Principles of the GDPR

Article 5.

The GDPR sets out the principles that organisations must follow when processing personal data. In simpler terms, it outlines the basic rules for how organisations should handle and protect people's personal information.

The principles set out in Article 5 are:

Lawfulness, fairness, and transparency: Organisations must process personal data lawfully, fairly, and in a transparent manner.

> This principle means that personal data must be processed lawfully, meaning that there must be a legitimate reason for processing the data, such as obtaining the individual's consent, fulfilling a contractual obligation, or complying with a legal obligation. The processing must also be fair, which means that individuals must be informed about how their data will be used and have the ability to control how it is processed. Finally, the processing must be transparent, which means that individuals must be provided with clear and accessible information about how their data will be processed.

Purpose limitation: Personal data must be collected and processed for specified, explicit, and legitimate purposes.

> Personal data must be collected and processed for specified, explicit, and legitimate purposes. This means that organisations must have a clear reason for collecting and processing personal data and must inform individuals about the purpose for which their data is being collected. Organisations cannot use the data for other purposes unless they have obtained the individual's consent or have a legitimate reason for doing so.

Data minimisation: Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

> This principle requires that organisations only collect and process the personal data that is necessary for the purpose for which it is being processed. This means that organisations should avoid collecting excessive or unnecessary data and should not keep the data for longer than is necessary.

Accuracy: Personal data must be accurate and kept up to date, with appropriate measures in place to ensure inaccuracies are corrected or erased.

Organisations must take steps to ensure that personal data is accurate and up to date and should provide individuals with the ability to update their data if necessary.

Storage limitation: Personal data must not be kept for longer than is necessary for the purposes for which it is processed.

Organisations must have a clear retention policy for personal data and must ensure that the data is securely erased or anonymised when it is no longer needed.

Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

Organisations must take appropriate technical and organisational measures to protect personal data and must ensure that only authorised personnel have access to the data.

Accountability: Organisations are responsible for ensuring that they comply with the GDPR, including each of the foregoing principles and must be able to demonstrate this compliance.

This means that organisations must have appropriate policies and procedures in place to ensure compliance with the GDPR and must be able to demonstrate that they are complying with these policies and procedures.

In summary, Article 5 of the GDPR requires organisations to process personal data lawfully, fairly, and transparently, for specified purposes and with appropriate safeguards in place to protect against unauthorised processing, inaccuracies, and other risks to individuals' privacy. Organisations must also be able to demonstrate that they are complying with these principles and be accountable for their data processing activities.