Data Protection Guidelines and Data Protection Policy of the Reiling Group

Table of contents

I. The aim of data protection guidelines

As part of our social awareness and responsibility, the Reiling Group is committed to comply with international data protection laws. Maintaining data protection is fundamental for a reliable and trustworthy business relationship and is of upmost importance for an excellent reputation as an attractive provider of employment.

Data protection guidelines provide one of the necessary basic conditions for the transmission of data[1] within the Reiling Group. The guidelines also guarantee the required level of data protection required by European Data Protection Regulations[2] and national laws for cross-border data transmission, even in countries where no such level of data protection is necessary by law[3].

II. Scope and amendments of data protection guidelines

Data protection guidelines apply to all companies within the Reiling Group, i.e. to all dependent companies belonging to the Reiling Group, as well as affiliated companies and their employees. The data protection guidelines include the processing of all personal data[4]. Anonymised data[5], e.g. for statistical analysis or research are also subject to data protection guidelines.

The individual company groups are not entitled to implement regulations that deviate in any way from data protection guidelines. Amendments to data protection guidelines can only be carried out in coordination with the data protection manager. The changes will be immediately reported to the Reiling Group within the procedure specified for changes to guidelines.

The current version of the data protection guidelines can be found under data protection information on the website of the Reiling Group at www.reiling.de.

III. Application of state law

This data protection guideline incorporates the worldwide acceptance of data protection principles without replacing existing national law, it supplements the respective national data protection laws. The respective national law takes precedence if it requires deviations from these data protection guidelines or imposes more extensive requirements. The contents of data protection guidelines are to be observed even if there is no corresponding state law.

---

[1] See XV

[2] EU regulation 2016/679 of the European Parliament and Council of 27 April 2016 for the protection of individuals with regard to the processing of personal data, on the free movement of all such data and repealing directive 95/46/EG (General Data Protection Regulations GDPR) available under http://eur-lex.europa.eu/legal-content/DE/TET/?uri=CELEX:3201GR0679

[3] See XV

[4] See XV

[5] See XV

Each company within the Reiling Group is responsible for complying with the data protection guidelines and its legal obligations. If any one company has reason to believe that legal obligations conflict with the obligations contained in the data protection guidelines, the company concerned must inform the data protection manager immediately without delay. In the event of a conflict between national law and data protection guidelines, Reiling GmbH & Co. KG will work together with the company group concerned in order to find a reasonable solution in accordance with the objectives of the data protection guidelines.

IV. Principles for the processing of personal data

1. Lawfulness

When processing personal data, the personal rights of the data subject[6] must be considered and respected. Personal data must be collected and processed in a lawful manner.

2. Purpose limitation

The processing of personal data may only pursue the purposes that were determined before the collection of the data. Subsequent changes to the purposes are only possible to a limited extent and require justification.

3. Transparency

The person concerned must be informed about the handling of his / her data. In principle, personal data must be collected from those affected themselves. When collecting the data, the subject should be able to at least be able to perceive, or be informed accordingly regarding the following:

- The identity and contact details of the controller[7]
- Contact details of the data protection manager
- The purpose of data processing and its legal justification
- Third parties[8] or categories of third parties to whom the data may be transmitted to.
- The duration of the planned storage, e.g. the criteria for determining it.
- The legal right to information from the data processor on the personal data concerned, as well as the right to rectification, deletion, restriction of processing, object to processing and finally the right to data portability.
- The right of appeal to a supervisory authority.

[6] See XV
[7] See XV
[8] See XV

- Whether the provision of personal data is required by law, or by contract, or is necessary before the completion of a contract, whether the data subject concerned is subject to provide the requested personal data, and what the possible consequences would be for not doing so.

4. Data avoidance and data reduction

Before processing personal data, it must be checked whether, and to what extent this is necessary[9] in order to achieve the intended purpose of processing. Anonymised and statistical data must be used to a reasonable extent when possible. Personal data may not be retained for potential future purposes.

5. Deletion

Personal data that is no longer required due to the expiry of legal and business process-related retention periods must be deleted. If there are any indications of legitimate data protection in an individual case, the data must be retained until this has been legally clarified.

