basis of any content in this FAQ without seeking legal or other professional advice.

Acronis

For additional information, please visit **https://www.acronis.com/en-us/gdpr/**