

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Lawful basis for processing: Identify the lawful basis for processing personal data. For example, the lawful basis may be the consent of the individual, or the processing may be necessary for the performance of a contract.

Purpose: Ensure that the processing of personal data is necessary to achieve the intended purpose. There should be no function creep, meaning the processing of data should be limited to what is strictly necessary to achieve the purpose.

Data quality and minimization: Ensure that the personal data collected is accurate, up-to-date, and relevant to the purpose for which it is processed. Personal data should not be kept for longer than necessary.

Transparency and individuals' rights: Provide individuals with clear and concise information about the processing of their personal data, including the lawful basis for processing, the purpose of processing, the categories of personal data processed, and the retention period. Individuals have the right to access, rectify, erase, and restrict processing of their personal data.

Processor compliance: Ensure that any third-party processors comply with data protection requirements by putting in place a data processing agreement that includes appropriate safeguards.

International transfers: If personal data is transferred to a country outside the European Economic Area (EEA), ensure that appropriate safeguards are in place, such as standard contractual clauses or binding corporate rules.