Advanced Certificate in AI in Regulatory Affairs

Data Privacy and Security in AI

Data Privacy and Security in AI Glossary

1. Artificial Intelligence (AI)
AI refers to the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using it), reasoning (using rules to reach approximate or definite conclusions), and self-correction.

Related Terms: Machine Learning, Deep Learning, Natural Language Processing

2. Data Privacy
Data privacy refers to the protection of personal information and data from unauthorized access, use, or disclosure. It involves the proper handling of sensitive data to ensure confidentiality and prevent misuse.

Related Terms: Personally Identifiable Information (PII), Data Protection, Privacy Regulations

3. Data Security
Data security involves the protection of data from unauthorized access, use, disclosure, disruption, modification, or destruction. It aims to ensure the confidentiality, integrity, and availability of data.

Related Terms: Encryption, Access Control, Cybersecurity

4. Consent Management
Consent management refers to the process of obtaining, storing, and managing user consent for the collection and use of their personal data. It is crucial for ensuring compliance with data privacy regulations such as the GDPR.

Related Terms: Consent Form, Opt-in/Opt-out, Consent Revocation

5. Encryption
Encryption is the process of converting data into a code to prevent unauthorized access. It ensures data security by making it unreadable to anyone without the proper decryption key.

Related Terms: Decryption, Encryption Algorithm, Public Key Infrastructure (PKI)

6. Personally Identifiable Information (PII)
PII refers to any information that can be used to identify a specific individual. This includes names, addresses, social security numbers, and other sensitive data that can be used for identity theft.

Related Terms: Data Minimization, Anonymization, De-identification

7. General Data Protection Regulation (GDPR)
The GDPR is a regulation in EU law on data protection and privacy for all individuals within the European

Union and the European Economic Area. It aims to give control to individuals over their personal data and simplify the regulatory environment for international business.

Related Terms: Data Subject Rights, Data Controller, Data Processor

8. Biometric Data
Biometric data refers to physical or behavioral characteristics that can be used to verify a person's identity. This includes fingerprints, facial recognition, iris scans, and voice patterns.

Related Terms: Biometric Authentication, Biometric Database, Biometric Privacy

9. Data Breach
A data breach is the unauthorized access, disclosure, or acquisition of sensitive data. It poses a significant risk to data privacy and security, leading to potential harm to individuals and organizations.

Related Terms: Cyberattack, Data Leak, Security Incident Response

10. Risk Assessment
Risk assessment involves identifying, analyzing, and evaluating potential risks to data privacy and security. It helps organizations understand their vulnerabilities and develop strategies to mitigate threats.

Related Terms: Risk Management, Threat Modeling, Vulnerability Assessment

11. Privacy by Design
Privacy by design is an approach to system engineering that takes privacy into account throughout the entire development process. It aims to embed privacy protections into the design of technologies, processes, and systems.

Related Terms: Privacy Impact Assessment (PIA), Data Protection by Design and by Default, Privacy Engineering

12. Data Retention
Data retention refers to the storage of data for a specific period based on legal, regulatory, or business requirements. It involves defining policies for how long data should be retained and when it should be securely disposed of.

Related Terms: Data Lifecycle Management, Data Archiving, Data Destruction

13. Privacy Policy
A privacy policy is a statement or legal document that explains how an organization collects, uses, discloses, and manages personal data. It informs individuals about their rights and how their data is protected.

Related Terms: Terms of Service, Data Processing Agreement, Privacy Notice

14. Data Governance
Data governance is a set of processes, policies, standards, and guidelines that ensure data is managed effectively and securely. It involves defining roles and responsibilities for data management within an

organization.

Related Terms: Data Quality, Data Stewardship, Data Management

15. Accountability
Accountability refers to the responsibility of organizations to demonstrate compliance with data privacy and security regulations. It involves implementing measures to protect data and being able to prove adherence to legal requirements.

Related Terms: Compliance, Auditing, Transparency

16. Anonymization
Anonymization is the process of removing or modifying personal data to prevent identification of individuals. It helps protect privacy by de-identifying data while maintaining its utility for analysis and research.

