GDPR

Class: DataProtectionFrameworkAndPrinciples

Description: This class represents the basic framework and principles for data protection within the DYWIDAG organization. It defines the minimum standards and requirements for ensuring, monitoring, and maintaining an adequate level of personal data security.

Attributes:

- Transparency: Indicates that personal information is collected in a transparent way with the full cooperation and knowledge of interested parties.

- Data Collection Principles: Specifies the principles to be applied to personal data once collected, including accuracy, legitimate purposes, limited retention, fair and lawful processing, protection against unauthorized access, and relevance.

- Restrictions on Data Communication: Indicates that personal data will not be communicated internally without a purpose, and not transferred to organizations or countries without adequate data protection policies.

- Obligations towards Individuals: Specifies the obligations of each entity in the DYWIDAG Group towards individuals, including providing information about their processed data, data processing methods, and access to the information.

- Data Handling Provisions: Outlines provisions for handling lost, corrupted, or compromised data and allowing individuals to request modifications or erasure of their data.

- Measures for Data Protection: Lists various measures to ensure an adequate level of personal data protection, including access restrictions, transparent data collection procedures, employee training, secure networks, privacy breach reporting procedures, contract clauses or statements on data handling, and data protection best practices.

Class: PersonalDataProcessingPrinciples

Description: This class represents the main principles that apply when processing personal data. These principles enforce fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation and deletion, and data security.

Attributes:

- Fairness, Lawfulness, and Transparency: Personal data may only be collected and processed for specified, explicit, and legitimate purposes in a fair, transparent, and lawful manner. Data subjects must be informed about how their data is being handled, including the identity of the data controller, the purpose of data processing, and third-party recipients if applicable.

- Purpose Limitation: Personal data must only be collected and processed for the purpose defined before collection and should not be further processed in a way incompatible with those purposes.

- Data Minimization: Personal data must be restricted to what is adequate, necessary, and relevant for the purpose of processing. Data should not be collected in advance and stored for potential future purposes without appropriate consent or legal basis.

- Accuracy: Personal data on file must be correct, complete, and kept up to date. Steps should be taken to correct or update inaccurate or incomplete data.

- Storage Limitation and Deletion: Personal data should be retained only as long as necessary to achieve the intended purposes of collection and processing. After the expiration of legal or business process-related periods, data that is no longer needed must be securely deleted.

- Integrity and Confidentiality, Data Security: Personal data must be processed with adequate security measures to ensure data integrity and confidentiality. Technical and organizational security measures (TOM) must be in place to prevent unauthorized access, misuse, modification, or destruction of data.

Class: LawfulnessOfProcessing

Description: This class represents the lawful grounds for processing personal data. It outlines the legal bases on which DYWIDAG can process personal data in compliance with data protection regulations.

Attributes:

- Consent: Personal data can be processed based on the data subject's consent, obtained explicitly for specific purposes (e.g., job applicants submitting CVs, marketing newsletter).

- Contractual Obligation: Processing is lawful when it is necessary for entering into or fulfilling a contract with the data subject (e.g., employment contract).

- Legal Obligation: Data can be processed to comply with a legal obligation to which DYWIDAG and its affiliates (data controllers) are subject (e.g., social security and tax filings).

- Legitimate Interest: Processing may be carried out based on DYWIDAG's or the party's legitimate interest to whom the personal data is disclosed (e.g., storing user log files or IP addresses for network function and security).

- Vital Interests: Processing can be lawful for protecting the vital interests of the public and other stakeholders.

- Public Tasks and Obligations: Data processing may be permitted for fulfilling public tasks and obligations.

Class: DataSubjectRights

Description: This class represents the rights that data subjects have concerning their personal data, as well as the procedures for handling data subject access requests.

Attributes:

- Access to Personal Data: Data subjects have the right to request access to any personal data held about them by a data controller.

- Objection and Restriction: Data subjects can prevent, object to, or restrict the processing of their personal data, especially for direct marketing purposes.

- Amendment of Inaccurate Data: Data subjects can request the correction of inaccurate personal data.

- Information on Data Recipients: Data subjects have the right to request information about the identity of recipients or categories of recipients to whom their personal data has been transmitted (e.g., sub-contracted data processors).

- Data Deletion: Data subjects can request the deletion of their data if the processing has no legal basis or if the purpose for data processing is no longer applicable. However, legal retention periods may override this right, and compliance with such periods must be monitored.

Class: PersonalDataTransfersAndProcessingOnBehalf

Description: This class represents the principles and requirements related to personal data transfers within the organization (intra-group) and data processing on behalf of a data controller. It ensures compliance with applicable data protection laws and regulations.

Attributes:

- Intra-Group Personal Data Transmission: Represents the principles to be followed when transmitting personal data within the organization's entities.

- Data Processing on Behalf: Explains the concept of data processing on behalf of a data controller, where a processor carries out personal data processing according to the controller's instructions.

