# Company Privacy Policy

## Information about the controller and the data protection officer:


**Data Controller**

Humanizing Technologies GmbH

In der Trift 1
57462 Olpe
Germany
contact@humanizing.com
+ 49 (0) 221 71 59 75 75

www.humanizing.com

**Data Protection Officer**

DataCo GmbH

Dachauer Str. 65
80335 Munich
Germany
datenschutz@dataguard.de
+49 (0) 89 41207033

www.dataguard.de

HUMANIZING
TECHNOLOGIES

## I. Scope of application and objectives of this corporate guideline

This directive provides a binding basis for handling personal data within the company in a manner that complies with data protection requirements. The implementation of this directive is intended to protect the fundamental rights and freedoms of the persons concerned and to ensure a level of data protection appropriate to the risk. The primary objective is to ensure that all actions of the company that are relevant to data protection comply with the applicable data protection provisions (in particular the General Data Protection Regulation and the Federal Data Protection Act).

This policy applies to the entire company and all companies affiliated with the company that are economically managed by the company or in which the company holds a direct or indirect interest of more than 50%.

The provisions of this Policy apply to all employees and officers of the Company. The policy is handed out to each employee at the beginning of the employment relationship and can be accessed in the company's internal system at any time.

This Directive applies to all operations involving the processing of personal data of natural or legal persons. It is irrelevant whether the processing of personal data is carried out electronically or in paper form.

The provisions of this Policy supplement, but do not replace, the applicable data protection legislation. In the event of a conflict or discrepancy between the applicable data protection regulations and the provisions of this Policy, the applicable data protection regulations shall prevail.

Changes to this policy are only possible with the approval of the data protection officer. Deviating regulations made by the company or affiliated companies are not permitted.

The determination of when this policy will be put into effect is the responsibility of management.

## II. Definitions

This policy is based on the following definitions:

**Personal data** means any information relating to an identified or identifiable natural person (hereinafter "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 identification number, 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.

**Special categories of personal data** include any information about a natural person's racial or ethnic origin, religious or philosophical beliefs, political opinions, possible trade union membership, genetic or biometric data, health, or sexual orientation or life.

**Processing of personal data** means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Data subjects** are natural persons whose personal data are processed.

**Profiling** means any kind of automated processing of personal data that consists in using such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or change of location.

**Pseudonymization** means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures which ensure that the personal data are not attributed to an identified or identifiable natural person.

**File system** means any structured collection of personal data accessible according to specific criteria, whether such collection is maintained centrally, decentrally or according to functional or geographical criteria.

**Controller** means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its designation may be provided for under Union or Member State law.

**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**Recipient** means a natural or legal person, public authority, agency or other body to whom personal data are disclosed, whether or not a third party. However, public authorities that may receive personal data in the context of a specific investigation mandate under Union or Member State law shall not be considered as recipients; the processing of such data by the aforementioned authorities shall be carried out in accordance with the applicable data protection legislation, in accordance with the purposes of the processing.

**Third Party** means any natural or legal person, public authority, agency or other body, other than the Data Subject, the Controller, the Processor and the persons authorized to process the Personal Data under the direct responsibility of the Controller or the Processor.

**Data subject's consent** means any freely given specific, informed and unambiguous indication of his or her wishes in the form of a statement or other unambiguous affirmative act by which the data subject signifies his or her agreement to the processing of personal data concerning him or her.

**Personal data breach** means a breach of security resulting in the destruction, loss, or alteration, whether accidental or unlawful, or unauthorized disclosure of or access to personal data transmitted, stored, or otherwise processed.

**Health data** means personal data relating to the physical or mental health of a natural person, including the provision of health care services, revealing information about his or her health status.

**Enterprise** means a natural or legal person engaged in economic activity, regardless of its legal form, including partnerships or associations regularly engaged in economic activity.

**Group of companies** is a group consisting of a controlling company and the companies dependent on it.

## III. Data Privacy Officer

The data protection officer monitors compliance with the statutory provisions on data protection and the provisions of this policy. He advises and informs the management on the fulfillment of its obligations under data protection law. In addition, he acts as a point of contact for data subjects and supervisory authorities on issues relating to the processing of personal data.