6. Factual accuracy and data actuality

Personal data should be kept accurate, complete and if necessary, updated. Appropriate measures must be taken to ensure that inaccurate, incomplete or outdated data is deleted, corrected, completed or updated.

7. Confidentiality and data processing

Data confidentiality applies to personal data. All data must be treated confidentially and be secured by appropriate organizational and technical measures against unauthorised access, unlawful processing or disclosure, accidental loss, alteration or destruction.

V. Legitimacy of data processing

The collection, processing and use of personal data is only permitted if one of the following circumstances should exist. Such an authorisation is also required if the intention for collection, processing and use of personal data is to be changed in any way from the original circumstances.

1. Customer and partner data

1.1 Data processing for a commercial / contractual relationship

Personal data of the interested party, existing customer or partner concerned, may be processed and used to justify the implementation and conditions of a contract. This also includes the support of the contractual partner, insofar as this is relevant to the purpose of the contract. In the run-up to a contract, i.e. in the contract initiation phase, the processing of personal data for the preparation of

[9] See XV

all offers, or for the fulfilment of other wishes of the interested party directed towards the conclusion of a contract may be contacted during the initiation phase using the data which they have provided. Any expressed restrictions by the party concerned must be observed. The following requirements under V. 1.2 must be met for advertising measures that go beyond this.

1.2 Data processing for marketing purposes

If the person concerned contacts a company within the Reiling Group with an information request (e.g. requests for information material on a specific product), so is data processing permissible /authorised to fulfil this request.

Customer relations and advertising campaigns require additional legal requirements. Data for the purposes of advertising or market and opinion research is permitted, provided this is compatible with the purpose for which the data was originally collected. The data subject is to be informed about the use of the data for advertising purposes. If data is collected exclusively for advertising purposes, the information provided by the person concerned is voluntary. The person concerned must also be informed about the voluntary nature of the provision of data for this purpose, and their right to revoke this information at any time. As part of the communication with the person concerned, the data subject's consent[10] to the processing of their data for advertising purposes must be obtained. The person concerned should be able to choose between the various available contact channels, such as by post, email and telephone within the framework of the consent.

(see consent V. 1.3)

If the data subject objects to the use of their data for advertising purposes, further use of the data is not permitted and must be frozen for these purposes. In addition, there are restrictions in some countries regarding the use of data for advertising purposes.

1.3 Consent to data processing

Data processing may take place on the basis of the consent of the person concerned. Before consent is given, the data subject must be informed in accordance with IV.3. of this data protection guidelines and be advised of their rights to revoke this consent at any time. For reasons of legal proof, the declaration of consent must be obtained in writing or via email.

1.4 Data processing based on legal authorisation

The processing of personal data is also permitted if state legal provisions require or permit data processing. The type and scope of the data processing must be necessary for the legally permissible data processing and are based on this legal provision.

1.5 Data processing based on legitimate interest

The processing of personal data may also take place if this is necessary for the realisation of a legitimate interest of one or more companies within the Reiling Group. Legitimate interests are

[10] See XV

usually of a legal nature (e.g. enforcement of outstanding payments) or commercial (e.g. prevention of breach of contract). Processing of personal data based on a legitimate interest may not take place if, in individual cases, there is an indication that the meriting protection interests of the person concerned, outweigh the interest of the processing. The interests requiring protection must be reviewed before processing.

1.6 Processing of data meriting protection

The processing of particularly sensitive data[11] may only take place if this is required by law or, the person concerned has consented to this procedure. Processing of this data is also permitted if it is absolutely necessary in order to assert or defend legal claims against the data subject. If the processing data meriting protection is planned the data protection manager must be informed in advance.

1.7 Automated individual decision-making

Automated processing of personal data by which individual characteristic attributes (e.g. job applications) are assessed must not be the exclusive basis for decisions with negative legal consequences or significant disadvantages /impairment for the person concerned. Those affected must be informed of the fact and the result of automated individual decision-making and given the opportunity to comment. To avoid incorrect decisions a supervisory and verification inspection must be assured and carried out by a member of staff.