Related Terms: Pseudonymization, Data Masking, De-identification

17. Data Minimization
Data minimization is the practice of limiting the collection and retention of personal data to only what is necessary for a specific purpose. It helps reduce the risk of data breaches and privacy violations.

Related Terms: Data Collection, Data Processing, Data Purging

18. Consent Management Platform
A consent management platform is a tool or system used to manage user consent preferences and permissions for data processing. It helps organizations track and document consent to ensure compliance with privacy regulations.

Related Terms: Consent Management Software, Consent Management Service, Consent Management API

19. Data Subject Rights
Data subject rights are the rights granted to individuals regarding the processing of their personal data. These rights include the right to access, rectify, erase, and restrict the processing of personal data.

Related Terms: Right to be Forgotten, Right to Data Portability, Right to Object

20. Privacy Shield
Privacy Shield was a framework for transatlantic data transfers between the European Union and the United States. It was designed to ensure that personal data transferred outside the EU was adequately protected.

Related Terms: EU-US Privacy Shield, Data Transfer Agreement, Data Protection Adequacy

21. Two-Factor Authentication (2FA)
Two-factor authentication is a security process that requires users to provide two different authentication factors to verify their identity. This typically involves something the user knows (password) and something the user has (smartphone).

Related Terms: Multi-Factor Authentication, Authentication Factor, One-Time Password (OTP)

22. Data Masking
Data masking is a technique used to protect sensitive data by replacing real data with fictional or scrambled values. It allows organizations to use realistic but anonymized data for testing and development purposes.

Related Terms: Data Obfuscation, Data Redaction, Data Transformation

23. Consent Revocation
Consent revocation is the process of withdrawing previously given consent for the collection and processing of personal data. Individuals have the right to revoke their consent at any time under data privacy regulations.

Related Terms: Opt-out, Withdrawal of Consent, Data Erasure

24. Data Portability
Data portability is the ability of individuals to obtain and reuse their personal data for their own purposes across different services. It allows users to transfer their data from one platform to another easily.

Related Terms: Data Export, Interoperability, Data Transfer

25. Data Classification
Data classification is the process of categorizing data based on its sensitivity and importance. It helps organizations identify and apply appropriate security controls to protect data according to its classification.

Related Terms: Data Labeling, Data Categorization, Data Sensitivity

26. Data Localization
Data localization refers to laws or regulations that require data to be stored and processed within a specific geographic location. It is often imposed to protect data privacy and security or promote national interests.

Related Terms: Data Sovereignty, Data Residency, Cross-Border Data Transfers

27. Data Breach Notification
Data breach notification is the process of informing individuals and authorities about a security incident that compromises personal data. It helps affected parties take necessary steps to mitigate the impact of the breach.

Related Terms: Incident Response, Data Breach Response Plan, Notification Obligations

28. Data Processing Agreement
A data processing agreement is a contract between a data controller and a data processor that outlines the terms of data processing activities. It ensures that both parties comply with data protection regulations and safeguard personal data.

Related Terms: Data Controller, Data Processor, Data Sharing Agreement

29. Data Sovereignty
Data sovereignty refers to the concept that data is subject to the laws and regulations of the country in which it is located. It raises concerns about who has jurisdiction over data and how it can be accessed or transferred.

Related Terms: Data Jurisdiction, Data Localization, Data Protection Laws

30. Data Ethics
Data ethics involves considering the moral and ethical implications of data collection, storage, processing, and usage. It addresses issues such as privacy, consent, transparency, bias, and accountability in data-driven decision-making.

Related Terms: Ethical AI, Algorithmic Bias, Fairness and Accountability in AI

31. Data Security Incident Response Plan
A data security incident response plan outlines the steps an organization must take in the event of a data breach or security incident. It includes procedures for detection, containment, eradication, and recovery from the incident.

Related Terms: Cyber Incident Response Plan, Security Breach Response, Incident Handling

32. Data Subject Access Request (DSAR)
A data subject access request is a formal request from an individual to access their personal data held by an organization. Data controllers are required to respond to DSARs within a specified timeframe under data protection regulations.

