617-357-5233 | www.quoininc.com

Highlights of the European Union General Data Protection Regulation (GDPR)

Boston

Charlotte

Washington, D.C.

Nicaragua

186 South Street, Suite 400
Boston, Massachusetts 02111

In a nutshell…..

The regulation applies if the data controller (an organisation that collects data from EU residents), or processor (an organisation that processes data on behalf of a data controller like cloud service providers), or the data subject (person) is based in the EU. Under certain circumstances, the regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU. The regulation does not apply to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity." (Recital 18)

What does that mean?

The requirement is for "data protection by design and by default."

- Spells out the rights of the user or 'data subject.'
- The definition of 'personal data' is broad.
- Cannot be an afterthought - it has to be built in either using automation or a defined process.
- Cannot delegate adherence to a third-party like you can with PCI compliance.
- An escalating set of sanctions culminating in €20 million or up to 4% of the prior year's revenue.
- Applies to non-EU countries that have users in the EU.
- All business organizations, regardless of size, are required to comply.

What is 'Personal Data'?

From a press release issued by the European Commission:

> "Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

EVERY USE is an opt-in not out! If the use changes, the processor must get consent.

A Few Rights of the "Data Subject"

- The right to be forgotten - Data must be erased from the system (and backups) upon request.
- The right to restriction of processing - Processor keeps the data but it can't be touched without consent.
- The right to data portability - Export the data in a machine-readable format upon request.
- The right to rectification - Fix personal data upon request or allow the user to fix it themselves.
- The right to be informed with human-readable information.
- The right to access - The user should be able to see all the data you have about them.

Key Rules

(excerpted from the European Commission website)

- **Lawfulness, Fairness and Transparency** - Personal data must be processed in a lawful and transparent manner, ensuring fairness towards the individuals.
- **Purpose Limitation** - Have specific purposes for processing the data and you must indicate those purposes to individuals when collecting their personal data. You can't further use the personal data for other purposes that aren't compatible with the original purpose of collection.
- **Data Minimisation** - Collect and process only the personal data that is necessary to fulfil that purpose.
- **Accuracy** - Ensure the personal data is accurate and up-to-date, have regard to the purposes for which it's processed, and correct it if not.
- **Storage Limitation** - Ensure that personal data is stored for no longer than necessary for the purposes for which it was collected.
- **Integrity and Confidentiality** - Install appropriate technical and organisational safeguards that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology.

Questions?

Further Reading

- The official regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- A more nicely formatted version: https://gdpr-info.eu/
- A good interpretation for Software Developers: https://techblog.bozho.net/gdpr-practical-guide-developers/
- Info from the European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en