Data Protection Policy

Company:	Process:	Document type:	Author:
Hoval	Compliance	Management guidelines	elleta AG, Frick Claudio

Table of contents

1 Subject-matter and objectives (Sect. 1 GDPR) 2
2 Material scope (Sect. 2 GDPR) 2
3 Territorial scope (Sect. 3 GDPR) 2
4 Principles (Sect. 4 GDPR) 2
5 Principles relating to the processing of personal data (Sect. 5 GDPR) 2
5.1. Legality of data processing (Sect. 6-11 GDPR) 3
5.2 Fairness and transparency (Sect. 12 GDPR) 3
5.3 Purpose of processing & data minimisation (Sect. 5 GDPR) 4
5.4 Accuracy (Sect. 5 GDPR) 4
5.5 Storage limitation (Sect. 5 GDPR) 4
5.6 Integrity and confidentiality (Sect. 5 GDPR) 4
6 Data protection organisation and responsibilities within the Hoval Group 4
6.1 Responsible for processing principles (Sect. 5 GDPR) 4
6.2 Responsibility for the processing activity (Sect. 5 GDPR) 4
6.3 Data Protection Officer (Sect. 37-39 GDPR) 5
6.3.1 Organisation 5
6.3.2 Contact procedure 5
6.3.3 Tasks of the Data Protection Officer (Sect. 39 GDPR) 5
7 Obligations of data controllers for processing (Sect. 24 GDPR) 6
7.1 Data protection risk management (Sect. 24 GDPR) 6
7.2 Data protection by design and by default (Sect. 25/35-36 GDPR) 6
7.3 Controllers and processors (Sect. 26-29 GDPR) 7
7.4 Records of processing activities (Sect. 30 GDPR) 7
7.5 Security of processing (Sect. 31 GDPR) 7
7.6 Assessment of the transfer of personal data and the provisions and regulations governing the basis for the transfer of data to third countries or international organisations (Sect. 44-49 GDPR) 8
8 Rights of the data subjects (Sect. 13-14 GDPR) 8
8.1 The right to information 8
8.2 Data subjects' rights (Sect. 15-22 GDPR) 8

Data Protection Policy

1 Subject-matter and objectives (Sect. 1 GDPR)

This data protection policy (hereinafter policy) regulates the handling and protection of personal data and their processing within the Hoval Group: the policy serves to clarify and explain the provisions of the General Data Protection Regulation at European level (Regulation (EU) 2016/679, GDPR).

2 Material scope (Sect. 2 GDPR)

This policy applies to the manually and wholly or partly automated processing of personal data within the Hoval Group stored in a file system or physically processed or maintained in a systematic collection. The regulations, therefore, apply to automated processing as well as to the manual processing of personal data. Examples of such processing activities may be:

- Processing of applicant data for recruitment purposes
- Processing of employee data for personnel administration
- Processing of customer data for marketing purposes
- Processing of customer data for product improvement
- Processing of customer data for service improvement

Excluded from the scope of the regulation are:

- Records or collections of files or folders that are not sorted according to specific criteria, whereby personnel files that are systematically and equally sorted do not fall under this exception
- Data processed by natural persons (employees) of the Hoval Group exclusively for personal or family activities
- Data of deceased persons, unless otherwise regulated by national law
- Anonymised personal data
- Data of legal persons

3 Territorial scope (Sect. 3 GDPR)

This policy applies to the entire Hoval Group and the processing activities of personal data carried out within it.

If necessary, this policy can be enhanced and supplemented by national directives or other laws or regulations. These must be submitted in advance to the Hoval Group's data protection officer for review and approval.

4 Principles (Sect. 4 GDPR)

Personal data referred in this policy means: Any information relating to an identifiable or identified natural person. These include for example: Name, contact, address, date of birth, employee abbreviations, personal number, social security number, customer number, online identification, e-mail, pictures as well as personal data (for example, cultural origin, political, religious and philosophical beliefs, health, sexuality) and/or combinations thereof.

Anonymous data is therefore not considered as personal data.

Processing: 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 of personal data.

The controller of processing: The Management Board of Hoval Group as well as the Management Board of the Hoval subsidiaries (hereinafter management) is responsible for data protection compliance requirements for the processing of personal data. The individual processing activities give rise to the responsibility of the Hoval Group and the individual Hoval subsidiaries. For each processing operation, a record shall be kept of who is responsible for the processing operation or whether more than one person is responsible for the operation (hereinafter process owner). The term controller contains management as well as process owner.

5 Principles relating to the processing of personal data (Sect. 5 GDPR)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation

- Accuracy
- Storage limitation
- Integrity and confidentiality

5.1. Legality of data processing (Sect. 6-11 GDPR)

For each processing of personal data, the controller documents the lawfulness of processing in the record of processing activities.

