sempre | analytics

Seven Core Principles of GDPR in Practice

Regulations like GDPR provide a framework for data privacy controls. The seven guiding principles have been outlined below. Health records are often a good example to demonstrate how each principle might be applied and how technology can support the implementation of each principle.

1 Lawfulness, Fairness, and Transparency

There should be good reason to process someone's data. For data processing to be lawful, one of the following conditions must apply;

1. explicit consent has been given
2. there is a contractual or legal necessity
3. to protect vital interests
4. it must be in the public interest or
5. legitimate interest

For example, when a patient shares medical records with a health insurer, only necessary data should be accessible, and explicit consent must be given. Alternatively, if health records are accessed accident and emergency practitioner to give treatment, it is in the vital interest of the patient.

Data catalogues ensure that information is well-documented and only available to authorised personnel, building trust and reducing privacy risks.

2 Purpose Limitation

Data should be processed only for its intended purpose. With the healthcare example, patient information should be used for assessing a claim, not to sell insurance products.

Documenting the initial use case and making that searchable ensures that employees understand the limitations on data use, while auditing access helps enforce these rules.

3 Data Minimisation

Insurance companies should collect only the information necessary for a claim. The idea of only capturing what is necessary limits exposure and reduces privacy risks from the outset.

4 Accuracy

Through data quality processes, organisations can validate, correct, and even delete outdated or inaccurate information, ensuring that decisions are based on reliable data.

5 Storage Limitation

Under GDPR, data shouldn't be kept longer than necessary. This principle requires businesses to document why data was collected, how long it will be kept, and when it should be reviewed. Technology solutions can help by automating these timelines.

6 Integrity and Confidentiality

Protecting data from unauthorised access is at the core of data privacy. Using technology to control and track access requests, implementing masking, and continuously monitoring access ensures that data remains secure.

7 Accountability

Organisations need to demonstrate compliance with all of these principles. This is where tools like data catalogues and marketplaces shine. By providing visibility into data quality, access, and usage, we ensure that our approach to data privacy is transparent and auditable. Which should in turn mean fewer sleepless nights.

Almost all of these principles can be managed using technology solutions. To learn more, read our blog Optimising Data Privacy with Cutting-Edge Technology Solutions or contact us to find out more.