Graduate Certificate in Advanced Studies in Data Privacy Law

Foundations of Data Privacy Law

Foundations of Data Privacy Law

Data privacy law is a legal framework that governs the collection, use, storage, and sharing of personal data. It aims to protect individuals' privacy rights and ensure that their personal information is handled responsibly by organizations. The foundations of data privacy law are based on several key principles and concepts that shape the way data privacy is regulated and enforced. This glossary will explore some of the essential terms and concepts in data privacy law, focusing on the Graduate Certificate in Advanced Studies in Data Privacy Law.

1. Anonymization

Anonymization is the process of removing personally identifiable information from data sets to protect individuals' privacy. By anonymizing data, organizations can use it for analysis and research purposes without revealing the identities of the individuals involved. However, it is essential to note that complete anonymization is challenging to achieve, as there is always a risk of re-identification if the data is combined with other information.

Related terms: Pseudonymization, De-identification, Re-identification

2. Consent

Consent is a fundamental principle of data privacy law that requires individuals to give explicit permission for their personal data to be collected, processed, or shared by organizations. Consent must be freely given, specific, informed, and unambiguous, and individuals have the right to withdraw their consent at any time. Organizations must obtain consent in a clear and transparent manner, and they are required to keep records of consent to demonstrate compliance with data privacy regulations.

Related terms: Opt-in, Opt-out, Explicit consent, Implied consent

3. Data Breach

A data breach occurs when there is unauthorized access to or disclosure of personal data. Data breaches can result from cyberattacks, human error, or system vulnerabilities, and they can have serious consequences for individuals and organizations. In the event of a data breach, organizations are required to notify affected individuals and regulatory authorities promptly and take steps to mitigate the impact of the breach. Data breach notification requirements are a key aspect of data privacy laws worldwide.

Related terms: Data breach response plan, Data breach notification, Data breach investigation

4. Data Controller

A data controller is an entity that determines the purposes and means of processing personal data. Data controllers are responsible for ensuring that personal data is processed lawfully, fairly, and transparently, in accordance with data privacy regulations. They must implement appropriate security measures to protect the data and uphold individuals' privacy rights. Data controllers have legal obligations under data privacy laws to fulfill certain requirements, such as providing individuals with access to their data and responding to data subject requests.

Related terms: Data processor, Data protection officer, Joint data controllers

5. Data Minimization

Data minimization is a principle of data privacy law that requires organizations to collect only the personal data that is necessary for a specific purpose. By minimizing the amount of data collected and processed, organizations can reduce the risk of data breaches and unauthorized access. Data minimization also helps to protect individuals' privacy rights by limiting the exposure of their personal information. Organizations must carefully assess their data processing activities and only collect the data that is essential for achieving their goals.

Related terms: Data retention, Data collection, Purpose limitation

6. Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a tool used by organizations to identify and mitigate the risks associated with data processing activities. DPIAs help organizations assess the impact of their data processing on individuals' privacy rights and determine the measures needed to ensure compliance with data privacy regulations. Organizations are required to conduct DPIAs for high-risk processing activities, such as those involving sensitive personal data or large-scale data processing. DPIAs are an essential component of data privacy compliance programs.

Related terms: Privacy impact assessment, Risk assessment, Data protection by design and by default

7. Data Subject

A data subject is an individual who is the subject of personal data. Data subjects have rights under data privacy laws, such as the right to access their data, the right to rectify inaccuracies, and the right to erasure. Data subjects also have the right to object to the processing of their data and to restrict its use in certain circumstances. Organizations must respect and uphold data subjects' rights by implementing appropriate data protection measures and processes.

Related terms: Data subject rights, Data subject access request, Data subject consent

8. Encryption

Encryption is a method of protecting data by encoding it in a way that only authorized parties can access and read it. Encrypted data is scrambled using algorithms and keys, making it unreadable to anyone without the decryption key. Encryption is an essential security measure for protecting sensitive and confidential

information from unauthorized access or disclosure. Organizations are encouraged to use encryption to safeguard personal data and comply with data privacy regulations that require data security measures.

