The General Data Protection Regulation (GDPR) is a comprehensive data protection law in the European Union (EU) and the European Economic Area (EEA). It aims to give individuals more control over their personal data and to create a uniform data protection framework across Europe.

Here are the key requirements of the GDPR:

1. Lawful, Fair, and Transparent Processing:

- Personal data must be processed lawfully, fairly, and in a transparent manner.
- Individuals have the right to be informed about how their data is collected, used, and shared.

2. Purpose Limitation:

- Personal data can only be collected for specified, explicit, and legitimate purposes.
- It cannot be further processed in a manner incompatible with those purposes.

3. Data Minimization:

- Organizations should only collect and process the personal data that is necessary for the intended purpose.

4. Accuracy:

- Personal data must be accurate and kept up to date.
- Inaccurate data should be rectified or erased promptly.

5. Storage Limitation:

- Personal data should not be kept for longer than is necessary for the purposes for which it was collected.

6. Integrity and Confidentiality (Security):

- Personal data must be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

7. Accountability:

- Organizations are responsible for demonstrating compliance with the GDPR.
- They must implement appropriate technical and organizational measures to ensure and demonstrate compliance.

8. Data Subject Rights:

- Individuals have several rights under the GDPR, including:
    - The right to be informed about how their data is processed.
    - The right of access to their personal data.
    - The right to rectification of inaccurate data.
    - The right to erasure ("right to be forgotten").
    - The right to restrict processing.
    - The right to data portability.
    - The right to object to processing.
    - Rights related to automated decision-making and profiling.

9. Consent:

- In many cases, organizations need to obtain individuals' consent before collecting or processing their personal data.
- Consent must be freely given, specific, informed, and unambiguous.
- Individuals have the right to withdraw their consent at any time.

10. Data Breach Notification:

- Organizations must notify the relevant supervisory authority of a personal data breach within 72 hours of becoming aware of it.
- In some cases, they may also need to inform the affected individuals.

11. Data Protection Impact Assessment (DPIA):

- A DPIA is required when a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

12. Data Protection Officer (DPO):

- In certain circumstances, organizations must appoint a DPO to oversee their data protection activities.

13. International Data Transfers:

- Transfers of personal data outside the EU/EEA are subject to specific rules to ensure that the level of protection is not undermined.

Non-compliance with the GDPR can result in significant fines. The maximum fine is €20 million or 4% of the organization's global annual turnover, whichever is higher.

It's important to note that the GDPR is a complex regulation, and the specific requirements may vary depending on the nature of the data processing activities. Organizations should seek legal advice to ensure compliance.

Sources

1. jumpcloud.com/blog/prepare-gdpr-compliant
2. www.roam.ai/blog/what-is-general-data-protection-regulation-compliance
3. www.lepide.com/blog/consumer-privacy-rights-under-gdpr/
4. woolconcept.be/en/privacy