- Written Contract for EU Processing on Behalf: Specifies that any processing on behalf of data controllers within the EU must be governed by a binding written contract. The contract should outline the subject-matter, duration, nature, purpose, types of personal data, categories of data subjects, and the obligations and rights of the DYWIDAG entity acting as the controller (as per Article 28 of the EU GDPR).

- Data Protection Level for Recipients outside the EU: If personal data is transferred from a DYWIDAG entity (data controller) within the EU to a recipient (data processor) outside the EU, including intra-group transfers, the recipient must maintain a data protection level equivalent to this Data Protection Policy.

- Sufficient Guarantees for Data Processors: The data controller should use data processors that provide sufficient guarantees for implementing appropriate technical and organizational measures to meet the requirements of the data protection policy and protect the rights of data subjects.

Class: ConfidentialityOfProcessing

Description: This class represents the principles and obligations related to the confidentiality of personal data processing within the organization. It ensures that personal data is handled with strict confidentiality and access is limited to authorized individuals for legitimate purposes.

Attributes:

- Prohibition of Unauthorized Collection and Processing: Any unauthorized collection and processing of personal data by employees are strictly prohibited.

- Limitation of Data Processing to Authorized Duties: Employees are only allowed to process personal data as part of their legitimate duties and responsibilities.

- Need-to-Know Principle: Employees may have access to personal information only if it is necessary and appropriate for the specific tasks they are assigned to. This principle requires careful breakdown and separation of roles and responsibilities.

- Prohibition of Personal and Unauthorized Disclosure: Employees are prohibited from using collected personal data for private or commercial purposes or disclosing it to unauthorized individuals.

- Obligation to Inform Employees: Employers must inform their employees about the obligation to protect data secrecy at the start of the employment relationship. Employees should be made familiar with the data protection policy, and written confirmation of understanding may be required.

- Continuing Obligation: The obligation to protect data secrecy remains in force even after the employment relationship has ended.

Class: SecurityOfProcessing

Description: This class represents the principles and measures related to the security of personal data processing. It ensures that personal data is protected from unauthorized access, unlawful processing, accidental loss, modification, or destruction, regardless of the format in which data is processed.

Attributes:

- Safeguarding Personal Data: Personal data must be protected from unauthorized access, unlawful processing, and accidental loss, modification, or destruction.

- State-of-the-Art Security Measures: Security measures should be based on state-of-the-art and modern technologies, taking into account the risks of processing and the sensitivity of the data to be protected.

- Building and Office Security: Buildings and office rooms must be adequately protected against unauthorized access using measures such as alarm systems and entrance controls.

- Secure Storage of Data: Personal data should be stored securely using modern software that is kept up to date.

- Limiting Access: Access to personal data should be limited to authorized personnel, and appropriate security measures should be in place to prevent unauthorized sharing of information.

- Secure Data Transfer: Personal data should only be transferred using secured means, such as email/laptop encryption and encrypted USB sticks.

- Monitoring and Logging: Access to personal data should be monitored and logged, including audit trails for data entries and log trails.

- Data Availability and Recovery: Measures should be in place to ensure data availability and recovery, including backup and disaster recovery procedures, firewalls, and anti-virus programs.

- Secure Data Deletion: Personal data should be deleted securely to ensure irrecoverable deletion.

- Controls for External Data Processors: Adequate controls should be in place when personal data is outsourced to external data processors.

- Incident Reporting and Management: Security incidents, data breaches, and other incidents should be properly reported and managed.

Class: DataProtectionAwareness

Description: This class represents the importance of data protection awareness within the organization and outlines the responsibilities of management to promote data protection and data privacy among all employees who process personal data for DYWIDAG.

Attributes:

- Importance of Data Protection Awareness: Data protection awareness is crucial for the effectiveness of the DYWIDAG data protection organization to ensure compliance with data protection and privacy regulations.

- Duty of Management: The management of each DYWIDAG entity has the responsibility to promote data protection awareness among all employees involved in processing personal data.

- Regular Training: Management should organize regular data protection trainings for employees, at least on an annual basis.

- Corporate Awareness Programs: In addition to trainings, management should conduct corporate awareness and sensitization programs, which may include online training or other suitable methods.

- On-Site Trainings: On-site trainings can be used as part of the awareness program to provide hands-on and interactive learning experiences for employees.

Class: OrganizationalStructure

Description: This class represents the organizational structure for ensuring an adequate data protection level within all DYWIDAG entities. It outlines the roles and functions required for effective data protection implementation and compliance with applicable laws.

Attributes:

- Responsibility of Executive Management: The Executive Management of all DYWIDAG entities holds the responsibility for ensuring an appropriate data protection level and compliance with relevant laws throughout its affiliates.

- Roles and Functions:

  - Data Protection Coordinators (DPCs): DPCs are appointed by the local management of each entity and serve as on-site contact persons for data protection. They can perform checks and inform employees about the data protection policy.

  - Data Protection Officers (DPOs): DPOs are appointed where required by applicable law to oversee data protection activities. They ensure sufficient involvement and timely access to all processes related to personal data processing. DPOs can directly report to the Chief Compliance Officer and must maintain secrecy and non-disclosure as per applicable laws.