The legal bases are conclusively enumerated in the GDPR. In individual cases, a single assessment may be necessary for each processing activity by the legal department. Without any claim to general validity or completeness for better understanding we list examples that elaborate on the principles.

First,

on the basis for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract.

Example: Employment contract and hiring procedure, a service contract with a customer, license agreement and usage agreements with end customers

Second,

for compliance with a legal obligation.

Example: Reporting of social security data to the authorities, processing of children's data to obtain child benefits, processing of personal data to meet legal retention periods

Third,

to safeguard the legitimate interests pursued by the Hoval Group, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Example: For the purpose of direct advertising for existing customers, passing on personal data within the Hoval Group for administrative and support purposes, to guarantee availability, authenticity, completeness and confidentiality of stored or transmitted personal data as well as for the security of related services or even if the processing is necessary for asserting or defending legal claims

Fourth,

should none of the legal basis listed apply, the data subject's consent must be obtained. In the case of the processing of special categories of data, the consent must be explicit.

Example: After employment and without any further legal obligations - such as the storage of documents for the defence against legal claims - application documents of rejected candidates must be deleted. For further processing (storage for future job vacancies, for example) the rejected applicant's consent must be obtained.

Example: When sending a newsletter to interested parties (non-customers) a prior consent is usually required.

If there is no legal basis for processing, the processing is illegal, and the personal data may not be processed. If the expiry of a legal basis is already known, this expiry period must also be included as a storage limitation.

Example: Processing applicant data after filling a job vacancy:

Legal basis: (Legal obligation) and, in the event of the applicant's rejection, the legal obligation under the Equality Act (in Germany) and to defend any legal claims, deadline: 6 months after filling the job vacancy.

5.2 Fairness and transparency (Sect. 12 GDPR)

Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are processed and for what purpose, etc.. The principle of transparency requires that the controller gives the relevant information concerning the processing of personal data to the data subject.

5.3 Purpose of processing & data minimisation (Sect. 5 GDPR)

The purpose of processing is a central principle which determines what data are required and may be processed for this specified purpose. Several simultaneous purposes are also permitted.

Example: Customer data for customer administration and to meet the legal retention period for business records

It is therefore in principle not permitted to process the collected and processed data for another purpose without justification.

This also includes the principle of data minimisation, namely that only data which are needed for the fulfilment of the purpose and for which there is legitimacy may be collected and processed. Data must be handled sparingly, both concerning the amount of data and access to it.

5.4 Accuracy (Sect. 5 GDPR)

If personal data is used, they must be factually correct concerning the processing purpose.

5.5 Storage limitation (Sect. 5 GDPR)

The storage limit describes a time limit for processing. Once this limitation has expired, the Hoval Group ceases processing the data, for example by deleting or by pseudonymisation this.

Example: Personal data of customers is deleted or made anonymous after a certain period has elapsed after the end of a business relationship

5.6 Integrity and confidentiality (Sect. 5 GDPR)

Processing must ensure adequate safeguards of personal data. For this purpose, appropriate technical and organisational measures must be taken to ensure integrity and confidentiality of the data. Further information on this subject can be found in the "Safety of processing" section.

6 Data protection organisation and responsibilities within the Hoval Group

6.1 Responsible for processing principles (Sect. 5 GDPR)

The Hoval Group Management Board is responsible for setting and complying with the Hoval Group's data protection regulations.

The Hoval Group Management Board may delegate their duties, such as compliance with the principles of processing, the obligations and rights of the controller, security of processing and safeguarding the exercise of the rights of data subjects, within the organisation.

The delegation does not release the Hoval Group Management Board from overall responsibility, but merely allows the actual implementation of the requirements within the Hoval Group at the operational level. The responsibilities within the Hoval Group are reported to the Data Protection Officer by the Executive Board or the divisional officers and documented by him/her.

6.2 Responsibility for the processing activity (Sect. 5 GDPR)

Each owner of a processing activity (process manager, line manager) is responsible for compliance with the data protection requirements in his or her own area and is required to provide and disclose the necessary information to the Data Protection Officer and to provide support in monitoring compliance with the internal data protection requirements and the GDPR or legal obligations.

This responsibility is documented and is also recorded in the record of processing activities.

6.3 Data Protection Officer (Sect. 37-39 GDPR)

6.3.1 Organisation

The Hoval Group appoints a group-wide Data Protection Officer at the designated headquarters.

The Data Protection Officer is a member of the Hoval Group's staff and is appointed due to his/her professional qualities and, in particular, expert knowledge of data protection law and practices. To be able to process the various inquiries and topics of the group of companies, the Data Protection Officer is supported by additional persons in a data protection team (DPT).