1.8 User data and internet

If personal data is collected, processes and or used on websites or apps, the data subject concerned should be informed about this through data protection notices and, if applicable cookie notices. The data protection notices and, if applicable, cookie notices are to be integrated in such a way that they are easily identifiable and immediately accessible to the person concerned.
If a user profile is created for the evaluation of usage behaviour of websites and apps (tracking), those affected must be informed through data protection notices. Personal tracking may only take place if national law permits this, or if the person concerned has consented to the procedure. If tracking should take place under a pseudonym, the subjects concerned should be given the opportunity to object in a data protection notice (opt-out).
If access to personal data is enabled on websites or apps in an area that is subject to registration, the identification and authentication of those affected must be designed in such a way that appropriate protection is achieved for the respective access.

[11] See XV

2 Personnel data.

2.1 Data Processing for employment relationship purposes

For the employment relationship, personal data that is necessary for the establishment, implementation and the termination of the employment contract may be processed. When initiating an employment relationship, applicants' personal data may be processed. After rejection the applicant's data must be deleted, considering time limits for evidence, unless the applicant has consented to further storage for a subsequent selection process. Consent is also required for the data to be used for further application procedures or before the application is passed on to another group within the company.

In an existing employment relationship, data processing must always be related to the purpose of the employment contract, unless one of the following permissions for data processing intervenes.

If the collection of further information concerning the applicant from a third party is required during the initiation of the employment relationship, or in an existing employment relationship, national legal requirements are to be taken into account. In the event of uncertainty, the consent of the person concerned must be obtained.

For the processing of personal data that is in context of the employment relationship but does not originally serve the fulfilment of the employment contract, a legal legitimation must be submitted in each individual case. These can be legal requirements, consent of the employee or the legitimate interests of the company.

2.2 Data processing based on legal authorization

The processing of personal employee data is also permitted if state legislation requires, demands or permits the data processing. The nature and volume of the data processing has to be necessary for the legally permissible data processing and base on these legal provisions. If there is legal room for leeway or flexibility, the interests of the employee must be taken into account and protected.

2.3 Consent to data processing

Processing of employee data may take place based on the consent of the person concerned. Declarations of consent must be given voluntarily. Involuntary consent is invalid. For evidential proof, the declaration of consent must always be obtained in writing or electronically. Before giving consent, the data subject must be informed in accordance with IV.3 of these data protection guidelines and made aware of his or her legal right to withdraw their given consent at any time.

2.4 Data processing based on legitimate interests

The processing of personal employee data may also take place if this is necessary for the pursuit of a legitimate interest of a company within the Reiling Group. Legitimate interests are usually legally (e.g. the assertion, execution or defence of legal claims), or economically motivated (e.g. the valuation of companies).

Processing of personal data on the basis of a legitimate interest may not take place if there is an indication in the individual case, that employee interests meriting protection outweigh the company interests of the processing. The existence of legitimate interests requiring protection must be evaluated for each processing operation.
Control procedures that require the processing of employee data may only be carried out if there is a legal obligation or a justified cause to do so. In the event of a justified cause, the proportionality of the control procedures must be examined. The legitimate interests of the company in the implementation of the control procedures (e.g. compliance with legal provisions and internal company rules) must be carefully weighed against a possible legitimate interest of the employee affected by the procedures, such procedures may only be implemented if they are appropriate. The legitimate interest of the company and the protection of the possible legitimate interests of all employees concerned must be determined, weighed and documented before any procedure should commence. In addition, further requirements that exist under national law (e.g. information rights of the data subject concerned) must be considered.

2.5 Processing of special categories of personal data

Special categories of personal data may only be processed under certain conditions. Special categories of personal data is data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. According to national law further data categories may also be classified as requiring special protection, or the content of the data categories may be defined differently. Likewise, data relating to criminal offenses are only allowed to be processed under special conditions issued and established by national law.
The processing must be explicitly permitted or prescribed by state law. In addition, processing may be permitted if it is necessary so that the responsible body may comply with labour rights and obligations in the field of labour law. The employee concerned may also voluntarily express consent to the processing.
If the processing of highly confidential date is planned, the data protection officer must be informed in advance.

