Data Protection Guidelines

This is the English translation of the Privacy Policy (Datenschutzrichtlinie) of Glassomer GmbH. This is a translation only; the German Version is legally binding.

Issue Date: March 2024

Content

1 Introduction

This privacy policy sets out how Glassomer GmbH (hereinafter referred to as “Company”) collects, uses, stores and protects personal data. The company is committed to complying with the General Data Protection Regulation (GDPR) and all relevant German data protection laws.

2 Responsible body

The person responsible for processing within the meaning of the GDPR is:

Bastian E. Rapp, Chief Information (CIO) Glassomer GmbH, In den Kirchenmatten 54, 79110 Freiburg i. Br. cio@glassomer.com.

3 Purpose of data processing

The Company processes personal data only for legitimate and lawful purposes. The collection and use of personal data is carried out transparently and comprehensibly, in accordance with this data protection policy. The company ensures that the principles of data minimization and purpose limitation in accordance with the GDPR are adhered to.

3.1 Processing purposes

Personal data is only collected for pre-determined, legally permissible and openly communicated purposes. These purposes will be communicated transparently to data subjects, whether through data protection information, privacy statements or other appropriate means. The company clearly informs data subjects about the purposes for which their data is collected and processed.

The processing of personal data is carried out exclusively to fulfill the specified purposes. Only the data necessary to achieve these purposes will be collected and no further processing will take place that is incompatible with the communicated purposes.

Example processing purposes can be:

- Providing and improving our products or services
- Communication with customers, suppliers and other business partners
- Managing customer relationships, including customer care, support and service
- Processing orders, contracts and payments
- Human resources management, including application processes, employee administration and payroll
- Compliance with legal obligations, including tax and accounting records
- Ensuring the security of our systems and data and combating fraud and abuse
- Market research, analysis and development of new products or services
- Fulfilling government requests and legal obligations

The company updates its privacy policy regularly to ensure that all processing purposes are communicated clearly and up to date. This transparent communication about the purposes of data processing helps to strengthen the trust of data subjects and ensure compliance with data protection laws.

3.2 Consent

If the processing of personal data is based on the consent of the data subjects, the company attaches great importance to ensuring that this consent is voluntary, informed and clear. Before consent is obtained, data subjects are provided with transparent information about the purpose of the processing, the type of data processed, the identity of the controller and any recipients of the data.

Consent is obtained specifically for the respective processing purpose and is not obtained through the mere acceptance of general terms and conditions or data protection guidelines. The company ensures that data subjects have the opportunity to refuse or withdraw their consent without negative consequences.

Data subjects have the unrestricted right to revoke their consent at any time. The revocation has no impact on the lawfulness of the processing before the revocation.

To ensure that consent complies with the requirements of the General Data Protection Regulation (GDPR), the Company uses clear consent forms or other clearly identifiable means of consent and documents the collection of consent in accordance with legal requirements.

Compliance with these principles ensures that the processing of personal data is carried out in accordance with the provisions of the GDPR and other applicable data protection laws.

3.3 Contract execution

Personal data is processed if this is necessary to fulfill contractual obligations. This includes processing data to provide products or services, to fulfill contracts or to carry out pre-contractual measures upon request.

3.4 Legal Obligations

The company processes personal data to comply with legal obligations. This includes, among other things, the fulfillment of tax and accounting obligations in accordance with applicable laws and regulations. This includes the retention and documentation of data required for tax purposes, as well as the preparation of reports and invoices in accordance with legal requirements.

In addition, the company cooperates with government requests and complies with all legal obligations arising from national and international laws and regulations. This may include cooperating with regulators, law enforcement agencies or other government agencies to respond to inquiries, conduct investigations or comply with legal requirements.

The processing of personal data to fulfill legal obligations takes place within the framework of the respective legal basis and considering the data protection principles of the GDPR and other applicable data protection laws. The company ensures that the data is only used for the respective legally prescribed purposes and that the necessary security measures are taken to ensure the confidentiality, integrity and availability of the data.

Compliance with these legal obligations is critical to the Company and underlines our commitment to complying with applicable laws and regulations and protecting the rights and interests of data subjects.

