Policy name: Data Protection GDPR Policy
Owner: Radosław Bieliński
Approver: Radosław Bieliński
Approval date: 12.05.2020
Chief Compliance Officer review date: 12.05.2020

VERSION	AUTHOR	DESCRIPTION OF CHANGE	APPROVED BY
2020.06.16	Radosław Bieliński	Policies new naming system introduction	Radosław Bieliński

DYWIDAG
SAFER. STRONGER. SMARTER.

Contents

1. Introduction

Privacy is a fundamental right and its protection is important to our organization. DYWIDAG, as a global group, is therefore committed to comply with all the laws, rules and regulations related to Data Protection that its affiliates are governed by including, but not limited to, the General Data Protection Regulation ("GDPR").

DYWIDAG collects, stores and processes personal data relating to divers Data Subjects, such as its employees, job applicants, customers, suppliers and other third parties. The correct and lawful treatment of personal data shall be maintained with confidence and following the reputation of the DYWIDAG Group as a socially responsible business partner and employer.

This policy set out the requirements all those in scope must adhere and comprises the internationally accepted data privacy principles. Such requirements apply to all DYWIDAG's affiliates, its employees, contractors, temporary employees, and agency workers – including anyone we collaborate with or acts on our behalf and may need occasional access to data. The policy covers all processing activities involving personal data and will help you to recognize what may be personal data, as well as your rights and obligations with respect to such data.

DYWIDAG's Data Protection Policy either supplements the national data privacy laws or is applicable in the absence of national legislation. DYWIDAG's affiliates to which this policy does not directly apply due to existing governance rules (e.g. joint ventures) must implement their own policies and procedures based on their national legislation and requirements.

An infringement of relevant data privacy laws may cause enormous damage to DYWIDAG in the form of loss of reputation, severe fines and affect the trust of customers, employees, and the public as well as all other stakeholders. Therefore, we rely on you to follow the requirements set forth in this Policy.

2. Scope

The scope of this Policy covers:

- all processing activities involving personal and sensitive personal data where DYWIDAG acts as the Data Controller, including personal data in physical form stored in a relevant filling system
- all Employees, Contractors, Third Parties, Processors, or others who process Personal or Sensitive personal Data on behalf of the DYWIDAG Group
- all geographic territories, including Third Countries outside the European Union (EU). All DYWIDAG affiliates and its employees must process personal data with due diligence and in compliance with the statutory requirements and this policy.

In particular, for Entities and data processing activities that are subject to the GDPR, additional local guidelines and procedures are essential and must be developed and set up by local management or an appointed delegate for the compliance with the rules that have been enforced since May 2018 in addition to possible national law. Additional local policies and guidelines must also be developed by affiliates operating outside the European Union if this is necessary for compliance with their national legislation and data protection laws. DYWIDAG affiliates that have no national data protection laws must adopt and apply this policy.

If relevant national laws conflicts or has stricter requirements, they may override this policy. It is responsibility of the Entity's local Management to monitor the national data protection legislation and its development or amendments. In case amendments of national legislation conflict with this policy, this must be reported to Chief Compliance Officer.

3. Definitions

- "Personal data": any information relating to an identified or identifiable natural person, the so-called "data subject"
- "Data subject": an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an address, an identification number, any kind of location data, an online identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that natural person. Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, health and sexual life, criminal allegations or offences are considered sensitive and belong to special categories of personal data. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently.