Related terms: Decryption, Encryption key, Encryption at rest, Encryption in transit

9. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive data privacy law that applies to organizations operating within the European Union (EU) and the European Economic Area (EEA). The GDPR sets out rules for the collection, processing, and sharing of personal data and aims to strengthen individuals' privacy rights. The GDPR introduces requirements for organizations to obtain consent for data processing, implement data protection measures, and appoint a Data Protection Officer (DPO). Non-compliance with the GDPR can result in significant fines and penalties.

Related terms: Personal data, Data protection authority, GDPR compliance, GDPR principles

10. Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) is the UK's independent regulatory authority responsible for enforcing data protection laws, including the GDPR and the Data Protection Act 2018. The ICO oversees organizations' compliance with data privacy regulations, investigates data breaches, and issues fines for non-compliance. The ICO provides guidance and support to organizations on data protection best practices and helps individuals understand their privacy rights. Organizations operating in the UK must register with the ICO and adhere to its data protection requirements.

Related terms: Data protection authority, Data protection regulator, Privacy commissioner

11. Privacy by Design

Privacy by Design is a concept that emphasizes integrating data protection measures into the design and development of products, services, and systems. By considering privacy issues from the outset, organizations can build privacy-enhancing features and controls into their processes and technologies. Privacy by Design aims to prevent privacy risks and protect individuals' personal data throughout its lifecycle. Organizations are encouraged to adopt Privacy by Design principles as part of their data privacy compliance efforts.

Related terms: Data protection by default, Privacy engineering, Privacy-enhancing technologies

12. Right to be Forgotten

The Right to be Forgotten is a privacy right that allows individuals to request the deletion or removal of their personal data from an organization's records. The Right to be Forgotten is enshrined in the GDPR and gives individuals the power to control the information that is stored about them online. Organizations must comply with requests to erase data under certain conditions, such as when the data is no longer necessary for its original purpose or when the individual withdraws consent for processing. The Right to be Forgotten is a key privacy right that empowers individuals to manage their digital footprint.

Related terms: Data erasure, Data deletion, Right to erasure, Right to delete

13. Sensitive Personal Data

Sensitive personal data, also known as special categories of data, is a classification of personal information that is considered particularly sensitive and deserving of enhanced protection. Sensitive personal data includes information about an individual's race, ethnic origin, political opinions, religious beliefs, health, sexual orientation, genetic data, and biometric data. Organizations are subject to strict requirements when processing sensitive personal data, such as obtaining explicit consent, implementing additional security measures, and restricting access to the data. Sensitive personal data is defined and regulated under data privacy laws to safeguard individuals' privacy rights and prevent discrimination or harm.

Related terms: Special categories of data, Highly sensitive data, Restricted data

14. Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is a process that helps organizations identify and assess the privacy risks associated with their data processing activities. PIAs involve evaluating the impact of data processing on individuals' privacy rights, identifying potential risks and vulnerabilities, and implementing measures to mitigate them. PIAs are used to ensure that organizations comply with data privacy regulations, such as the GDPR, and protect individuals' personal data. Conducting PIAs is a best practice for organizations to demonstrate accountability and transparency in their data processing practices.

Related terms: Data protection impact assessment, Privacy risk assessment, Privacy compliance assessment

15. Data Protection Officer (DPO)

A Data Protection Officer (DPO) is a designated individual within an organization who is responsible for overseeing data protection and privacy compliance. The DPO's role includes advising on data protection requirements, monitoring compliance with data privacy laws, and coordinating responses to data subject requests and data breaches. The DPO acts as a point of contact for regulatory authorities and data subjects and helps organizations establish and maintain effective data protection practices. Certain organizations are required to appoint a DPO under data privacy regulations, such as the GDPR.