3.5 Legitimate Interests

Where necessary and permitted by law, the Company reserves the right to process personal data based on its legitimate interests. A careful balancing of interests is always carried out to ensure that the rights and interests of the data subjects are adequately taken into account.

Processing personal data based on legitimate interests may include various purposes, such as:

- Ensuring the security and integrity of the company's systems and data
- Prevention of fraud, abuse or unlawful conduct
- Improve the quality, safety and performance of products or services
- Carrying out market analysis, customer profiling or marketing activities
- Safeguarding legal rights or enforcing contractual terms and conditions

When processing personal data based on legitimate interests, the company ensures that the processing is in accordance with the data protection principles of the GDPR and that the impact on the data subjects is minimized. In particular, the principles of data minimization, purpose limitation and transparency are observed.

The clear definition and documentation of the processing purposes and the underlying legitimate interests serve not only to comply with the GDPR and other data protection laws, but also to ensure transparency towards the data subjects. The Company will inform data subjects about the processing of their data based on legitimate interests in its privacy policy or other appropriate sources of information.

4 Data Security

The security and integrity of the data processed is of paramount importance to the company. We are committed to taking appropriate technical and organizational measures to ensure the confidentiality, availability and integrity of the personal data we process.

4.1 Access Control

Access to personal information is limited to authorized employees and service providers who need the information to perform their functions. All authorized persons are bound to confidentiality and receive regular training on data protection regulations and security procedures.

Access to personal information is strictly limited to authorized employees and service providers who need the information to perform their functions. The Company implements appropriate technical and organizational measures to ensure that only authorized persons have access to personal data and that such access is limited to the minimum necessary.

4.1.1 Authorization and Training

All employees and service providers who have access to personal data are pre-authorized and are granted access only to the data necessary to perform their specific tasks. In addition, all authorized persons are obliged to maintain the confidentiality of the data and to use it exclusively for the specified purposes.

It is ensured that all authorized persons receive regular training on data protection regulations and security procedures. This training covers aspects such as how to handle personal data securely, identifying security risks and reporting data breaches.

4.1.2 Monitoring and logging

The Company monitors and logs access to personal data to ensure that only authorized persons access the data and to detect suspicious activity. Any unauthorized access attempts or suspicious activity will be promptly investigated and appropriate measures will be taken to ensure the security of the data.

4.1.3 Physical Security

Adequate security measures are taken to physically protect personal information to prevent unauthorized access, theft or misuse. This includes security measures such as access controls, surveillance cameras and security guards at locations where personal data is stored or processed. This happens in an ISO 27001 certified data center in which the company's computer systems are installed.

Implementing these access control measures ensures the confidentiality and integrity of personal data and helps increase data subjects' confidence in data protection.

4.2 Encryption and Transmission

Personal information is encrypted during transmission between users and systems to ensure the confidentiality and integrity of the data. We use secure transmission protocols to ensure that data is protected from unauthorized access during transmission.

4.3 Data Backup and Restore

Regular backups are performed to ensure that personal data can be restored in the event of data loss, corruption or destruction. Recovery plans are regularly reviewed and updated to ensure quick and efficient recovery when needed. All data is stored exclusively on an encrypted data backup system (symmetrical encryption using AES-256) and protected from physical access in a data center certified according to ISO 27001.

4.4 Monitoring and Auditing

We conduct ongoing monitoring and regular audits of our systems to identify and address potential security threats. Any unauthorized access or suspicious activity will be promptly investigated and appropriate measures will be taken to address security incidents.

4.5 Employee awareness

Our employees understand the importance of data security and receive regular training to ensure they understand and apply best security practices. This includes raising awareness of phishing attacks and other potential security risks.

4.6 Data Protection Impact Assessment (DPIA)

Before introducing new processing activities, particularly those that pose a high risk to the rights and freedoms of natural persons, we carry out data protection impact assessments (DPIAs) to assess potential risks and implement appropriate safeguards. A data protection impact assessment is carried out when new processing activities are introduced that are likely to pose a high risk to the rights and freedoms of natural persons.

