Cheatography

GDPR: Six Data Protection Principles Cheat Sheet

by [deleted] via cheatography.com/2754/cs/16380/

Introduction

The EU General Data Protection Regulation (GDPR) outlines six data protection principles that organisations need to follow when collecting, processing and storing individuals' personal data. The data controller is responsible for complying with the principles and must be able to demonstrate the organisation's compliance practices. We've listed the six principles here with advice on how you can follow them.

Source: https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

1. Lawfulness, fairness and transparency

Organisations need to make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects. To remain lawful, you need to have a thorough understanding of the GDPR and its rules for data collection. To remain transparent with data subjects, you should state in your privacy policy the type of data you collect and the reason you're collecting it.

2. Purpose limitation

Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

Processing that's done for archiving purposes in the public interest or for scientific, historical or statistical purposes is given more freedom.

3. Data Minimisation

Organisations must only process the personal data that they need to achieve its processing purposes. Doing so has two major benefits. First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data. Second, data minimisation makes it easier to keep data accurate and up to date.

4. Accuracy

The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete.

Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

EU GPDR

5. Storage limitation

Organisations need to delete personal data when it's no longer necessary.

How do you know when information is no longer necessary? According to marketing company Epsilon Abacus, organisations might argue that they "should be allowed to store the data for as long as the individual can be considered a customer. So the question really is: For how long after completing a purchase can the individual be considered a customer?"

The answer will vary between industries and the reasons that data is collected. Any organisation that is uncertain how long it should keep personal data should consult a legal professional.

6. Integrity and confidentiality

This is the only principle that deals explicitly with security. The GDPR states that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The GDPR is deliberately vague about what measures organisations should take, because technological and organisational best practices are constantly changing. Currently, organisations should encrypt and/or pseudonymise personal data wherever possible, but they should also consider whatever other options are suitable