Related Terms: Subject Access Request, Data Access Rights, Right of Access

33. Differential Privacy
Differential privacy is a privacy-preserving data analysis technique that adds noise to query responses to protect individual data privacy. It allows for aggregate analysis while preventing the disclosure of individual data points.

Related Terms: Privacy-Preserving Data Mining, Statistical Disclosure Control, Privacy Guarantees

34. Federated Learning
Federated learning is a machine learning approach that allows multiple parties to collaboratively train a shared model without sharing their raw data. It enables decentralized model training while preserving data privacy and security.

Related Terms: Collaborative Learning, Decentralized Learning, Privacy-Preserving Machine Learning

35. Homomorphic Encryption
Homomorphic encryption is a form of encryption that allows computations to be performed on encrypted data without decrypting it. It enables secure data processing while preserving data confidentiality.

Related Terms: Fully Homomorphic Encryption, Partially Homomorphic Encryption, Secure Multi-Party

Computation

36. Privacy-Preserving Machine Learning
Privacy-preserving machine learning refers to techniques that enable machine learning models to be trained on sensitive data without exposing the data itself. It ensures data privacy while allowing for model development.

Related Terms: Secure Machine Learning, Privacy-Preserving Data Analysis, Confidential Machine Learning

37. Secure Multi-Party Computation (MPC)
Secure multi-party computation is a cryptographic technique that allows multiple parties to jointly compute a function over their private inputs without revealing them. It enables collaborative data analysis while protecting data privacy.

Related Terms: Secure Computation, Privacy-Preserving Computation, Secret Sharing

38. Privacy-Enhancing Technologies (PETs)
Privacy-enhancing technologies are tools and techniques designed to protect data privacy and enhance security. They include encryption, anonymization, data masking, and other methods to safeguard personal information.

Related Terms: Privacy Tools, Privacy Solutions, Privacy Enhancers

39. Secure Enclave
A secure enclave is a hardware-based security feature that provides a protected area within a processor for storing and processing sensitive data. It ensures data confidentiality and integrity against unauthorized access.

Related Terms: Trusted Execution Environment, Secure Element, Hardware Security Module

40. Secure Federated Learning
Secure federated learning is an extension of federated learning that incorporates additional security measures to protect data privacy. It enhances the confidentiality and integrity of model updates during collaborative training.

Related Terms: Secure Aggregation, Secure Model Update, Privacy-Preserving Collaboration

41. Zero-Knowledge Proof
A zero-knowledge proof is a cryptographic protocol that allows one party to prove to another party that a statement is true without revealing any additional information. It enables verification of data without exposing the underlying data itself.

Related Terms: Non-Interactive Zero-Knowledge Proof, Proof of Knowledge, Secure Authentication

42. Secure Data Sharing
Secure data sharing involves transferring data between parties in a way that protects data privacy and security. It ensures that sensitive information remains confidential and is only accessible to authorized users.

Related Terms: Data Exchange, Secure Data Transfer, Encrypted Data Sharing

43. Privacy-Preserving Data Analysis
Privacy-preserving data analysis refers to techniques that enable analysis of sensitive data without compromising individual privacy. It allows for insights to be derived from data while protecting personal information.

Related Terms: Privacy-Preserving Statistics, Confidential Data Analysis, Secure Data Mining

44. Differential Privacy Mechanism
A differential privacy mechanism is a mathematical algorithm that introduces noise into query responses to prevent the identification of individual data points. It ensures privacy protection while enabling statistical analysis.

Related Terms: Privacy-Preserving Query, Differential Privacy Guarantee, Privacy-Enhanced Data Analysis

45. Secure Data Aggregation
Secure data aggregation is the process of combining and summarizing data from multiple sources while preserving data privacy and confidentiality. It allows for analysis of aggregated data without exposing individual records.

Related Terms: Privacy-Preserving Aggregation, Secure Data Fusion, Confidential Data Summarization

46. Privacy-Preserving Data Labeling
Privacy-preserving data labeling involves annotating data with labels or tags while protecting the privacy of sensitive information. It allows for the training of machine learning models without revealing individual data points.

