WOLFTANK GROUP

Wolftank Group | 11th May 2023 | Innsbruck

DATA BREACH & PRIVACY POLICIES

DATA BREACH POLICY

1 Scope of the policy 3

2 Area of application 3

3 Definitions 3

4 Responsibilities 3

5 Methods of execution 4

5.1 Identification of the breach 4
5.2 Risk assessment related to the breach 4
5.3 Notification of data breach to the Supervisory Authority 6
5.4 Notification of the data breach to the data subject 6
5.5 Documentation of the data breach 7

6 References 7

7 Archiving 8

1 Scope of the policy

The purpose of the policy is to define the methods and responsibilities for carrying out:

- the notification of a personal data breach to the supervisory Authority;
- the communication of a personal data breach to the data subject;

also ensuring:

- identification of the violation;
- the analysis of the causes of the violation;
- the definition of measures to be taken to remedy the personal data breach and mitigate its possible negative effects;
- the recording of information about the violation, the measures identified, and their effectiveness.

2 Area of application

The procedure applies to all activities carried out by Wolftank Group, with particular reference to the management of all archives/paper documents and all information systems through which personal data of data subjects (customers, suppliers, other third parties, etc.) are processed, also with the support of external suppliers.

3 Definitions

Data Controller: the natural or legal person, public authority, service 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 applicable to its designation may be established by Union or member state law.

Control Authority/Authority: the independent public Authority established by a member state.

4 Responsibilities

- System Administrator
- Labour Consultant
- Competent Doctor

- Data Controller

5 Methods of execution

5.1 Identification of the breach

Personal data breaches are a type of information security incident involving any type of data of a personal nature (biographical data, personal card numbers, identification codes, health data, biometric data, bank account data, etc.).

Personal data breaches can be classified according to the following three information security principles:

- breach of confidentiality - in case of unauthorised or accidental disclosure or access to personal data;
- breach of integrity - in case of unauthorised or accidental modification of personal data;
- breach of availability - accidental or unauthorised loss of access to or destruction of personal data.

Anyone can discover a personal data breach. This person shall immediately notify the Data Controller, in the person of the Corporate RSPP, informing him/her of the nature of the breach (virus, malware, physical removal of documents, etc.). The Data Controller will determine the actual existence of the breach and, if the breach is confirmed, will initiate the activities described below.

5.2 Risk assessment related to the breach

In order to determine how to handle a breach and any notification and/or reporting requirements, the Data Controller will conduct a risk assessment.

The level of risk is defined on the basis of two parameters:

- severity: the relevance of the adverse impact that the breach is likely to have on the rights and freedoms of data subjects (e.g. the privacy of data subjects).
- probability: the degree of possibility that one or more of the feared events will occur.

DANGER	RISK ASSESSMENT	ACTIONS TAKEN BY THE DATA CONTROLLER	RESIDUAL RISK ASSESSMENT
PERSONAL DATA BREACH	LOW MEDIUM X HIGH	PC ANTIVIRUS, PC AND CELL PHONE PASSWORDS, WIFI PROTECTION, LOCKING CABINETS CONTAINING PERSONAL DATA INFO AND SERVER ROOM, CLOUD PROTECTION.	LOW X MEDIUM HIGH

Severity	Impact of the violation on the rights and freedoms of those affected: • Low: no impact • Medium: minor impact, reversible • High: major, irreversible impact
Probability	Chance of occurrence of one or more feared events: • Low: the feared event does not occur • Medium: the feared event could occur • High: the feared event has occurred

		Severity		
		Low	**Medium**	**High**
Probability	**Low**	1	2	3
	Medium	2	4	6
	High	3	6	9

	Description	**Notification to the Authority**	**Communication to interested parties**
Risk	**Low**: No prejudice to the rights and freedoms of data subjects or the security of personal data involved	NO	NO
	Medium: possible prejudice to the rights and freedoms of data subjects and the security of personal data involved	YES	NO
	High: Certain prejudice to the rights and freedoms of data subjects and the security of personal data involved	YES	YES

Based on the above elements, the Data Controller shall assess the severity and probability of the breach and classify the risk; documents the decision taken as a result of the risk assessment in the 'Breach Register'; and, if the risk is not considered to be high and it is not deemed necessary to proceed with the notification, the justification for this decision.

5.3 Notification of data breach to the Supervisory Authority

As soon as you become aware of a personal data breach that poses a risk of any level above the "low" level to the rights and freedoms of the individuals involved, you must notify the Authority. It is understood that the Data Controller knows of the breach when he or she has a reasonable degree of certainty that an information security incident has occurred that has compromised personal data. In order to attest to the time of becoming aware of the violation, report the violation by email to the Data Controller by sending appropriate information about its nature and the outcomes of the above risk assessment. The notification shall be made within 72 hours of the Data Controller becoming aware of it.