Anonymized data and data not related to a natural person (e.g. company data such as company names and addresses) are not subject to this policy

- "Processing": of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- A "data controller": is "a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing of personal data"
- "Data processors": process personal data on behalf of a data controller (e.g. payroll agency hired for payroll accounting by DYWIDAG, who is the data controller)
- "Security breach": is any incident that results in unauthorized access of data, applications, services, networks and/or devices by passing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential, or unauthorized logical IT perimeter. A security breach is also known as a security violation and potentially ends up in a personal data breach
- "Data breach": is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data
- "Third Party" means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

4. Data Protection Framework and Principles

This section describes the basic framework and principles, defines the minimum standards and requirements of our data protection organization and is a guideline for ensuring, monitoring, and maintaining an adequate level of personal data security. Within the DYWIDAG organization, personal information is collected in a transparent way and only with the full cooperation and knowledge of interested parties. Once personal data have been collected, the following principles shall be applied:

Personal data and all processing activities will be

- recorded accurately and kept up to date
- collected for specified, explicit and legitimate purposes only
- retained only for as long as necessary and according to statutory retention period requirements
- processed fairly and lawfully
- protected against any unauthorized or illegal access and misuse by internal or external parties
- adequate, relevant, and limited to what is necessary.

They will not be:

- communicated internally without a purpose
- transferred to organizations (and affiliates), states or countries that do not have adequate data protection policies and regulations.

In addition to ways of handling the data, each entity in the DYWIDAG Group has direct obligations towards individuals to whom the data belongs. Specifically, on their request, we must inform a) which of their data is processed, b) how we process such data and c) who has access to the information.

We must also

- have provisions in cases of lost, corrupted or compromised data
- allow individuals to request that we modify, erase, reduce or correct data contained in our databases.

For ensuring an adequate level of personal data protection we are committed to:

- Restrict and monitor access to personal data, specially to sensitive personal data

- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses whenever considered as necessary or communicate statements on how we handle data
- Establish data protection best practices (access controls to buildings, offices and IT systems, document shredding, secure locks, devices and data encryption, frequent backups, access authorization, disaster recovery plans etc.)

Those principles are further described in the below sections of this policy.

4.1 Main Principles for Processing of Personal Data

When processing personal data, the following enforceable principles apply:

- Fairness, lawfulness, and transparency: personal data may only be collected and processed for specified, explicit and legitimate purposes in a fair and transparent manner and in compliance with the applicable law. The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of a) the identity of the data controller b) the purpose of data processing and c) third parties or categories of third parties to whom the data might be transmitted
- Purpose limitation: personal data may only be collected and processed for the purpose that was defined before the collection, limited to what is necessary in relation to the purposes for which they are processed and may not be further processed in a way incompatible with those purposes
- Data Minimisation: personal data must be restricted to the adequate, necessary, and relevant extent to achieve the purpose for its processing. Personal data must not be collected in advance and stored for potential future purposes unless the Data Subject has given consent or is required or permitted by national law
- Accuracy: Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented, or updated

- Storage Limitation and Deletion: personal data must be maintained in a manner only as long as this is required to achieve the intended purposes of collection and processing. After the expiration of legal or business process-related periods, Personal Data that is no longer needed must be securely deleted
- Integrity and Confidentiality, Data Security: personal data must be processed in a manner that a) ensures adequate security of the data; b) data is stored securely using suitable, modern systems and software that is kept-up-to-date.

Adequate Technical and Organizational Security Measures (TOM - e.g. such as access controls, password rules, physical security of servers, back-up guidelines, etc.) must be in place and formally described by all our Entities to prevent unauthorized or illegal access and misuse, processing or distribution, as well as accidental loss, modification or destruction.

The adherence to those principles must be supported by a record of (IT) systems and processing activities where all information and procedures related to personal data are documented (e.g. category of data subject, category of Personal Data, purpose of processing) . All Entities must keep such Record of Processing Activities, specially the Entities with processing activities subject to the GDPR (Art. 30 GDPR).

4.2 Lawfulness of Processing

DYWIDAG must ensure processing is lawful and document the lawful grounds of processing. For personal data to be processed lawfully, it must be processed based on one of the following legal grounds:

- The data subject's consent to the processing (e.g. from job applicants submitting CVs, Marketing Newsletter)
- The processing is necessary for entering in to or for the fulfilment of a contract with the data subject (e.g. employment contract)
- For the compliance with a legal obligation to which DYWIDAG and its affiliates (the data controllers) is subject to (e.g. social security and tax filings)

- For the legitimate interest of DYWIDAG or the party to whom the personal data is disclosed (e.g. user log files or IP addresses may be temporarily stored, and this is justified to assure proper network function and security)
- For the vital interest of the public and other stakeholders
- For public tasks and obligations.

