Professional Certificate in GDPR and AI Data Privacy Compliance

Data Protection By Design

Accountability in the context of GDPR refers to the responsibility of organizations to demonstrate their compliance with the regulation, ensuring that they have implemented appropriate measures to protect personal data. This concept is closely related to data protection by design, which requires organizations to consider data protection principles from the outset of any project or process.

Algorithmic decision-making refers to the use of algorithms to make decisions about individuals, often based on their personal data. This concept is relevant to GDPR and AI data privacy compliance, as it raises concerns about bias and transparency in decision-making processes.

Anonymization is the process of removing or obscuring personal data to prevent identification of individuals. This concept is related to data protection by design, as it requires organizations to consider how to protect personal data from the outset.

Artificial intelligence (AI) refers to the use of computer systems to perform tasks that would typically require human intelligence, such as decision-making or problem-solving. This concept is closely related to GDPR and data privacy compliance, as it raises concerns about bias and transparency in decision-making processes.

Authentication refers to the process of verifying the identity of individuals or systems, often using credentials such as passwords or biometric data. This concept is relevant to GDPR and data protection by design, as it requires organizations to ensure that only authorized individuals have access to personal data.

Authorization refers to the process of granting access to personal data or systems, often based on the role or permissions of individuals. This concept is closely related to GDPR and data protection by design, as it requires organizations to ensure that only authorized individuals have access to personal data.

Automated decision-making refers to the use of algorithms or computer systems to make decisions about individuals, often without human intervention.

Bias in the context of AI and GDPR refers to the presence of prejudices or discriminatory patterns in algorithms or decision-making processes. This concept is closely related to fairness and transparency in decision-making processes.

Bring Your Own Device (BYOD) refers to the practice of allowing employees to use their personal devices for work purposes, often raising concerns about data security and compliance. This concept is relevant to GDPR and data protection by design, as it requires organizations to ensure that personal data is protected

regardless of the device used to access it.

Cloud computing refers to the use of remote servers or cloud-based services to store, process, or manage data, often raising concerns about data security and compliance. This concept is closely related to GDPR and data protection by design, as it requires organizations to ensure that personal data is protected regardless of where it is stored or processed.

Compliance in the context of GDPR refers to the responsibility of organizations to demonstrate their adherence to the regulation, ensuring that they have implemented appropriate measures to protect personal data. This concept is closely related to accountability and data protection by design.

Consent in the context of GDPR refers to the explicit agreement of individuals to the processing of their personal data, often requiring organizations to provide clear and transparent information about the purposes and consequences of processing.

Data breach refers to the unauthorized or unlawful disclosure, access, or loss of personal data, often requiring organizations to notify affected individuals and regulatory authorities. This concept is closely related to GDPR and data protection by design, as it requires organizations to have procedures in place to respond to data breaches.

Data controller in the context of GDPR refers to the organization or individual that determines the purposes and means of processing personal data, often responsible for ensuring compliance with the regulation.

Data minimization in the context of GDPR refers to the principle of collecting and processing only the minimum amount of personal data necessary to achieve a specific purpose, often requiring organizations to consider data protection by design.

Data portability in the context of GDPR refers to the right of individuals to transfer their personal data from one organization to another, often requiring organizations to provide machine-readable formats for data transfer.

Data processor in the context of GDPR refers to the organization or individual that processes personal data on behalf of the data controller, often responsible for ensuring compliance with the regulation.

Data protection by design in the context of GDPR refers to the principle of considering data protection principles from the outset of any project or process, often requiring organizations to implement technical and organizational measures to protect personal data.

Data protection impact assessment (DPIA) refers to the process of evaluating the potential risks and consequences of processing personal data, often requiring organizations to consider data protection by design.

Data protection officer (DPO) refers to the individual or team responsible for overseeing an organization's data protection practices and ensuring compliance with GDPR.

Data security in the context of GDPR refers to the measures taken to protect personal data from unauthorized or unlawful access, disclosure, or loss, often requiring organizations to implement technical and organizational measures.

Data subject in the context of GDPR refers to the individual whose personal data is being processed, often having rights such as access, rectification, and erasure.

Data transfer in the context of GDPR refers to the transfer of personal data from one organization to another, often requiring organizations to ensure that the transfer is lawful and secure.

Encryption refers to the process of converting personal data into a code to protect it from unauthorized access, often requiring organizations to implement technical measures to protect personal data.

Fairness in the context of AI and GDPR refers to the principle of ensuring that algorithms or decision-making processes are unbiased and non-discriminatory, often requiring organizations to consider data protection by design.

General Data Protection Regulation (GDPR) refers to the European Union's regulation on the protection of personal data, often requiring organizations to implement technical and organizational measures to protect personal data.

Information commissioner's office (ICO) refers to the regulatory authority responsible for overseeing data protection practices in the United Kingdom, often providing guidance and enforcement of GDPR.

International data transfer in the context of GDPR refers to the transfer of personal data from the European Union to a third country, often requiring organizations to ensure that the transfer is lawful and secure.

Machine learning refers to the use of algorithms to enable computer systems to learn from data and improve their performance, often raising concerns about bias and transparency in decision-making processes.

Natural language processing (NLP) refers to the use of algorithms to enable computer systems to understand and generate human language, often raising concerns about bias and transparency in decision-making processes.

Personal data in the context of GDPR refers to any information relating to an identified or identifiable individual, often including names, addresses, and identification numbers.

Privacy by design in the context of GDPR refers to the principle of considering privacy principles from the outset of any project or process, often requiring organizations to implement technical and organizational

measures to protect personal data.

Pseudonymization refers to the process of replacing personal data with artificial identifiers to protect individuals' privacy, often requiring organizations to consider data protection by design.

Right to be forgotten in the context of GDPR refers to the right of individuals to request the erasure of their personal data, often requiring organizations to consider data protection by design.

Right to access in the context of GDPR refers to the right of individuals to access their personal data, often requiring organizations to provide clear and transparent information about the purposes and consequences of processing.

Right to rectification in the context of GDPR refers to the right of individuals to request the rectification of their personal data, often requiring organizations to consider data protection by design.

Risk assessment in the context of GDPR refers to the process of evaluating the potential risks and consequences of processing personal data, often requiring organizations to consider data protection by design.

Security by design in the context of GDPR refers to the principle of considering security principles from the outset of any project or process, often requiring organizations to implement technical and organizational measures to protect personal data.

Supervisory authority in the context of GDPR refers to the regulatory authority responsible for overseeing data protection practices in a member state, often providing guidance and enforcement of GDPR.

Transparency in the context of AI and GDPR refers to the principle of providing clear and intelligible information about the purposes and consequences of processing personal data, often requiring organizations to consider data protection by design.

Vendor management in the context of GDPR refers to the process of managing the relationship between an organization and its vendors or third-party providers, often requiring organizations to ensure that vendors comply with GDPR.

Workforce management in the context of GDPR refers to the process of managing an organization's workforce to ensure compliance with the regulation, often requiring organizations to provide training and awareness programs for employees.