2.6 Automated individual decision-making

If personal data related to an employment relationship is automatically processed in order to assess individual characteristics (e.g. in the context of personnel selection or the evaluation of capability and skill), such automated processing should not be the sole basis for decisions resulting in negative consequences or significant disadvantages for the employee concerned. The employee concerned must be informed of the fact and the result of the automated individual decision-making and be given the opportunity to comment.

2.7 Telecommunication and internet

Telephone systems, e-mail addresses, intranet and internet as well as internal social media networks are primarily provided by the company within the boundaries of operational tasks. They are work tools and company resource. They may be used within the framework of the applicable legal provisions and the company`s legal guidelines.

In the case of permitted use for private purposes, telecommunications secrecy privacy and the applicable national telecommunications law must be respected insofar as the apply.

There is no general monitoring of telephone and e-mail communication, or of internet and intranet access. In order to ward off possible attacks on the IT infrastructure or on individual users, protective measures may be implemented at the interfaces to the network of the individual companies within the Reiling Group which block technical harmful content, or analyse patterns of attack. For security reasons, the use of telephone systems, e-mail addresses, the intranet and internet as well as internal social networks may only be logged and monitored for a limited period of time. Evaluation of this personal data may only be carried out in the event of a concrete justified suspicion of the violation of the law. Such verifications may only be carried out by authorised investigation departments, or qualified approved personnel, which are subject to the principle of proportionality. Respective national laws are to be equally observed as are existing regulations within the Reiling Group.

VI. Transmission of personal data

The transfer of personal data to recipients either within or outside the Reiling Group, is subject to the admissibility requirement for the processing of personal data under section V. The recipient of such data must be placed under the obligation to use this personal data for specified purposes only.

In the event of data transmission to a recipient outside the Reiling Group in a third country[12], the level of data protection must be equivalent to the data protection guidelines within the Reiling Group and is to be guaranteed.

In the event of data transfer from third parties to the Reiling Group, it must be ensured that the data may be used for the intended purposes.

VII. Contract processing

Commissioned processing occurs when a contractor (processor) is commissioned to process personal data without assuming responsibility for the associated business processes. In such instances, an agreement on commissioned data processing must be reached between both the external contractors and the companies within the Reiling Group. The commissioning company retains full responsibility for the correct implementation of the data processing. The contractor may only process personal data as instructed by the client. When assigning the contract, the following requirement

[12] See XV

must be complied with; and the authorized commissioning department must ensure implementation.

1. The contractor is to be appointed on the grounds of his/her qualifications and ability to guarantee the required technical and organisational protection measures.
2. The contract is to be submitted in writing. The guidelines on data processing and the responsibilities of the client and the contractor must be documented.
3. The contract standards already provided by the Data Protection Officer must be applied.
4. The client must convince himself of the compliance with the obligations of the contractor before starting the data processing. A contractor can verify compliance with the data security by submitting the corresponding certification. Depending on the risk of data processing, verification may need to be repeated regularly during the contract period.
5. In the event of cross-border commissioned processing, the respective national requirements for the transfer of personal data abroad must be met. In particular, the processing of personal data from the European Economic Area (EEA) may only take place in a third country if the contractor can prove a level of data protection that is equivalent to existing data protection. Appropriate instruments may be as follows:
   a. Agreements regarding EU standard contractual clauses for commissioned processing in third countries together with the contractor and possible subcontractors.
   b. Participation of the contractor in a certification system recognised by the EU to create an appropriate level of data protection.
   c. Recognition of binding company policies of the contractor in order to provide an adequate level of data protection by the responsible data protection supervisory authorities.

VIII. Legal rights of the affected party.

Every data subject can claim the following rights. The assertion of these rights must be carried out immediately by the responsible department and must not lead to any disadvantages for the person concerned.

1. The data subject may request information regarding his/her personal data, the nature of the data and for what purpose the data is being stored. Should the employment relationship provide further extensive rights of access to the employer's documents (e.g. personnel files) under the respective labour laws, this shall remain unaffected.
2. Should personal data be transmitted to third parties, information concerning the identity and the categorisation of the recipient must be disclosed. If personal data should be transmitted to a recipient in a third country or an international organisation, the person concerned must be informed of the appropriate safeguards that entitle the data to be transmitted.
3. Should personal data be incorrect or incomplete, the data subject may request the data to be corrected and or supplemented.

