

International Data Transfers

Adequacy Decision refers to a decision made by the European Commission that a non-EU country has an adequate level of protection for personal data, allowing for the transfer of data from the EU to that country without the need for additional safeguards. Related terms include third-country transfers and data protection.

Anonymization is the process of transforming personal data into a de-identified form, making it impossible to link the data to an individual. Related terms include pseudonymization and data protection by design. Anonymization is a technique used to protect personal data, and it is often used in conjunction with other data protection measures.

Artificial Intelligence refers to the development of computer systems that can perform tasks that would typically require human intelligence, such as learning, problem-solving, and decision-making. Related terms include machine learning and data analytics. Artificial Intelligence is a key concept in the field of data science, and it has many practical applications in areas such as healthcare and finance.

Binding Corporate Rules refer to a set of data protection rules that are adopted by a multinational company to ensure the protection of personal data across all its subsidiaries and affiliates. Related terms include data protection policies and compliance programs. Binding Corporate Rules are a type of data transfer mechanism that allows companies to transfer personal data within their organization while ensuring that the data is protected.

Cloud Computing refers to the delivery of computing services over the internet, allowing users to access and store data remotely. Related terms include cloud storage and software as a service. Cloud Computing is a key concept in the field of information technology, and it has many practical applications in areas such as business and education.

Consent refers to the agreement of an individual to the processing of their personal data for a specific purpose. Related terms include data subject rights and privacy notices. Consent is a key concept in the field of data protection, and it is often required before personal data can be processed.

Cookie refers to a small text file that is stored on a user's device by a website, allowing the website to track the user's online activities. Related terms include tracking technologies and online advertising. Cookies are commonly used by websites to collect data about their users, and they can be used to deliver targeted advertisements.

Data Breach refers to the unauthorized access, disclosure, or loss of personal data. Related terms include

data security and incident response. Data Breach is a key concept in the field of data protection, and it can have serious consequences for individuals and organizations.

Data Controller refers to the entity that determines the purposes and means of the processing of personal data. Related terms include data processor and data protection officer. Data Controller is a key concept in the field of data protection, and it is often responsible for ensuring that personal data is processed in accordance with data protection laws.

Data Erasure refers to the process of permanently deleting or destroying personal data. Related terms include data minimization and data retention. Data Erasure is a technique used to protect personal data, and it is often used in conjunction with other data protection measures.

Data Minimization refers to the principle of collecting and processing only the minimum amount of personal data necessary to achieve a specific purpose. Related terms include data quality and data protection by design. Data Minimization is a key concept in the field of data protection, and it is often required by data protection laws.

Data Portability refers to the right of an individual to transfer their personal data from one organization to another. Related terms include data subject rights and interoperability. Data Portability is a key concept in the field of data protection, and it is often required by data protection laws.

Data Processor refers to the entity that processes personal data on behalf of a data controller. Related terms include data controller and data protection officer. Data Processor is a key concept in the field of data protection, and it is often responsible for ensuring that personal data is processed in accordance with data protection laws.

Data Protection by Design refers to the principle of designing systems and processes to protect personal data from the outset. Related terms include data protection by default and privacy by design. Data Protection by Design is a key concept in the field of data protection, and it is often required by data protection laws.

Data Protection Impact Assessment refers to the process of assessing the potential risks and impacts of processing personal data on individuals. Related terms include data protection officer and risk assessment. Data Protection Impact Assessment is a technique used to protect personal data, and it is often used in conjunction with other data protection measures.

Data Protection Officer refers to the individual responsible for ensuring that an organization complies with data protection laws and regulations. Related terms include data controller and compliance program. Data Protection Officer is a key concept in the field of data protection, and it is often required by data protection laws.

Data Subject refers to the individual whose personal data is being processed. Data Subject is a key concept

in the field of data protection, and it is often the focus of data protection laws.

Data Subject Rights refer to the rights of an individual to control their personal data, including the right to access, rectify, and erase their data. Related terms include data protection and privacy notices. Data Subject Rights are a key concept in the field of data protection, and they are often required by data protection laws.

Data Transfer Agreement refers to a contract between two organizations that outlines the terms and conditions for the transfer of personal data. Related terms include data protection and compliance program. Data Transfer Agreement is a type of data transfer mechanism that allows organizations to transfer personal data while ensuring that the data is protected.

Encryption refers to the process of transforming plaintext into unreadable ciphertext to protect personal data. Related terms include data security and access control. Encryption is a technique used to protect personal data, and it is often used in conjunction with other data protection measures.

European Data Protection Board refers to the independent body responsible for ensuring the consistent application of data protection laws across the EU. European Data Protection Board is a key concept in the field of data protection, and it plays a crucial role in ensuring that data protection laws are enforced.

General Data Protection Regulation refers to the EU regulation that outlines the rules and regulations for the processing of personal data. General Data Protection Regulation is a key concept in the field of data protection, and it is often required by data protection laws.