The notification document shall contain at least the following elements:

- the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects involved and the categories and approximate number of personal data records affected;
- the name and contact details of the Data Protection Officer or another contact point from which further information can be obtained;
- the possible consequences of the personal data breach;
- the measures taken or proposed by the Data Controller to remedy the breach;
- the reasons for the delay if the notification to the supervisory Authority is not made within 72 hours;
- where applicable, a statement that some of the required information is missing and an undertaking to provide the additional information as soon as possible, at one or more later stages.

5.4 Notification of the data breach to the data subject

In the event of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, as assessed in accordance with the section 'Risk assessment related to the breach", the data subject of the breach shall be notified, except if:

- the controller had implemented appropriate technical and organisational security measures and those measures were applied to the personal data affected by the personal data breach, in particular measures to render the personal data unintelligible to unauthorised persons, such as encryption;

- the controller has subsequently taken measures to prevent a high risk to the rights and freedoms of data subjects;

- such notification would require a disproportionate effort. In such a case, a public notice or similar measure shall be provided, by which the data subjects are informed with similar effectiveness.

The notice should include at least the nature of the breach, the contact details of the Data Protection Officer who can be contacted for further details, the likely consequences of the breach and the steps the Data Controller has taken to remedy it. For sharing the notice, it is important to choose the communication channel that maximises the likelihood that the message will reach all stakeholders.

5.5 Documentation of the data breach

For each breach that is determined to have occurred, the Data Controller shall compile a 'Breach Log', which shall show:

- progressive numbering;
- date of discovery;
- the area/process involved in the breach;
- description of the breach;
- categories of data subjects affected;
- the approximate number of data subjects affected;
- categories of personal data records involved;
- the approximate number of personal data records involved;
- causes of the breach;
- consequences of the breach;
- measures to remedy the personal data breach and mitigate its potential adverse effects, including the responsibilities and timeframes for implementing the measures;
- elements to support the risk assessment: severity, likelihood, level of risk;
- the need to notify the Authority and the date/time of notification, if applicable;
- the necessity of notification to the data subject and date/time of notification, if applicable;
- verification of the implementation of the measures;
- review of the effectiveness of the measures.

In addition to the records, the Data Controller shall collect and retain all documents relating to each breach, including those relating to the circumstances surrounding it, its consequences and the measures taken to remedy it. Such documentation shall be made available to the Supervisory Authority for any review within its competence.

6 References

- Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016, on the protection of individuals concerning the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation);
- industry best practices developed in light of the Code and case law of the Data Protection Authority;
- guidelines on the notification of personal data breaches under Regulation 679/2016 (WP250), adopted by the Article 29 Working Party ("WP29") in final form on February 6, 2018;

- guidelines concerning data protection impact assessment as well as criteria for determining whether a processing operation "may present a high risk" under Regulation 2016/679 (WP248), adopted by WP29, in final form, on October 4, 2017;
- statement on the role of a risk-based approach in the data protection framework (WP218), adopted by WP29 on May 30, 2014;
- recommendations for a methodology for assessing the severity of personal data breaches, adopted by the European Union Agency for Network and Information Security (ENISA) on December 20, 2013.

7 Archiving

The 'Notification' and 'Communication' attachments and all related documents, as well as the 'Breach Log' and the 'Data Breach Scenarios' document shall be archived by the Data Controller.

The most comprehensive version of the Data Breach Policy is available to all Wolftank Group employees on the company intranet. This version summarises the key aspects of the policy.

PRIVACY POLICY

1 Purpose 10

2 References 10

3 Responsibilities 10

4 Employees authorised for data handling 10

5 Scope of application 10

6 Purpose of data processing and legal basis for processing 11

7 Types of data processed telematically 14

1. Purpose

With this Privacy Policy (hereafter just "Policy") we would like to explain to you clearly and transparently what personal data we collect and how we use and manage it in order to conduct our business activities and ensure the best possible service to you. Acting in your best interest, we are committed to protecting and safeguarding any personal data you provide to us, and we release our contact information for you to contact us if you have any questions about personal data. We would also like to inform you that if you do not agree with this Policy, we encourage you to discontinue using Wolftank Group services.

2. References

European Regulation 679/16 “General Data Protection Regulation” or GDPR.

3. Responsibilities

The Data Controller is each legal entity of the Wolftank Group, headed by Wolftank-Adisa Holding AG. To exercise your rights, listed in the "Rights of Data Subjects" section of this Notice, as well as for any other requests, you may contact privacy@wolftank.com.

4. Employees authorised for data handling

Personal data may be processed by employees and collaborators of the various business functions of the Data Controller, including the sales and purchasing network, administration and accounting, IT department, marketing, and personnel department, deputed to the pursuit of the purposes set out below. Employees and collaborators have been expressly authorized for processing, have received operational instructions and have been adequately sensitized and trained.

