Lesson 1 | Introduction to GDPR

Updated 2020-09-21

GDPR is a newer regulation that went into effect in 2018. The regulations themselves were written in 2016 so companies had plenty of time to prepare. The goal of GDPR is to protect the personal data of European citizens.

GDPR stands for the General Data Protection Regulation. It governs the collection and use of personal data of EU citizens. It extends to all companies that collect and use EU citizen data, regardless of where those companies are from.

The regulation is extensive. 88% of companies reported having spent $1M to comply with GDPR. It has 99 articles, though most are not relevant to all employees of companies that comply with GDPR.

If we were to summarize GDPR, as a practical guide to thinking about GDPR, the following principles represent the very short version of the GDPR.

- **Transparency in data practices**. Companies need to be open and honest with the market, both in public documentation and readily available documentation when requested, about the collection and use of EU citizen data.
- **Creation and maintenance of a privacy and security program** (Security by Design and Default). Companies need to create a maintain a compliance program. If this is a new initiative for a company, it can be expensive and tedious.
- **End-user Data rights.** GDPR grants all EU citizens certain data rights, or data subject rights, including the right to data, the right to be forgotten, right to change data.
- **Breach notification.** In order to comply with GDPR, organizations must notify users of breaches within 72 hours. This is not easy. It involves policies and workflows that have been tested and are ready to activate upon detection of a breach.
- **Penalties.** GDPR penalties can be up to 4% of global revenue for an organization. GDPR fines hit $63M in the first year after it went into effect.

Your users data is paramount (always but especially under GDPR) - understand how your company uses it and be responsive to user data requests