The Data Privacy Officer works free of instructions and using his or her expertise. He reports directly to the highest management level.

The company has appointed a data protection officer. He can be reached as follows:

DataCo GmbH
Dachauer Str. 65
80335 Munich
Germany
+49 (0) 89 7400 45840

datenschutz@dataguard.de
www.dataguard.de

Employees of the company can contact the data protection officer in confidence at any time. In particular, the data protection officer should be involved as early as possible in the following issues:

- Requests or complaints from the data subjects
- Inquiries from supervisory authorities
- Data breaches (violations of the protection of personal data)
- Questions regarding data protection documentation
- Conceptual design of new corporate strategies that are related to data protection
- Data privacy compliance of products and services offered as well as tools and programs used (privacy by design/privacy by default - see IV.)

## IV. Principles for The Processing of Personal Data

When processing personal data, it is mandatory to observe the following principles:

**Lawfulness of processing** - personal data must be processed in a lawful manner (see V.).

**Purpose limitation** - Personal data may only be collected for specified, explicit and legitimate purposes. They may not be further processed in a manner that deviates from these purposes. A subsequent change of purpose requires separate justification in each case. In particular, the following points must be taken into account:

- the connection between the original and intended purpose of the data processing,
- the context in which the personal data were collected,
- the nature of the personal data being processed,
- the possible consequences of the data processing, and
- the existence of appropriate safeguards

**Transparency** - the handling of personal data should be carried out in a manner that is comprehensible to the data subject. Information obligations, which the controller must comply with, play an important role in this regard. When properly implemented, data subjects are informed about the purpose of the data processing, which controller the data subject can contact with questions, and whether or to which third parties the data will be transferred. In certain cases, the data subject must be informed subsequently that his or her personal data originate from other sources (i.e., were not collected directly from the data subject). The data subject must also be informed accordingly if the purposes change.

Transparency of data processing also plays an important role for data controllers, system operators or controlling bodies. This enables these groups of persons to understand at any time which data are processed for which purposes by which bodies and by which means. This can help to ensure that deficiencies in data processing are quickly identified and remedied.

**Data minimization** - the core content of data minimization includes the principle of necessity. According to this principle, all processing operations must be designed in such a way that only as much personal data is processed as is needed to achieve the specific purpose. These principles play a decisive role, for example, in the definition of internal deletion routines.

Before processing personal data, it must be checked whether and to what extent the respective processing purpose is achieved with the intended processing. If the purpose can also be achieved without recourse to personal data, for example by processing anonymized or pseudonymized data, this variant of data processing is to be preferred.

**Storage limitation** - the retention of personal data for unprovoked or future purposes is not permitted. Personal data shall only be stored for as long as it is necessary for the respective processing purpose.

**Accuracy** - the accuracy, completeness and timeliness of the personal data collected shall be ensured. Incorrect, incomplete or no longer up-to-date data shall be corrected, supplemented, updated or deleted without delay.

**Integrity** - personal data must be treated confidentially. Appropriate technical as well as organizational measures shall be taken in any case to ensure adequate protection against unauthorized or unlawful processing, accidental loss, destruction or damage.

**Deletion** - as soon as the purposes of the data processing cease to apply and the statutory retention periods have expired, personal data must be deleted.

**Availability** - the core element of availability includes the possibility of immediate access to personal data and their proper use within the framework of a specific processing process. This includes, in particular, the ability to find the data, the structured way in which it is presented, and the ability of data processing systems to present personal data in a format appropriate for users. In addition, technical measures must be taken to ensure that:

- personal data can be quickly recovered in the event of technical incidents;

- data processing systems remain functional in the event of a high load;
- measures are implemented that can remedy or mitigate the consequences of a data breach.

**Integrity** - integrity requires that the personal data being processed remain complete, current, accurate and intact. In addition, internal processes must be implemented that preclude deviations from these characteristics or allow deviations to be tracked for the purpose of correction. In particular, when systems are under heavy load and automated assessment and decision-making processes are in place, it is important to ensure that aspects of data integrity are maintained.