Information Commissioner's Office refers to the independent body responsible for enforcing data protection laws in the UK. Information Commissioner's Office is a key concept in the field of data protection, and it plays a crucial role in ensuring that data protection laws are enforced.

International Data Transfer refers to the transfer of personal data from one country to another. International Data Transfer is a key concept in the field of data protection, and it is often required by data protection laws.

Machine Learning refers to the development of computer systems that can learn and improve their performance on a task without being explicitly programmed. Related terms include artificial intelligence and data analytics. Machine Learning is a key concept in the field of data science, and it has many practical applications in areas such as healthcare and finance.

Personal Data refers to any information that can be used to identify an individual, including names, addresses, and online identifiers. Personal Data is a key concept in the field of data protection, and it is often the focus of data protection laws.

Pseudonymization refers to the process of transforming personal data into a de-identified form, making it difficult to link the data to an individual. Related terms include anonymization and data protection by

design. Pseudonymization is a technique used to protect personal data, and it is often used in conjunction with other data protection measures.

Right to be Forgotten refers to the right of an individual to have their personal data erased or removed from the internet. Right to be Forgotten is a key concept in the field of data protection, and it is often required by data protection laws.

Sensitive Personal Data refers to personal data that is considered sensitive or special, such as health data or financial data. Sensitive Personal Data is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Standard Contractual Clauses refer to a set of contractual clauses that are used to protect personal data when it is transferred from one organization to another. Standard Contractual Clauses are a type of data transfer mechanism that allows organizations to transfer personal data while ensuring that the data is protected.

Third-Country Transfer refers to the transfer of personal data from the EU to a non-EU country. Third-Country Transfer is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Transfer Impact Assessment refers to the process of assessing the potential risks and impacts of transferring personal data from one organization to another. Transfer Impact Assessment is a technique used to protect personal data, and it is often used in conjunction with other data protection measures.

UK General Data Protection Regulation refers to the UK regulation that outlines the rules and regulations for the processing of personal data. UK General Data Protection Regulation is a key concept in the field of data protection, and it is often required by data protection laws.

Vendor Management refers to the process of managing and overseeing the activities of third-party vendors who process personal data on behalf of an organization. Vendor Management is a key concept in the field of data protection, and it is often required by data protection laws.

Withdrawal of Consent refers to the right of an individual to withdraw their consent to the processing of their personal data. Withdrawal of Consent is a key concept in the field of data protection, and it is often required by data protection laws.

Workforce Management refers to the process of managing and overseeing the activities of employees who process personal data on behalf of an organization. Workforce Management is a key concept in the field of data protection, and it is often required by data protection laws.

Data Localization refers to the requirement that personal data be stored and processed within a specific country or region. Data Localization is a key concept in the field of data protection, and it is often subject to

additional protections and safeguards.

Data Residency refers to the requirement that personal data be stored and processed within a specific country or region. Data Residency is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Data Sovereignty refers to the concept that personal data is subject to the laws and regulations of the country in which it is stored and processed. Data Sovereignty is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Data Transfer Addendum refers to a document that outlines the terms and conditions for the transfer of personal data from one organization to another. Data Transfer Addendum is a type of data transfer mechanism that allows organizations to transfer personal data while ensuring that the data is protected.

Intra-Group Data Transfer refers to the transfer of personal data within a group of companies. Intra-Group Data Transfer is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Model Contractual Clauses refer to a set of contractual clauses that are used to protect personal data when it is transferred from one organization to another. Model Contractual Clauses are a type of data transfer mechanism that allows organizations to transfer personal data while ensuring that the data is protected.

Onward Transfer refers to the transfer of personal data from one organization to another, where the data is then transferred to a third organization. Onward Transfer is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Processor Binding Corporate Rules refer to a set of data protection rules that are adopted by a processor to ensure the protection of personal data when it is processed on behalf of a controller. Processor Binding Corporate Rules are a type of data transfer mechanism that allows processors to process personal data while ensuring that the data is protected.

Restricted Transfer refers to the transfer of personal data from one organization to another, where the transfer is restricted by data protection laws or regulations. Restricted Transfer is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Service Provider refers to an organization that provides services to a controller or processor, such as cloud storage or software as a service. Service Provider is a key concept in the field of data protection, and it is often required to comply with data protection laws and regulations.

Sub-Processor refers to an organization that processes personal data on behalf of a processor. Sub-Processor is a key concept in the field of data protection, and it is often required to comply with data protection laws and regulations.

Supervisory Authority refers to an independent body that is responsible for enforcing data protection laws and regulations. Supervisory Authority is a key concept in the field of data protection, and it plays a crucial role in ensuring that data protection laws are enforced.

Third-Party Auditor refers to an independent organization that audits an organization's data protection practices and procedures. Third-Party Auditor is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Transfer Mechanism refers to a method or procedure that is used to transfer personal data from one organization to another. Transfer Mechanism is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Transferred Data refers to personal data that is transferred from one organization to another. Transferred Data is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Vendor refers to an organization that provides goods or services to a controller or processor. Vendor is a key concept in the field of data protection, and it is often required to comply with data protection laws and regulations.