The DPIA involves a systematic assessment of the potential impact of processing activities on the privacy and data protection rights of data subjects. This takes into account factors such as the type, scope, context and purposes of the processing, as well as the type of data concerned and the potential risks for the data subjects. Based on the results of the DPIA, appropriate protective measures are identified and implemented to minimize risks and ensure compliance with data protection laws.

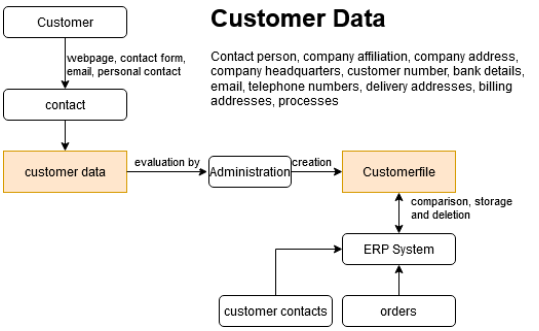
A DPIA is carried out under the direction of the CIO, recorded, presented to management and approved by them.

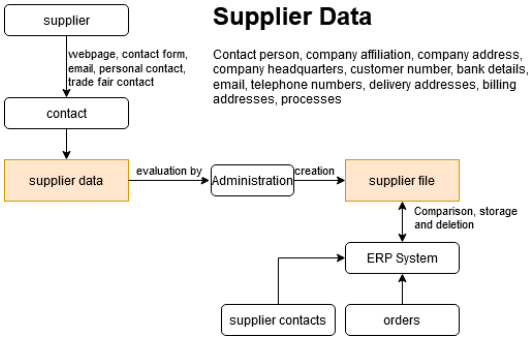
The implementation of these measures underlines our commitment to the security of personal data and ensures compliance with the GDPR and other relevant data protection laws.

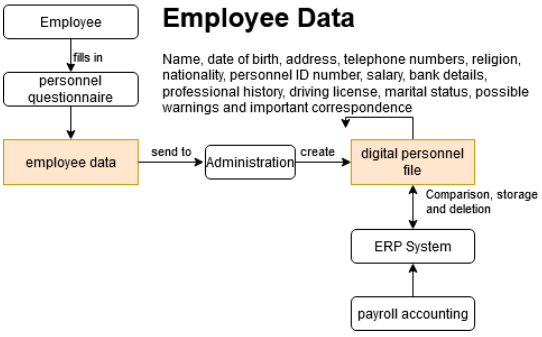
5 Disclosure of personal data

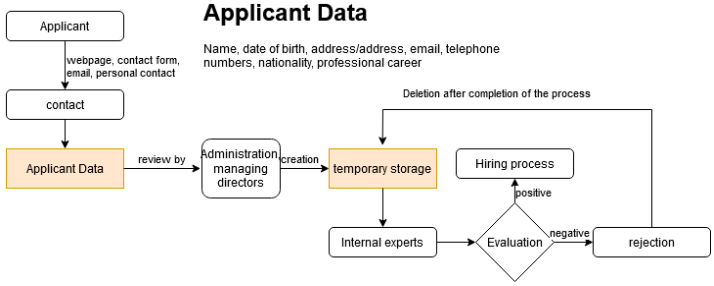
Personal data may be disclosed to third parties if this is necessary to comply with legal obligations, fulfill a contract or based on the legitimate interests of the company. The company ensures that third parties also adhere to appropriate data protection standards.

6 Data Flow Maps









7 Rights of those affected

Data subjects have the right to information, correction, deletion, restriction of processing, data portability and objection to the processing of their personal data. In order to exercise these rights, the data subject may contact the responsible body specified in Section 2.

8 Data Protection Officer

The company has appointed a data protection officer, contact details:

Bastian E. Rapp, Chief Information (CIO) Glassomer GmbH, In den Kirchenmatten 54, cio@glassomer.com.

9 Changes in the Privacy Policy

This Privacy Policy may be updated as necessary. Any material changes will be communicated to those affected.

10 Contact details

If you have any questions or concerns about the Privacy Policy, you can contact cio@glassomer.com.