The Data Protection Officer (DPO) is supported locally in the subsidiaries by local, national contact persons who handle data protection issues as part of their compliance activities.

To fulfil the respective tasks, the Hoval Group provides the Data Protection Officer, his or her team and the national contact person with the necessary resources and the required access to personal data and processing operations in his or her area of responsibility.

The Data Protection Officer is independent in his duties and deliberations and reports directly to the highest management level of the Hoval Group.

If the Hoval Group's Data Protection Officer is a member of the management or in a managerial position, it must be guaranteed that there is no conflict of interest. In this case Hoval Group's data protection organisation is subject to independent external auditing on a regular basis, but at least once a year.

6.3.2 Contact procedure

The Data Protection Officer and his team can effectively communicate with those affected by the provisions of the data protection rules and to cooperate efficiently with the supervisory authorities. The communication language is that of the data subject or the supervisory authority if possible in German or English.

The data protection officer’s contact details, possibilities and communication channels with the data protection officer and his or her team are reachable are communicated in the intranet in a way that is easy to find for all employees.

For external contact, the data protection officer's contact details are displayed on the available websites, homepages etc. and communicated to the supervisory authority.

6.3.3 Tasks of the Data Protection Officer (Sect. 39 GDPR)

The Data Protection Officer performs his duties in an advisory capacity.

The duties of the Data Protection Officer are his responsibility, but the performance of which can be delegated to other persons on a regular or on an individual basis. The Data Protection Officer remains responsible and accountable if he/she makes use of such a delegation.

Specifically, the Data Protection Officer carries out the following tasks, although these tasks are not exhaustive:

Advice and supervision:

- The application of risk management to assess the risks associated with existing processing activities for the persons concerned
- To carry out a data protection check before processing (data protection by design and by default)
- Appoint joint data controllers and define their contractual obligations
- Monitoring of current and future processors
- Test suitable technical and organisational measures to ensure safeguards of processing.
- Advising on data protection impact assessments and, where required, consult with the supervisory authorities
- Examines the safeguards and the rules and regulations governing the transfers of personal data to third countries or international organisations.
- To inform the Hoval Group, contractors and employees how to comply with the regulation.
- To make aware and train employees involved in the processing operations
- Keeping a record of processing activities based on declarations and notifications made by those responsible for processing

For this purpose, he/she draws up instructions, templates and processes with group-wide and local validity on behalf of the responsible persons, if necessary together with specialist contacts.

He/she is responsible for monitoring and verifying compliance with the regulation and the directives issued by the Hoval Group through regular audits. Within the scope of this monitoring obligation, the Data Protection Officer is notably authorised to

- collect information to identify data processing activities
- analyse and monitor compliance with the requirements for data processing activities
- inform and advise the responsible person and to make recommendations to him/her.

Besides, the Data Protection Officer supports the group of companies in the following tasks:

- Reporting breaches of the protection of personal data to the supervisory authorities and the role of the regulatory liaison officer
- Coordinating the notification of persons affected by the violation of the protection of personal data

If the controller does not comply with the recommendations of the Data Protection Officer or if he does not agree with them, this must be justified and recorded by the Data Protection Officer.

7 Obligations of data controllers for processing (Sect. 24 GDPR)

7.1 Data protection risk management (Sect. 24 GDPR)

The Hoval Group maintains a central risk management system for assessing compliance with data protection objectives:

- Lawfulness, fair processing and transparency
- Purpose limitation
- Data minimisation/ data economy
- Limited storage periods (obligation to erase)
- The accuracy of the personal data
- Non-identifiability (profiling)
- The possibility of recourse (rights of the data subject)
- Availability
- Confidentiality
- Integrity
- The resilience of processing system
- Ability to restore the availability and access to personal data

To consider the overall data protection risks associated with the respective processing activities, the cooperation and feedback from specialists and information security officers are necessary. The implementation and verification of compliance with the protection goals and the risk assessment are outlined separately in a directive for the employees commissioned with this task.

7.2 Data protection by design and by default (Sect. 25/35-36 GDPR)

When redesigning, adapting or cancelling a basis for a processing activity, such as updating an application, contracting a processor, extending the amount of personal data to be processed, etc., the data protection officer must be involved at an early stage during the planning phase in order to guarantee data protection by default and by design.

If in principle, the adjustment does not result in a data protection appropriate modification of the existing processing activity, the inclusion of the Data Protection Officer is not necessary.