Vendor Risk Management refers to the process of managing and overseeing the activities of vendors who process personal data on behalf of an organization. Vendor Risk Management is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Workforce Data refers to personal data that is collected and processed by an organization about its employees. Workforce Data is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Data Privacy refers to the protection of personal data from unauthorized access, disclosure, or use. Data Privacy is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Officer Training refers to the training and education provided to data protection officers to ensure that they have the necessary skills and knowledge to perform their duties. Data Protection Officer Training is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Policy refers to a document that outlines an organization's policies and procedures for protecting personal data. Data Protection Policy is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Principles refers to the fundamental principles that underlie data protection laws and

regulations, such as transparency, fairness, and accountability. Data Protection Principles is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Security refers to the measures taken to protect personal data from unauthorized access, disclosure, or use. Data Security is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Subject Access Request refers to a request made by an individual to access their personal data that is held by an organization. Data Subject Access Request is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Transfer Agreement Template refers to a template document that outlines the terms and conditions for the transfer of personal data from one organization to another. Data Transfer Agreement Template is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

GDPR Compliance refers to the process of ensuring that an organization is compliant with the General Data Protection Regulation. GDPR Compliance is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Information Security refers to the measures taken to protect personal data from unauthorized access, disclosure, or use. Information Security is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

International Data Transfers refers to the transfer of personal data from one country to another. International Data Transfers is a key concept in the field of data protection, and it is often subject to additional protections and safeguards.

Personal Data Breach refers to the unauthorized access, disclosure, or loss of personal data. Personal Data Breach is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Privacy by Design refers to the principle of designing systems and processes to protect personal data from the outset. Privacy by Design is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Privacy Impact Assessment refers to the process of assessing the potential risks and impacts of processing personal data on individuals. Privacy Impact Assessment is a technique used to protect personal data, and it is often used in conjunction with other data protection measures.

Privacy Notice refers to a document that outlines an organization's policies and procedures for protecting personal data. Privacy Notice is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Processor Agreement refers to a contract between a controller and a processor that outlines the terms and conditions for the processing of personal data. Processor Agreement is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Pseudonymization Techniques refer to the methods and techniques used to transform personal data into a de-identified form, making it difficult to link the data to an individual. Pseudonymization Techniques are a key concept in the field of data protection, and they are often used in conjunction with other data protection measures.

Security Measures refer to the measures taken to protect personal data from unauthorized access, disclosure, or use. Security Measures is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Sub-Processing Agreement refers to a contract between a processor and a sub-processor that outlines the terms and conditions for the processing of personal data. Sub-Processing Agreement is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Supervisory Authority Guidance refers to the guidance and advice provided by supervisory authorities to organizations on how to comply with data protection laws and regulations. Supervisory Authority Guidance is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Third-Party Risk Management refers to the process of managing and overseeing the activities of third-party vendors who process personal data on behalf of an organization. Third-Party Risk Management is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Vendor Due Diligence refers to the process of evaluating and assessing the data protection practices and procedures of vendors who process personal data on behalf of an organization. Vendor Due Diligence is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Workforce Training refers to the training and education provided to employees on data protection and compliance programs. Workforce Training is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Loss Prevention refers to the measures taken to prevent the unauthorized access, disclosure, or loss of personal data. Data Loss Prevention is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection as a Service refers to the provision of data protection services to organizations, such as data protection officer services and data protection consulting. Data Protection as a Service is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Certification refers to the process of certifying that an organization's data protection practices and procedures comply with data protection laws and regulations. Data Protection Certification is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Framework refers to the overall structure and approach to data protection, including the policies, procedures, and controls in place to protect personal data. Data Protection Framework is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Governance refers to the overall management and oversight of an organization's data protection practices and procedures. Data Protection Governance is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Management refers to the process of managing and overseeing an organization's data protection practices and procedures. Data Protection Management is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Officer Role refers to the role and responsibilities of a data protection officer, including ensuring that an organization's data protection practices and procedures comply with data protection laws and regulations. Data Protection Officer Role is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Policy Template refers to a template document that outlines an organization's policies and procedures for protecting personal data. Data Protection Policy Template is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Principles for AI refers to the principles and guidelines for protecting personal data in the context of artificial intelligence and machine learning. Data Protection Principles for AI is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Protection Training refers to the training and education provided to employees on data protection and compliance programs. Data Protection Training is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Quality refers to the accuracy, completeness, and relevance of personal data. Data Quality is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Quality Management refers to the process of managing and overseeing the quality of personal data. Data Quality Management is a key concept in the field of data protection, and it is often required by data protection laws and regulations.

Data Retention refers to the period of time for which personal data is stored and retained. Data Retention is

a key concept in the field of data protection, and it is often required by data protection laws and regulations.