5. Scope of application

This Policy defines the processing of data and information that may relate to or be associated with a person who is part of one or more of the following categories of individuals: customers and potential customers, suppliers, business partners, users of Wolftank Group's websites, platforms

and any other online application that refers to or contains a link to this Policy (of also just "Data Subject").

6. Purpose of data processing and legal basis for processing

Personal data may be processed for the following purposes:

- entering into and executing contracts, i.e., executing pre-contractual measures taken at the request of the Interested Party, as well as fulfilling contractual and legal obligations related to the following purpose (e.g., handling orders, requesting contact data of customer and supplier contacts, giving effect to agreed payment arrangements, providing regular billing and maintenance of customer and supplier accounts, customer care and handling of any complaints, etc.).

Legal basis: performance of a contract ex art. 6(b) GDPR, and legal obligation ex art. 6(c) GDPR:

- internal operational, organizational and management needs, (e.g., compiling master records and archiving, asset management, compiling internal statistics and reports, insurance needs, etc.).

Legal basis: legitimate interest under Article 6 letter f) of the GDPR aimed at the conduct of our economic activity:

- carry out personnel selection processes and properly evaluate the data subject's application for a specific job offer, i.e. spontaneously sent to the Data Controller, through the examination of the curriculum vitae and other documents (e.g. application form, cover letter etc.) containing personal data of the Data Subject.

Legal basis: consent of the data subject under Article 6 a) of the GDPR, optional and revocable at any time:

- protect claims and manage any debts, and in general defend the rights and interests of the Holder in the course of any extrajudicial and judicial disputes, including in the context of disputes arising in connection with the services offered.

Legal basis: legitimate interest under Article 6 f) of the GDPR aimed at protecting one's rights and preventing wrongdoing:

- fulfil legal obligations of any nature (civil, tax, fiscal etc.), arising from EU and international regulations.

Legal basis: legal obligations under Art. 6 c) of the GDPR:

Personal data collected

The Data Controller may collect and process the following types of data for the above purposes:

- so-called "common" personal data, merely by way of example anagraphic data (first name, last name, language, e-mail address and telephone numbers, etc.), data relating to the type of work, salary, business role and personal interests, user data when registering to portals or platforms of the Data Controller, data relating to the type of use of services, audio, photos, videos and images, or statements and information voluntarily released by the Data Subject.

Origin of data collection

As a rule, the Data Controller collects data directly from the Data Subject (e.g. through the Controller's web pages or social profiles, registration to its own platforms or portals, compilation of contractual documentation, etc.). The Data Controller may also process data that has been collected from third parties (e.g. through data acquisition from external databases for commercial information, public directories, subsidiaries, etc.) In the latter case, the Controller will provide this privacy policy at the first useful contact with the Data Subject.

Method and location of processing

Concerning the purposes previously indicated, personal data may be processed in paper form, or by means of computer and telematic tools (e.g. e-mail, newsletters, use of management software, registration on our websites or platforms, etc.), guaranteeing in all cases the security and confidentiality of the data processed, in full compliance with current legislation.

The personal data processed are usually subject to decision-making processes based on human intervention, but could also be subject to partly automated decision-making processes. In the latter case, human involvement is still ensured through effective control by persons with the authority and expertise to intervene in the final decision. Specific security measures are observed to prevent data loss, illicit or incorrect use and unauthorized access.

Personal data collected or voluntarily disclosed by the Data Subject are processed by the Data Controller within the European Economic Area.

Data retention period

Personal data will be processed by the Data Controller for a period of time strictly necessary to achieve the purposes set in these regulations. This means that the collected data will be destroyed or deleted from the systems or archives of the Data Controller if their storage is no longer necessary, and in any case no longer than the terms provided by law.

Area of communication and dissemination

In connection with the above purposes, personal data will be disclosed, if necessary, to third parties such as:

- companies related to, controlled by, and controlling companies of Wolftank Group;
- public administrations and/or judicial or police authorities, where required by law or to prevent or suppress the commission of a crime;

- credit institutions with which the Data Controller has relationships for credit/debt management and financial intermediation;
- suppliers/manufacturers in order to register products or to provide you with our services;
- third parties performing complementary activities for the delivery of Wolftank Group services;
- to all those natural and/or legal persons, public and/or private (e.g. legal, administrative and tax consulting firms, judicial offices, Chambers of Commerce etc.), when the communication is necessary or functional for the performance of our activity.

Personal data processed by our company are not subject to dissemination. Wolftank Group does not sell or give away your personal information.