Related Terms: Secure Data Annotation, Confidential Data Labeling, Privacy-Enhanced Dataset Creation

47. Data Security Compliance
Data security compliance refers to the adherence to laws, regulations, and standards related to data protection and security. It involves implementing measures to protect data and demonstrate compliance with legal requirements.

Related Terms: Regulatory Compliance, Data Protection Laws, Compliance Management

48. Secure Data Transmission
Secure data transmission ensures that data is transferred between systems or networks in a secure manner to prevent unauthorized access or interception. It involves encryption, authentication, and other security measures to protect data in transit.

Related Terms: Data Transfer Security, Secure Communication, Encrypted Data Exchange

49. Privacy-Preserving Data Collection
Privacy-preserving data collection involves gathering data from individuals in a way that protects their privacy and confidentiality. It includes obtaining informed consent, anonymizing data, and minimizing the

collection of sensitive information.

Related Terms: Secure Data Acquisition, Confidential Data Gathering, Privacy-Enhanced Data Collection

50. Secure Data Storage
Secure data storage involves safeguarding data while at rest to prevent unauthorized access, modification, or destruction. It includes encryption, access controls, backups, and other measures to protect data integrity and confidentiality.

Related Terms: Data Encryption, Secure Database, Data Backup and Recovery

51. Data Security Best Practices
Data security best practices are guidelines and recommendations for protecting data from security threats and breaches. They include measures such as encryption, access controls, regular audits, and employee training to enhance data security.

Related Terms: Security Standards, Data Protection Guidelines, Cybersecurity Best Practices

52. Secure Data Processing
Secure data processing involves handling data in a way that ensures confidentiality, integrity, and availability. It includes implementing security controls, monitoring data flows, and auditing processes to protect data during processing.

Related Terms: Data Integrity, Secure Processing Environment, Data Processing Controls

53. Privacy-Preserving Data Sharing
Privacy-preserving data sharing allows organizations to exchange data while protecting the privacy of individuals. It enables collaborative data analysis without revealing sensitive information or compromising data confidentiality.

Related Terms: Secure Data Collaboration, Confidential Data Exchange, Privacy-Enhanced Data Sharing

54. Secure Data Disposal
Secure data disposal involves permanently removing data from storage devices to prevent unauthorized access or recovery. It includes methods such as data wiping, degaussing, and physical destruction to ensure data is irretrievable.

Related Terms: Data Erasure, Data Destruction, Secure Data Retention Policy

55. Data Security Training
Data security training involves educating employees on best practices for protecting data and preventing security incidents. It helps raise awareness about data security risks and promotes a culture of security within organizations.

Related Terms: Security Awareness, Employee Training, Cybersecurity Education

56. Secure Data Governance

Secure data governance is the establishment of policies, processes, and controls to ensure data is managed securely and in compliance with regulations. It involves defining roles, responsibilities, and standards for data management.

Related Terms: Data Governance Framework, Information Security Governance, Data Compliance

57. Privacy-Preserving Data Processing
Privacy-preserving data processing involves analyzing data in a way that protects individual privacy and confidentiality. It allows for data insights to be derived while ensuring that sensitive information is not exposed.

Related Terms: Secure Data Analytics, Confidential Data Processing, Privacy-Enhanced Data Processing

58. Data Security Risk Assessment
A data security risk assessment is the process of identifying, analyzing, and evaluating potential threats to data security. It helps organizations understand their vulnerabilities and prioritize actions to mitigate security risks.

Related Terms: Risk Mitigation, Threat Assessment, Security Vulnerability Analysis

59. Secure Data Sharing Platform
A secure data sharing platform is a system or tool that facilitates the exchange of data while ensuring privacy and security. It enables organizations to collaborate on data projects without compromising data confidentiality.

Related Terms: Secure Data Exchange, Privacy-Preserving Collaboration Platform, Confidential Data Sharing

60. Privacy-Preserving Data Storage
Privacy-preserving data storage involves storing data