The processing of special categories of personal data must be expressively permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties regarding employment law. The employee may also expressively consent to processing.

Except for storage, processing shall cease immediately where there are no longer lawful grounds.

4.3 Rights of Data Subjects

Upon a data subject's request, the concerned Entity must inform them of the collected personal data within the scope of the applicable laws. In general, data subjects may:

- request access to any personal data held about them by a data controller
- prevent, object, or restrict the processing of their personal data, e.g. for direct marketing purposes
- ask to have inaccurate personal data amended
- request information on the identity of the recipient or the categories of recipients if their personal data have been transmitted to third parties (e.g. sub-contracted data processors)
- request their data to be deleted if the processing of such data has no legal basis, or if the legal basis no longer applies. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Legal retention periods might override this right and must be closely monitored.

If you received any Data Subject Access request, please contact Chief Compliance Officer immediately. Such request shall be completed as soon as possible but no more than 30 calendar days and communicated to the Data Subject securely.

4.4 Personal Data Transfers and (Contract) Data Processing on Behalf

Intra-group personal data transmission or personal data "Processing on Behalf" of a data controller must be based on the principles stated in sections 4.1 to 4.3 and be in compliance with the applicable laws and statutory data protection requirements of the relevant country.

"Data Processing on Behalf" means that a Processor is carrying out processing of personal data on behalf and according to instructions of a Controller, who determines the purposes and means of the processing of personal data. In other words, a Processor is hired by the data controller as a data processor to process personal data (e.g. outsourcing of payroll administration, outsourcing of the IT servers to a hosting/cloud provider).

"Processing on behalf" activities within the EU shall not be outsourced without a binding written contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of Data Subjects and the obligations and rights of the DYWIDAG Entity acting as Controller (Article 28 EU GDPR). In the event that personal data is transmitted from a DYWIDAG Entity (data controller) within the EU to a recipient (data processor) outside the EU (including intra-group transfers), this recipient must agree to maintain a data protection level equivalent to this Data Protection Policy.

The controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this policy and ensures the protection of the rights of the data subject.

4.5 Confidentiality of Processing

Any kind of personal data is subject to data secrecy, therefore:

- any unauthorized collection and processing of such data by employees is prohibited
- any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is prohibited.

The “need to know” principle applies: employees may have access to personal information only as this is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation of roles and responsibilities.

The employees´ use of our collected personal data for private or commercial purposes or their disclosure to unauthorized persons is prohibited; employers must inform their employees at the start of the employment relationship about the obligation to protect data secrecy and make them familiar with this policy (e.g. by requiring written confirmation of this policy). This obligation shall remain in force even after employment has ended.

4.6 Security of Processing

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. This applies regardless of whether data is processed electronically or in paper form. Those technical and organizational security measures must be based on the state-of-the-art and modern technologies, the risks of processing, and the sensitivity of the data to be protected. In general, each DYWIDAG and all affiliates must make sure that:

- buildings and office rooms are adequately protected against unauthorized access (e.g. alarm systems, entrance controls and registering)
- personal data is stored securely using modern software that is kept-up to date
- access to personal data is being limited only to personnel who need access and appropriate security measures are in place to avoid unauthorised sharing of information
- personnel data is transferred only by secured means (e.g. email/laptop encryption, encrypted USB sticks)
- access to personal data is monitored and protocolled (e.g. audit trails for data entries, log trails)
- availability and recovery of data (back-up and disaster recovery procedures, firewalls, anti-virus programs)
- when personal data is deleted, this is done securely in a way the deletion is irrecoverable
- adequate controls are in place when personal data are outsourced to an external data processor
- security incidents /data breaches and any other incidents are properly reported and managed.