**Confidentiality** - the confidentiality of personal data requires the establishment of transparent access and authorization rights for the entire corporate structure. In this context, persons who have no connection to a specific processing activity or to a group of data subjects should not gain access to personal data (e.g., implementation of the "need-to-know" principle).

In addition, special attention must be paid to the specific requirements for security and resilience of systems, as well as for remediation or mitigation of the consequences of a data breach.

**The non-concatenation principle** - according to the non-concatenation principle, personal data must not be merged. Otherwise, new data sets may be generated even though the original processing of individual data was based on different legal bases or processing purposes. Appropriate technical measures (such as pseudonymization of data) can prevent chaining.

**Intervenability** - intervenability requires that data subjects are effectively granted their rights. This is related to the obligation of the controller to implement internal company measures that allow access to the processing operations at any time (from collection to deletion of personal data) and quick identification of the data subjects.

- Example: the data subject revokes his or her declaration of consent. In order to ensure that no more processing takes place, effective systems should be implemented (such as consent management platforms or software). In this way, the consents given and any revocations remain documented. Further processing of personal data is also prevented.

Privacy by design/privacy by default - according to this principle, the principles of data protection must be integrated into the company's internal software applications or data processing services. When selecting data processing systems, data protection-friendly default settings and configuration options must be taken into account.

## V. Lawfulness of Processing

Personal data must be processed in a lawful manner. This requires that the processing can be based on the effective consent of the data subject or on a legal basis. These bases for data processing should be made known and observed within the company. The respective legal basis must be brought into line with the purpose of processing.

Processing is only lawful if one of the following conditions is met:

- the data subject has voluntarily and unambiguously consented to their personal data being processed for a specific purpose.
- the processing is necessary for the performance of a contract to which the data subject is a party or because the data subject has requested the Company to take certain steps prior to the conclusion of the contract.
- the processing is necessary for the company to comply with a legal obligation.
- the processing is necessary in order to protect the vital interests of the data subject or another natural person.
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- the processing is necessary to protect the legitimate interests of the company or the legitimate interests of a third party. This does not apply if there is a compelling reason for the protection of personal data of the data subject that overrides these legitimate interests.

## VI. Data Processing

In cases where personal data is processed on behalf of a contractor, a contract processing agreement must be concluded with the contractor, the content of which must comply with the requirements of Article 28 of the GDPR. In the relationship between the client and the contractor, the contractor must act in accordance with instructions.

Regardless of the commissioned processing, the controller must in any case ensure that personal data are processed in accordance with the above principles (see IV.) as well as lawfully (see V.). When selecting the processor, the controller must ensure that the processor is professionally suitable and that its technical and organizational measures are appropriate.

If the processor provides its services in a third country (country outside the European Union or the European Economic Area) or if the processor uses the services of another processor located in a third country, the controller must ensure that the data transfer is based on an adequacy decision of the EU Commission or appropriate safeguards within the meaning of the GDPR. Transfers of personal data to third countries must always be discussed in advance with the data protection officer.

## VII. Record of Processing Activities

The company shall maintain a register of processing activities containing information on all data processing operations. A responsible person is appointed for each specialist department who is responsible for documenting the department-related processing operations. The data protection officer shall be consulted when documenting the processing operations.

The content of the list of processing activities must comply with the requirements of Art. 30 DS-GVO.

## VIII. Ensuring the Rights of The Data Subjects

The company's internal (communication) systems must be set up in such a way that requests from the data subjects can be processed in a timely and complete manner. As soon as the data controller is confronted with a request from the data subject, the data protection officer must be involved as quickly as possible.

When responding to the requests, the time limit of one month must be observed in any case, which starts to run from the receipt of the request. The implemented measure must be notified to the data subject within this period.

The data subject has the following rights: **Right to information pursuant to Art. 15 DS-GVO, Section 34 BDSG.**

The data subject has the right to request information as to whether personal data relating to him or her is being processed in the company. If this is the case, the data subject may request information about which data is processed for which purpose, from which source and for which purpose. purpose, from which origin and for how long. In the event of data being transferred to third parties, information must also be provided about the identity of the recipient and the categories of recipients.

Before providing information, the responsible party must establish the identity of the data subject and, if necessary, take measures to dispel any doubts that may arise as to the identity of the requesting person.

