Nicole P. Satiembre **April 30, 2024**

Cebu Technological University - Main Campus

Data Privacy Rules - GDPR

GDPR stands for General Data Protection Legislation. It is a European Union (EU) law that came into effect on 25th May 2018. GDPR governs the way in which we can use, process, and store personal data (information about an identifiable, living person). Data subjects will now have the right to demand subject access to their personal information, and the right to demand that an organisation destroys their personal information.

GDPR Key Principles:

- Lawfulness, transparency and fairness
- Only using data for the specific lawful purpose that it was obtained, the most lenient of which is legitimate interests
- Only acquiring data that we strictly need
- Ensuring any data we possess is accurate
- Storage limitation
- Integrity and confidentiality
- Accountability

Why is GDPR important?

GDPR makes sure that everyone in the EU follows the same rules about protecting people's personal information, making things fairer and more transparent. It gives people more say in how their data is used, which helps build trust between businesses and customers. Businesses need to follow GDPR to avoid big fines and keep their customers' trust by protecting their data well.

Who Does GDPR apply to?

GDPR applies to any individual or organisation that handles personal data within the EU. Countries outside of the EU that handle personal data are known as 'Third Countries' under GDPR. They may have their own data protection legislation but they are required to comply with GDPR in the following circumstances:

When supplying goods/services to the EU.

When processing data about citizens residing within the EU.

The Key Aspects of GDPR

GDPR has replaced the 1995 Data Protection Directive, which established minimum requirements for data protection across Europe. Now, the changes established in the GDPR will provide better protection of data subjects' fundamental rights. This change includes: Extended Jurisdiction, Consent, Right to Access, Right to be Forgotten, Data Protection Officer, Penalties.

Why was GDPR needed

Society is now more data-driven than ever, therefore the vast amount of sensitive data stored upon computers, has resulted in a rise in cyber-attacks and data breaches. Phishing is one of the key ways that cyber-criminals can infiltrate personal information using scam emails, and even alter bank details and account details.

Does GDPR replace the DPA

The DPA was admittedly outdated and no longer reflected the digital/technological age in which we live. For example, a vast proportion of individuals in the UK use social media, many of us possess more than one digital device (phones, tablets, laptops), and almost all businesses rely on computer networks. The digital world that we live in has changed the way we process information, and the laws were updated accordingly.

Businesses must conduct a Data Protection Impact Assessment (DPIA) if a processing activity is likely to result in a high risk to individuals. This is intended to identify and minimise risk to individuals' personal data. The risk assessment considers both the likelihood and severity of impact of the risk. If whilst conducting a DPIA you identify a high risk which you cannot mitigate, you must inform the ICO. Consent is also more tightly regulated under GDPR, meaning that businesses need to familiarise themselves with these new requirements.