Related terms: Chief Privacy Officer, Privacy officer, Data protection team

16. Data Subject Access Request (DSAR)

A Data Subject Access Request (DSAR) is a formal request made by an individual to access their personal data held by an organization. Data subjects have the right to request information about how their data is being processed, what data is being collected, and for what purposes. Organizations are required to respond to DSARs promptly and provide individuals with a copy of their data in a clear and understandable format. DSARs are an essential mechanism for individuals to exercise their privacy rights and ensure that their personal data is being handled appropriately.

Related terms: Right of access, Subject access request, Data access request

17. Privacy Shield

The EU-U.S. Privacy Shield was a data protection framework that allowed companies to transfer personal data from the European Union to the United States in compliance with EU data protection laws. The Privacy Shield was designed to ensure that data transferred to the U.S. received adequate protection and was subject to privacy principles equivalent to those in the EU. However, the Privacy Shield was invalidated by the Court of Justice of the European Union in 2020, leading to uncertainty for organizations that relied on the framework for transatlantic data transfers.

Related terms: Data transfer mechanism, Privacy framework, EU data protection laws

18. Accountability

Accountability is a core principle of data privacy law that requires organizations to demonstrate compliance with data protection regulations and take responsibility for their data processing activities. Accountability involves implementing appropriate technical and organizational measures to protect personal data, documenting data processing activities, and conducting regular audits and assessments to ensure compliance. Organizations must be able to demonstrate accountability to regulatory authorities and data subjects by maintaining records of data processing, conducting impact assessments, and responding to privacy inquiries.

Related terms: Data governance, Compliance management, Data protection framework

19. Cross-Border Data Transfers

Cross-border data transfers involve the movement of personal data from one country to another, either within the same organization or between different entities. Cross-border data transfers raise privacy concerns, as data protection laws may vary between jurisdictions, leading to differences in data protection standards and requirements. Organizations must ensure that cross-border data transfers comply with applicable data privacy regulations, such as the GDPR, and provide adequate safeguards to protect personal data. Methods for legitimizing cross-border data transfers include standard contractual clauses, binding corporate rules, and data protection agreements.

Related terms: International data transfers, Data localization, Data export

20. Data Processing Agreement

A Data Processing Agreement (DPA) is a contract between a data controller and a data processor that governs the processing of personal data on behalf of the controller. DPAs outline the responsibilities of the parties regarding data protection, security measures, data processing activities, and compliance with data privacy laws. Data controllers are required to enter into DPAs with data processors to ensure that personal data is processed in accordance with legal requirements and that appropriate safeguards are in place to protect individuals' privacy rights. DPAs are an essential tool for managing data processing relationships and ensuring data privacy compliance.

Related terms: Data processing terms, Data protection contract, Controller-processor agreement

21. Data Retention

Data retention is the practice of storing personal data for a specified period to fulfill legal, regulatory, or operational requirements. Organizations must establish data retention policies that define the length of time personal data will be retained and the purposes for which it will be used. Data retention policies help organizations manage data storage, comply with data privacy regulations, and minimize the risk of data breaches. Organizations are required to delete or anonymize data that is no longer necessary for its intended purpose and to ensure that data is securely disposed of when it reaches the end of its retention period.

Related terms: Data disposal, Data retention policy, Retention period

22. Data Localization

Data localization refers to the practice of storing and processing data within a specific geographic location or jurisdiction. Data localization laws require organizations to keep personal data within the borders of a particular country or region, rather than transferring it internationally. Data localization laws are designed to protect individuals' privacy rights, promote data sovereignty, and ensure that data is subject to local data protection regulations. Organizations must comply with data localization requirements when processing personal data in jurisdictions that impose restrictions on cross-border data transfers.

Related terms: Data sovereignty, Data residency, Data residency requirement

23. Data Security

Data security encompasses measures and practices designed to protect personal data from unauthorized access, disclosure, alteration, or destruction. Data security includes physical, technical, and organizational safeguards to safeguard data against cybersecurity threats, data breaches, and other security incidents. Organizations must implement appropriate data security measures, such as encryption, access controls, and security protocols, to protect personal data and comply with data privacy regulations. Data security is a critical aspect of data privacy compliance and is essential for maintaining the confidentiality, integrity, and availability of personal data.

