Principles of the GDPR

Here is a simplified guide to the 7 Core Principles of the GDPR (Article 5).

Think of these not just as codes, but as the "Golden Rules" for how you handle data. If you violate these principles, you are violating the GDPR, even if your security is technically perfect.

1. Lawfulness, Fairness, and Transparency

Your Obligation: You must be honest and open about what you are doing.

Lawful: You cannot process data just because you want to. You need a valid legal reason (like Consent or a Contract).

Fair: You shouldn't do things with data that people wouldn't expect or that could mislead them. You must give them control over their information.

Transparent: You can't hide in the shadows. You must provide clear, accessible information (usually a Privacy Notice) explaining exactly how you process their data.

2. Purpose Limitation

Your Obligation: Be specific about why you need the data and stick to that reason.

The Rule: You must collect data for "specified, explicit, and legitimate purposes".

No "Scope Creep": You cannot collect data for one reason (e.g., "to deliver a pizza") and then use it for a completely different reason later (e.g., "to sell their address to a gym"), unless you get fresh consent or have another clear legal reason.

Communication: You must tell the individual this purpose at the start.

3. Data Minimisation

Your Obligation: Collect only what you strictly need.

The Rule: Data must be adequate, relevant, and limited to what is necessary for your specific purpose.

Practical Step: If you don't need someone's date of birth to sell them a book, don't ask for it. Avoid hoarding "just in case" data.

4. Accuracy

Your Obligation: Keep the data correct and up to date.

The Rule: You must take reasonable steps to ensure data is not incorrect or misleading.

Correction: If you find out data is wrong, you must fix it or erase it without delay. You should also give individuals an easy way to update their own records.

5. Storage Limitation

Your Obligation: Don't keep data forever.

The Rule: You must not keep personal data for longer than you actually need it for your stated purpose.

Guidance: There may be a statutory requirement for a retention period (e.g. Revenue), or a supervisory body providing guidance. If neither exist, then set your own retention period and document the justification for it.

Retention Policy: You need a clear policy that says when you will delete data. When that time comes, you must securely erase or anonymise it.

6. Integrity and Confidentiality (Security)

Your Obligation: Keep the data safe.

The Rule: You must protect data against unauthorised access, accidental loss, destruction, or damage.

Measures: This isn't just about firewalls. It includes organisational measures like taking data backups, restricting access so only the staff who need to see the data can see it, amongst other things.

Accountability

Your Obligation: Prove it.

The Rule: It is not enough to just comply with these principles. You must be able to demonstrate that you comply.

Documentation: This requires you to have written policies, records of your processing activities, and internal procedures in place to show regulators that you take these rules seriously.