4. The data subject may object to the processing of his/her personal data for the purposes of advertising or market and consumer research. Under such circumstances, consent may also be revoked at any given time. Should such cases occur, the data must be blocked.
5. The data subject is entitled to request the deletion or restriction of his/her data if the legal justification for the processing of the data is non-existent or has ceased to exist.
   The same applies if the purpose of the data processing has expired due to the lapse of time or for other valid reasons. Existing retention obligations and interests worthy of protection that conflict with deletion must be observed.
6. The person concerned/data subject has a fundamental right to object to the processing of his or her data, which must be taken into account if his or her, legitimate interests outweighs the interest in the processing due to a particular personal situation. However, this does not apply if legal regulation requires processing to be carried out.
7. The data subject has also the right to be informed of the personal data relating to him or her which he or she has provided.
8. The data subject has the right to be informed of his or her right to lodge a complaint with the responsible supervisory authorities.
9. The data subject has the right to receive all available information as to the source of his or her personal data.

IX. Confidential processing

Personal data is subject to data confidentiality. Employees are prohibited from the unauthorised collection, processing or utilisation of such data. Unauthorised processing is any kind of processing that is carried out by an employee without being entrusted to do so within the framework of his or her task, and without being authorised to do accordingly. The need-to-know principle applies: that is, employees may only have access to personal data if and to the extent that this is necessary for their respective roles and assignments. This requires a careful and accurate distribution and separation of roles and responsibilities, as well as their administration and upkeep within the framework of authorisation concepts.
Employees may not use personal data for their own private, or commercial interests. The transmission of personal data to unauthorised parties, or to make it accessible to them in any way is also strictly forbidden. Employers must inform their employees of the legal obligation to maintain data at the beginning of the work relationship. This legal obligation persists even after the employment has ended.

X. Processing safety

Personal data must be protected at all times against unauthorised access, unlawful processing, disclosure and loss, falsification or destruction. This applies regardless of whether the data is

processed electronically or in paper form. Before the introduction of new data processing procedures, in particular new IT systems, technical and organisational measures for the protection of personal data must be defined and implemented. These measures must be based on the level of technology, the risks assumed before the processing and the protection requirements of the data (protection classification listed in records of processing activities). The department concerned may consult the information security officer (ISO), data protection coordinator or the data protection manager. The technical organisational measures to protect personal data are part of the Reiling Group information security management, and therefore must be constantly updated to meet all technical and organisational innovations and modifications.

XI. Data protection monitoring

Compliance with the guidelines on data protection and the applicable data protection laws are regularly reviewed by means of data protection audits and other sources of monitoring. The execution of the latter is the concern and responsibility of the data protection manager, data protection coordinators and any other employees with audit authorisation, as well as appointed external auditors. The data protection manager must be informed of all data protection monitoring findings. The Reiling GmbH & Co. KG (holding company) advisory board is to be informed of any significant results within the limits of the respective reporting obligations. Upon request, the results of data protection monitoring are made available to the responsible data protection supervisory authorities. The relevant data protection authorities may, also carry out their own monitoring on compliance with the provisions of the directive within the limits of its authority under national law.

XII. Data protection incidents

In the event of a violation of the data protection guidelines or other protection regulations (data protection incident[13]) all employees must inform their respective supervisor or data protection manager immediately. The manager responsible for the function or the unit is obliged to inform the responsible data protection coordinator or data protection manager immediately in the case of any data protection incidents.

In events of

- unlawful transfer of personal data to third parties
- unlawful access by third parties to personal data
- or in the event of loss of personal data

[13] See XV

the notifications provided for in the company (Reiling data protection incident notification) must be made immediately so that existing reporting obligations of data protection incidents can be fulfilled under national law.