Technical and organizational must be defined and implemented before the introduction of new methods of personal data processing, particularly of new IT systems and applications. They must be continuously evaluated and assessed in respect of technical developments and organizational changes.

4.7 Data Protection Awareness

The effectiveness of the DYWIDAG data protection organization requires that all affiliates and all their employees who process personal data for DYWIDAG must be aware of the importance of data protection and data privacy.

Therefore, the management of each DYWIDAG Entity has the duty to promote this awareness to all employees processing personal data, for example, by regular, but at least annual data protection trainings, corporate awareness and sensitization programs in the form of online training or other suitable methods (e.g. on-site trainings).

4.8 Organizational Structure

The Executive Management of all DYWIDAG's Entities is responsible for ensuring an appropriate data protection level that complies with all applicable laws throughout its affiliates and enables the implementation of an adequate data protection organization.

For ensuring an adequate data protection level and enforcement of this policy, the implementation of the following roles and functions is required:

- Data Protection Coordinators ("DPCs") must be appointed by the local Management of each Entity. The data protection coordinators are the contact persons on site for data protection. They can perform checks and must inform the employees with the content of this data protection policy
- Data Protection Officers ("DPOs") where required by the applicable law.

National legal requirements may define additional roles and tasks. The Regional and/or Local Management of an Entity ensures that DPOs and DPCs:

- are sufficiently involved and in due time in all matters relating to the protection of personal data
- obtain access to all processes concerning the processing of personal data
- can directly report to the Chief Compliance Officer
- are obliged to secrecy and non-disclosure regarding their activities in compliance with the applicable laws.

The DPCs and DPOs may perform other tasks, duties, and functions if these do not constitute a conflict of interest regarding their activity as a DPC or DPO. The DPCs and DPOs may be appointed for several Entities of a region or a country if such an appointment is does not constitute a conflict of interest.

4.9 Data Protection Incidents

The following data protection-relevant incidents must be promptly reported by the regional or the local Management of an Entity to their local DPCs and/or DPOs in charge as well as to the Chief Compliance Officer and to the Legal Department:

- Any reported, anticipated, or potential data breach (e.g. E-mail sent to the wrong recipients, personal data disclosed to unauthorized persons, a security breach usually results into a data breach)
- data protection complaints, claims and accusations by data subjects (e.g. employees, customers, suppliers)
- data protection requests by any data subject (e.g. customer asking for processing activities of their personal data)
- violations or potential violations of data protection laws, as well as violation of this Data Protection Policy
- fines imposed by data protection authorities
- audits advised by data protection authorities
- Any security breaches or incidents of IT systems (e.g. compromised systems, system breakdowns, hacking attempts, intrusion of systems, unauthorized access attempts) that might result into a data breach.

The loss or theft of mobile devices (laptops, mobile phones, tablets, USB sticks) might result into a potential data breach and therefore have also to be reported to the local DPC/DPO, Chief Compliance Officer and to the Global Head of IT.

In addition to that, local Management must:

- maintain a record of all incidents and events mentioned above
- maintain all relevant documents, communication and measures taken related to those incidents and requests in a separate file and have it available on request

All appointed DPOs and DPCs as well as any subsequent changes must be reported with all their contact details to Chief Compliance Officer and/or Group Legal Department.

5. Responsibilities and Duties, Audit

Group and local Management staff is responsible for ensuring that all relevant organizational, HR, and technical measures are in place so that any personal data processing is carried out in accordance with national data protection laws. The adherence and compliance with those requirements are the responsibility of all relevant employees.

All DYWIDAG employees (including temporary employees and lease staff), executives and service providers who process personal data on DYWIDAG's premises, use DYWIDAG's data processing systems and equipment or are connected thereto are obliged to comply with this policy.

Group Internal Audit will periodically review the compliance with this Data Protection Policy by on-site or remote data protection or/and IT security reviews or similar assessments. Performing this task, Group Internal Audit is authorized to hire external auditors or experts of this area.