If the request for information is not made electronically, the data subject shall be provided with the information in writing. In addition, the controller shall provide a copy of the personal data and information listed in Article 15(1) of the GDPR that are the subject of the processing. If the data subject makes the request electronically, the information shall be provided in a commonly used electronic format.

**Right to Rectification Pursuant to Art. 16 DS-GVO.**

The data subject may request that personal data concerning him or her that is inaccurate or incomplete be corrected or supplemented without undue delay.

**Right to Deletion according to Art. 17 DS-GVO, § 35 BDSG**

The data subject is entitled to the immediate erasure of the personal data concerning him or her as soon as one of the following grounds for erasure is relevant:

- The purpose of the data processing does not (no longer) exist;
- A permission or legal basis for the data processing is missing or has ceased to exist (e.g. by the data subject revoking his/her consent);
- The data subject objects to the data processing and there are no overriding legitimate grounds for the processing;
- The data processing is unlawful;
- The processing of personal data is not (or is no longer) necessary for compliance with a legal obligation or for the assertion, exercise or defense of legal claims;
- There is no public interest in the processing that overrides the rights of the data subject.

**Right to restriction (Art. 18 DS-GVO)**

In the following cases, the data subject may assert his or her right to restriction of processing in relation to the controller:

- The data subject disputes the accuracy of the personal data. A restriction is imposed for the period during which the controller verifies the accuracy;
- The data processing is unlawful, but the data subject requests restriction of use instead of erasure of the personal data;
- The personal data is no longer needed by the controller for the purposes of processing, but the data subject needs it for the assertion, exercise or defense of legal claims;
- The data subject has objected to the processing. A restriction shall be imposed for the period during which the controller reviews the objection.

After an effective restriction of processing, the personal data concerned may be processed only with the consent of the data subject or for the establishment, exercise or defense of legal claims or for the protection of the rights of others or on grounds of important public interest. The data subject shall be informed of the lifting of the restriction.

**Right to Data Portability, Art. 20 DS-GVO**

Where data processing is based on consent or is necessary for the performance of a contract, the data subject shall have the right to transfer the personal data concerning him or her to another controller, where technically feasible.

**Right to Object, Art.21 DS-GVO**

The data subject has the right to object at any time to data processing that is based on consent or is necessary to protect legitimate interests. For this, the result of a weighing must show that the interest of the data subject worthy of protection resulting from a special situation outweighs the interest of the company in the processing. There is no right of objection if the processing serves the assertion, exercise or defense of legal claims.

**Right to Complain to a Supervisory Authority, Art.77 DS-GVO in conjunction with Section 19 BDSG**

In addition, the data subject has the right to lodge a complaint with the competent supervisory authority if the data subject considers that the processing of his or her personal data is unlawful.

In order to exercise the above rights, the data subject may contact the company's data protection officer.

## IX. Procedure in the Event of Personal Data Breaches (Data Mishaps)

the event of a personal data breach, the supervisory authority shall be notified without undue delay, if possible within 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of natural persons. Such a risk may exist in the case of risk of discrimination, identity theft, financial loss or damage to reputation. In any case, the Data Protection Officer must be informed of the personal data breach.

The data controller has a duty to notify the data subject without undue delay if the personal data breach is likely to result in a high risk to the rights and freedoms of that data subject.

Possible examples of data breaches:

- Personal data is stolen in a hacker attack.
- An email with sensitive content is sent to an unlimited number of people. Credit card data is publicly available on the Internet.
- Patient records are disposed of in household trash.
- A laptop with personal data is stolen without adequate security measures (password, encryption of data).
- Loss of hardware containing personal data (USB sticks, cell phone used for business or private purposes, etc.).

## X. Data Protection Training

The data protection officer provides the company with an online training platform. This is designed to help the company's employees create a comprehensive understanding of the applicable data protection regulations and raise their awareness of data protection in general.

Participants receive a certificate of successful participation at the end. Participation in this training is mandatory for all employees of the company who potentially come into contact with personal data (e.g. name, address, telephone number, etc.). Registration on the Academy platform is required for participation in the training. The link to the platform is provided to the company as part of the onboarding process.