> *Examples: Data protection relevance: The authorisation concept is changed. Mostly not data protection relevant: An authorisation is granted or withdrawn on basis of an existing concept*

The amendment is therefore exemplary:

- The change of purpose

- The modification of data types and categories, also by a new edition of a checklist
- Amendments to legal basis and obligations
- Adding or removing internal or external recipients or transmitting data to or from third countries
- The regular preparation of evaluations
- The change in systems used to process data
- Consulting or modifying a data processor relationship (supplier)

Without the Data Protection Officer's examination and, if necessary, the implementation of the recommended technical and organisational measures, a processing activity may not be implemented or mutated. The Data Protection Officer shall document the results of the risk assessment and any technical and organisational steps that may be taken and, if necessary, update the list of processing activities.

The process description and the procedure can be seen in a separate instruction/description.

7.3 Controllers and processors (Sect. 26-29 GDPR)

Where processing of personal data is currently or in future processed on behalf of the controller by a processor, a clear distinction must be made as to whether these external parties act as; joint controllers, processors or other third parties. This also applies to the group-wide internal data exchanges between the subsidiaries or the parent company and the subsidiaries. Typically, such a question arises in the context of outsourcing and support services or cooperation with external partners.

Example: A recruiting company is commissioned to fill a job vacancy. Here, it must be agreed who is responsible for which processing steps in the candidate's recruiting and onboarding.

Example: In the area of personnel administration, the external support of a consultant is regularly used to map the processes in the ERP system, he/ she receives regular and targeted access to employee data.

If the controller wishes to receive assistance from a processor, he/ she shall inform in advance the Data Protection Officer. With his support, similar to the data protection by design process, it is determined beforehand which guarantees are to be obtained and, if necessary, which measures to comply with the data protection regulations are to be implemented.

The Data Protection Officer will record the results in the record of processing activities and shall document the recipients and processors.

7.4 Records of processing activities (Sect. 30 GDPR)

The Data Protection Officer, assisted by those responsible for processing activities and local contact persons, keeps a group-wide record of processing activities relevant to data protection following the substantive requirements of the General Data Protection Regulation.

This list of processing operations will be reviewed on an annual basis or a case-by-case basis, whenever processing activities are changed. Upon request of the respective subsidiaries or branches, the Data Protection Officer will provide a record extract. The record is available in German or English.

The list of processing operations also contains essential results of the risk assessment from the appliedtechnical and organizational measures.

7.5 Security of processing (Sect. 31 GDPR)

The security of the processing activity is covered by the Hoval Group's information security management and the Hoval Group's information classification. In this classification, the Hoval Group distinguishes between public, internal and confidential data. Due to the data types and categories processed, personal data can be assigned either to the confidential and internal level.

Risk management of processing security is carried out responsibly by the Hoval Group's Information Security Officer. The Data Protection Officer assesses the results of risk management from the point of view of data protection objectives.

7.6 Assessment of the transfer of personal data and the provisions and regulations governing the basis for the transfer of data to third countries or international organisations (Sect. 44-49 GDPR)

If a transfer of personal data to a third country (except for the EU/EEA) or to an international organisation is planned or performed, the Data Protection Officer will, together with the contact person responsible for the processing activity, establish the basis of the transfer, this may be based on an EU adequacy decision, the existence of further guarantees such as standard contractual clauses or the existence of exceptional cases.

Transmission to third countries must be verified by the Data Protection Officer before transmission.

Examples of such a transfer include the use of plug-ins on the website, the transfer of data to Switzerland, the use of cloud services in third countries or the transfer of personal data to a branch of the Hoval Group in third countries.

8 Rights of the data subjects (Sect. 13-14 GDPR)

8.1 The right to information

The controller is required to inform the data subjects transparently at the point of data collection about the processing.

The information is concise, transparent, intelligible and in easily accessible form, using clear and plain language.

The controller shall involve the Data Protection Officer in the measures taken to fulfil the information duties, who will support and advise him/her in this regard, to achieve a uniform procedure.

Example: Visitors to the Hoval Group's website must be informed in a data protection declaration about the details of the processing activity following the information requirements of the regulation.

8.2 Data subjects' rights (Sect. 15-22 GDPR)

For each of the data subject's rights and safeguards, detailed procedures for the implementation and enforcement of the rights of the data subject will be formulated.

In principle, it should be noted that to safeguard the rights of the data subjects, the Data Protection Officer should, in any case, be consulted, for example, to inform other recipients of the personal data.

The rights of the data subjects shall include:

- Right to be informed where personal data are collected
- Right of rectification / completion
- Right to erasure
- Right to restrict the processing (both regarding content and time)
- Right to data portability
- Right to object

Example: A customer wants to know which data is processed within the scope of his service relationship. He addresses this concern to his contact person in the company. The latter shall inform the Data Protection Officer promptly of the request, and jointly they reply to the request in accordance with the internal policy.