Rights of Data Subjects

At any time, as a Data Subject, you may exercise your rights vis-à-vis the Data Controller under Articles 15 to 22 of the GDPR, where applicable, namely:

- obtain access to personal data about you (Art. 15 GDPR);
- rectification of inaccurate personal data and supplementation of incomplete personal data (Art. 16 GDPR);
- deletion of personal data concerning you (Art. 17 GDPR);
- limitation or blocking of the processing of personal data concerning you (Art. 18 GDPR);
- request a copy of the personal data concerning you, and, if technically feasible, the transmission of that data to another data controller, in a structured, commonly used and readable format (Art. 20 GDPR);
- opposition to the processing, in whole or in part, for a legitimate reason, of personal data concerning you (Art. 21 GDPR).

Regarding how to exercise the rights provided, you may send an application with the subject: "exercise privacy rights" to the Data Controller, at the addresses provided in the above Notice.

Please note that you have the right to lodge a complaint with the Data Protection Authority or the Supervisory Authority in the Member State where you normally reside, work, or the place where the alleged violation occurred, (Art. 77 GDPR).

Use of the data controller's website

In addition to the preceding paragraphs, the following provisions apply to the processing of personal data related to users and visitors (hereinafter also only "User" or "Users") of Wolftank Group websites (hereinafter also only "website").

When you visit one of our websites, fill out registration forms to take advantage of certain services or receive information, or access restricted areas, personal data is collected and processed in full compliance with the basic principles and security policies stated above.

7. Types of data processed telematically

Internet browsing data

The computer systems and software procedures used to operate the website acquire, in the course of their normal operation, some personal data, the transmission of which is implicit in the use of Internet communication protocols. This is information that is not collected in order to be associated with identified interested parties, but which by its very nature could, through processing and association with data held by third parties, allow Users to be identified. This category of data includes, for example, the IP addresses or domain names of the computers used by Users connecting to the website, the addresses in URI (Uniform Resource Identifier) notation of the requested resources, the time of the request, and other parameters related to the User's operating system and computer environment.

This data is used for the sole purpose of obtaining statistical information on the use of the website, checking its correct functioning and allowing you to take advantage of certain services on the website. In addition, the data is used anonymously, without automatic association with any other information provided by the User. The legal basis for the processing is the legitimate interest of the Data Controller ex art. 6 letter f) of the GDPR. Their storage will take place for the time strictly necessary for the pursuit of the above-mentioned purposes, and in any case not beyond the terms of the law.

This data could be used to ascertain liability in the event of any computer crimes that create damage to our website and its Users.

Cookies

We use cookies on our website to optimize the user experience and to provide certain functions. It is therefore in our legitimate interest to process personal data in this connection according to Article 6 (1) f) General Data Protection Regulation. The legal basis for the processing of personal data by us in conjunction with the use of cookies is Art. 6 (1) f) General Data Protection Regulation. When cookies are used, we store your personal data for as long as necessary to optimize your user experience on the website. The provision of this personal data is not prescribed by law or contract and it is not necessary for the purpose of entering into a contract. If you do not provide this data to us, we cannot optimize the user experience for you.

Third-party cookies may also be used on the website to collect information about our website and other sites on the internet. This information is then used for services such as web tracking, analyses or target audience-specific advertising. It is therefore in our legitimate interest to process personal data in this connection according to Article 6 (1) f) General Data Protection Regulation. The legal basis for the processing of personal data by third parties in conjunction with the use of cookies is Article 6 (1) f) General Data Protection Regulation. Personal data is stored in conjunction with the use of cookies for as long as is necessary for the purposes described above. The provision of this personal data is not prescribed by law or contract and it is not necessary for the purpose of entering into a contract. If you do not provide third parties with this data, the aforementioned purposes cannot be fulfilled.

Interaction with social networks and external platforms

The website may use so-called "social plug-ins," which are special tools that allow you to embed the functionality of social networks directly within a website (e.g. Facebook's "like" button, YouTube widgets, Twitter, Linkedin). Each of the social plug-ins on the website is identified by the social platform's proprietary logo. If you interact with the social plug-in, the information referable to you is directly communicated to the social platform, which processes your data as an independent owner. Therefore, in order to obtain more details about the purposes and methods of processing, the rights you can exercise and the storage of your personal data, please consult the privacy policy of the relevant social network.

Data voluntarily provided by the User

The optional, explicit and voluntary sending of electronic mail to the addresses indicated on the Web Site entails the subsequent acquisition of the e-mail address and the User's data necessary to respond to requests, as well as any other personal data included in the communication.

Underage visitors

Our websites and applications provide commercial content and are specifically intended and designed for use by adults. We recognize the need to protect data relating to minors, particularly in the online environment, and, therefore, we would like to inform you that consent to processing is only valid if you are an adult or a minor who is 16 years of age or older.