Legal Basis for Processing under the GDPR

Article 6, Article 7, Article 8, Article 9 and Article 10.

The 6 legal basis for processing:

Article 6 of the GDPR outlines the conditions under which it is lawful to process personal data. In simpler terms, it explains the reasons why organisations are allowed to collect and use your personal information.

There are six lawful bases for processing personal data:

Consent: You have given clear and specific consent for your data to be processed.

Contract: The processing is necessary for the performance of a contract to which you are a party.

Legal obligation: The processing is necessary for compliance with a legal obligation.

Vital interests: The processing is necessary to protect your vital interests or those of another natural person.

Public interest: The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Legitimate interests: The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by your fundamental rights and freedoms.

In summary, organisations are required to have a lawful basis for processing your personal data, and they must be transparent about the basis they are relying on. If you have any concerns about how your data is being used, you have the right to ask the organisation for more information and to object to the processing of your data under certain circumstances.

Conditions for obtaining consent:

Article 7 of the GDPR explains what an organisation must do in order to ask for your permission to use your personal information.

Consent must be:

Freely given: This means that you must have a real choice and the ability to say "yes" or "no" without facing negative consequences.

Informed: You must be provided with clear and understandable information about what you are consenting to, including who will be processing your data and why.

Specific: You must be asked to give consent for a specific purpose, rather than a broad or vague set of purposes.

Unambiguous: The request for consent must be clear and easily understandable, so that you know exactly what you are agreeing to.

Given through a clear affirmative action: You must actively and explicitly give your consent, for example by ticking a box or clicking a button.

Organisations must also be able to demonstrate that they have obtained valid consent, meaning that they have followed the above requirements and can prove that you have given your consent.

If you later decide that you no longer wish for your data to be processed, you have the right to withdraw your consent at any time. Organisations must respect your decision and stop processing your data as soon as possible after receiving your request.

Conditions on consent from children in relation to information society services:

Article 8 of the GDPR aims to protect the privacy of children when their personal information is collected and used.

If an organisation wants to process the personal data of a child (someone under 16 years old, although member states may choose to lower this age to 13), they must obtain consent from the child's parent or legal guardian.

In some cases, the organisation may be able to obtain consent directly from the child, but only if the child is old enough to understand what they are consenting to. In these cases, the organisation must take reasonable steps to verify that the child's parent or legal guardian has given their consent.

The organisation must also provide clear and age-appropriate information to the child about how their data will be used and obtain the child's consent for each specific purpose.

The purpose of this article is to protect children from being targeted with inappropriate advertising or having their personal information collected without their parent's or guardian's consent. The GDPR recognises that children are more vulnerable than adults when it comes to their personal information, and that they need special protections.

Overall, Article 8 emphasises the importance of obtaining consent from a child's parent or guardian when processing their personal information and ensuring that the child's privacy rights are respected.

What does “information society services” mean:

The reference to "information society services" refers to any service provided over the internet or other electronic means, such as social media, online games, or mobile apps.

This means that if an organisation is providing an online service that involves the processing of a child's personal data, such as their name, age, or location, they must obtain the consent of the child's parent or legal guardian before processing that data.

For example, if a child wants to sign up for an online game that requires them to provide personal information, the organisation providing the game must obtain the consent of the child's parent or guardian before processing that information.

Processing of special categories of personal data:

Article 9 of the GDPR sets out rules for how organisations should handle particularly sensitive types of personal information, such as information about a person's health, ethnicity, religion, or political opinions. Specifically:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning sex life, or sexual orientation

Processing of such sensitive data is generally prohibited, except in certain circumstances such as:

- The individual has given their explicit consent for the processing of their data.
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment or social security.
- The processing is necessary for reasons of public interest in the area of public health.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

If an organisation wants to process sensitive personal data, they must ensure that they have a lawful basis for doing so and that the processing meets one of the above criteria.

Additionally, any processing of sensitive data must be carried out with appropriate safeguards in place to protect the fundamental rights and freedoms of the individual, including their right to privacy.

Overall, Article 9 sets out clear rules for how organisations should handle particularly sensitive types of personal information, to ensure that individuals' privacy rights are protected and that their data is processed only when there is a legitimate need to do so.

Processing of personal data relating to criminal convictions and offences

Article 10 of the GDPR states that processing of personal data relating to criminal convictions and offenses, or related security measures, must be carried out under the control of official authority or when authorised by EU or Member State law.

This means that personal data related to criminal convictions and offenses, such as information about a person's criminal record or a history of driving offenses, must be processed in accordance with specific legal requirements. The processing of this type of personal data is considered particularly sensitive, and therefore, it must be carried out with appropriate safeguards in place to protect individuals' privacy rights.

The GDPR recognises that there may be legitimate reasons for processing this type of personal data, such as for the purposes of law enforcement or public security. However, it requires that such processing must be carried out under the control of official authority or authorised by EU or Member State law, to ensure that there are appropriate safeguards in place to protect individuals' rights and freedoms.

In short, Article 10 of the GDPR places strict requirements on the processing of personal data related to criminal convictions and offenses and ensures that any processing of this type of data is carried out in accordance with the law and with appropriate safeguards in place to protect individuals' privacy.