XIII. Responsibility and sanctions

The management of the group`s companies are responsible and accountable for data processing in their respective area of responsibility. They are therefore obliged to ensure that the legal data protection requirements and those contained in the data protection guidelines are taken into account (e.g. national registration requirements). It is a managerial task of the executives to ensure proper data processing in compliance with data protection through organisational, personnel and technical measures. The implementation of these requirements is the responsibility of the respective employee. In the event of data protection inspection by the authorities, the data protection manager must be informed immediately.

The respective management and plant manager of the Reiling Group not based in Germany but within Europe, must appoint a data protection coordinator to the data protection manager. In organisational terms, this task should be carried out in cooperation with the data protection manager. The data protection coordinators are the on-site contacts for data protection. They may also carry out monitoring and checks and are required to make sure that all employees are familiar with the content of the data protection guidelines. The respective management is obliged to support the data protection manager and the data protection coordinators in their activities. Those responsible for business processes and projects must inform the data protection coordinators in advance regarding any new processing of personal data. In cases of data processing projects that may result in particular risks for the personal rights of the data subject, the data protection manager must be involved before processing begins. This applies in particular to special categories of personal data. Managers must ensure that all their employees receive the necessary data protection training. Improper processing of personal data or other violations of the data protection laws are prosecuted under criminal law in many countries and may also result in claims for damages. Violations for which individual employees are responsible may lead to sanctions under labour law.

XIV. Data protection manager of The Reiling Group

The data protection manager, acting as an internal independent body, works to ensure compliance with national and international protection regulations. He is responsible for data protection guidelines and monitors their implementation. The data protection manager is appointed by the CEO, or the legal representative of Reiling GmbH & Co. KG. The data protection coordinators shall inform the data protection manager immediately regarding the possibility of any data protection risks.

All data subjects concerned, may contact the data protection manager or the data protection coordinator responsible for him/her with suggestions, queries, requests for information or complaints

in connection with any data protection or data security issues. Inquiries and complaints will be treated confidentially upon request.
If a respective data protection coordinator cannot resolve a complaint, stop or rectify a violation of the data protection guidelines, he or she must consult the data protection manager. The decisions taken by the data protection manager to rectify data protection violations must be taken into account by the executive management. Inquiries from supervisory authorities must be brought to the attention of the data protection manager.

The data protection manager may be contacted as follows:

Data protection manager. Reiling GmbH &Co. KG., Bussemasstraße 49, 33427 Marienfeld

E-Mail: datenschutzbeauftragten@reiling.de ; datenschutz@reiling.de

XV. Definitions

- An adequate and appropriate level of data protection in third countries is recognised by the EU Commission if the core element of privacy as it is in the member states of the EU is understood and substantially protected. The EU Commission takes into account all circumstances surrounding a data transfer or, a specific category of data transfers when making its decision. This also includes the assessment of national law as well as the respective ethical regulations and security measures.
- Data is anonymised if a personal reference can no longer be established by anyone. For example, if a personal reference could only be re-established with an unreasonable large effort in terms of time, costs and manpower.
- Particularly sensitive data is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Due to national law further data categories may be classified as requiring special protection, or the content of the data categories may differ. Furthermore data relating to criminal offences may often only be processed under specific conditions established by national law.
- The data subject within the meaning of this data protection guideline is any natural person from whom the data is processed. In some countries, legal bodies may also be affected.
- Data protection incidents are all occurrences in which there is a justified suspicion, that personal data has been or could be unlawfully accessed, exposed, copied, transmitted deleted or used. This can also refer to actions by third parties as well as employees.
- A third party is anyone other than the data subject, and the body responsible for the data processing. Processors are not third parties within the EU in terms of data protection law, as they are legally assigned to the responsible body.
- Third countries within the context of the Data Protection Directive are all countries outside the European Union /EEA. Exceptions are those states whose level of protection has been recognised as sufficient and acceptable by the EU Commission.
- Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- The processing of personal data is necessary if the lawful intention or the legitimate interest cannot be achieved without the respective personal data or can only be achieved with disproportionately high effort.
- The European Economic Area (EEA) is an economic zone associated with the EU, to which Norway, Iceland and Lichtenstein are members.
- Personal data means any information relating to an identified or identifiable natural person ('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.

- Processing 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.
- The controller is the legal independent company within the Reiling Group, who's business activities initiate the respective processing measures.