Related terms: Information security, Cybersecurity, Data protection measures

24. Data Breach Response Plan

A data breach response plan is a documented set of procedures and protocols that organizations follow in the event of a data breach. Data breach response plans outline the steps to be taken to identify, contain, investigate, and mitigate data breaches, as well as the procedures for notifying affected individuals and regulatory authorities. Organizations must have a data breach response plan in place to respond effectively to security incidents, protect individuals' privacy rights, and comply with data breach notification requirements. Data breach response plans are an essential component of data privacy compliance programs.

Related terms: Incident response plan, Data breach management, Data breach notification process

25. Data Protection Authority (DPA)

A Data Protection Authority (DPA) is an independent regulatory body responsible for enforcing data protection laws and overseeing compliance with data privacy regulations. DPAs are appointed by governments to monitor organizations' data processing activities, investigate complaints, and impose fines for non-compliance. DPAs provide guidance and support to organizations on data protection best practices and help individuals understand their privacy rights. DPAs play a crucial role in enforcing data privacy laws, promoting data protection, and safeguarding individuals' privacy rights.

Related terms: Information commissioner, Privacy regulator, Data protection agency

26. Data Breach Notification

Data breach notification is the process of informing affected individuals and regulatory authorities about a security incident that has resulted in unauthorized access to personal data. Data breach notification laws require organizations to notify individuals promptly when their personal data is compromised, so they can take steps to protect themselves from potential harm. Data breach notifications must include information about the nature of the breach, the types of data affected, and the steps individuals can take to mitigate the impact. Timely and transparent data breach notifications are essential for maintaining trust with data subjects and complying with data privacy regulations.

Related terms: Data breach communication, Data breach notification requirements, Data breach reporting

27. Data Mapping

Data mapping is the process of identifying, categorizing, and documenting the flow of personal data within an organization's systems, applications, and processes. Data mapping involves creating an inventory of data assets, mapping data flows, and documenting the types of personal data collected, stored, and processed. Data mapping helps organizations understand their data processing activities, assess privacy risks, and ensure compliance with data privacy regulations. By mapping data flows, organizations can identify potential vulnerabilities, implement data protection measures, and demonstrate accountability in their data processing practices.

Related terms: Data inventory, Data flow analysis, Data mapping tool

28. Data Privacy Impact Assessment (DPIA)

A Data Privacy Impact Assessment (DPIA) is a process that helps organizations identify and assess the privacy risks associated with new projects, products, or services that involve the processing of personal data. DPIAs help organizations evaluate the impact of data processing on individuals' privacy rights, identify potential risks and vulnerabilities, and implement measures to mitigate them. DPIAs are a proactive tool for ensuring that privacy considerations are integrated into project planning and decision-making processes. Conducting DPIAs is a best practice for organizations to assess and manage privacy risks effectively.

Related terms: Privacy risk assessment, Data protection impact assessment, Privacy compliance assessment

29. Data Subject Consent

Data subject consent is the legal basis for processing personal data under data privacy regulations, such as the GDPR. Data subjects must give explicit, informed, and unambiguous consent for their data to be collected, processed, or shared by organizations. Consent must be freely given, specific, and revocable, and organizations must obtain consent in a clear and transparent manner. Data subject consent is a key privacy principle that empowers individuals to control how their personal data is used and ensures that organizations process data lawfully and ethically.

Related terms: Consent management, Consent form, Consent revocation

30. Data Subject Rights

Data subject rights are the privacy rights that individuals have over their personal data, as enshrined in data privacy laws. Data subject rights include the right to access their data, the right to rectify inaccuracies, the right to erasure, the right to restrict processing, the right to data portability, and the right to object to processing. Data subjects can exercise their rights by submitting requests to organizations, known as data subject access requests (DSARs). Organizations must respect and uphold data subject rights by providing individuals with access to their data, responding to requests promptly, and ensuring that data processing activities comply with legal requirements.

Related terms: Privacy rights, Individual rights, Data subject requests

31. Privacy Policy

A privacy policy is