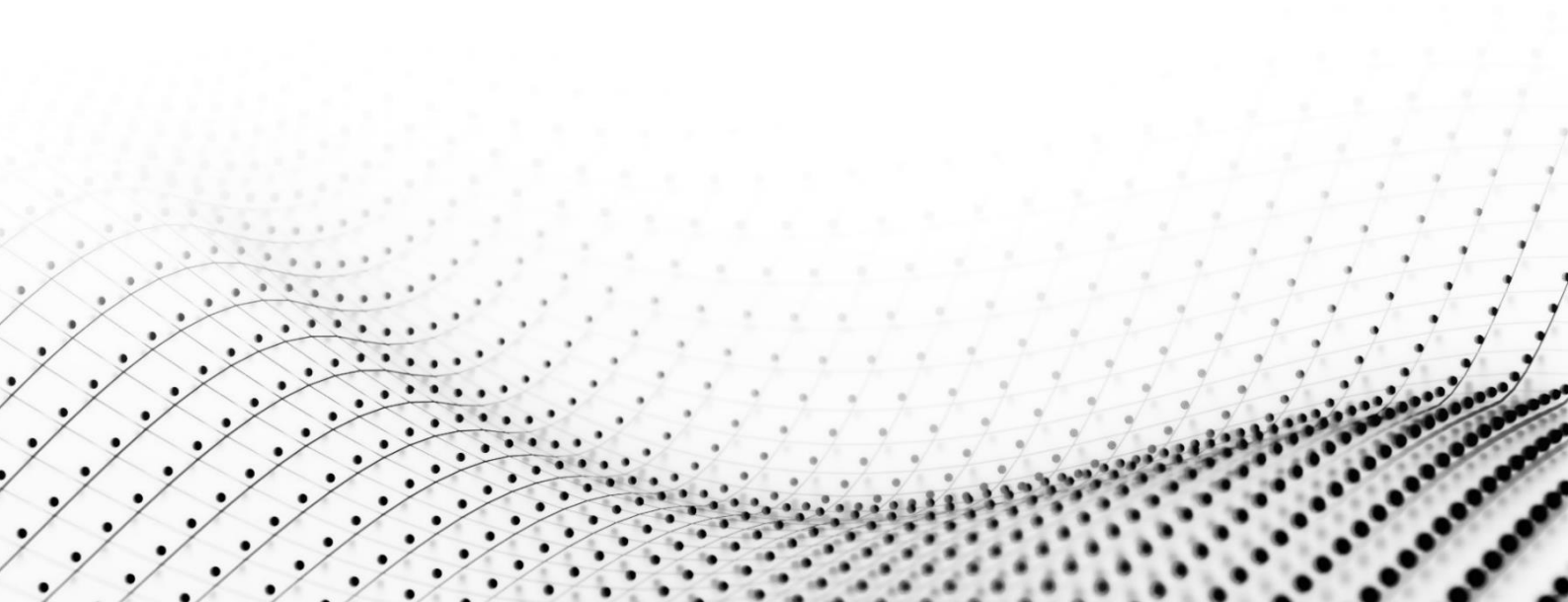


Data Protection Policy for Business Partners



Version control

Version	Date	Responsible	Remarks
1.0	26.9.2022	Clara-Ann Gordon	Initial version
1.1	28.2.2024	Marc Hirsbrunner	New Layout

Prevailing language

This Agreement shall be governed by and construed in accordance with the laws of Switzerland and the English language shall prevail in the case of any inconsistency or discrepancy between the versions in different languages.

Proper Usage

There are links to be updated if the below text is made available in any of our website. Please ensure they are **properly activated**.

1 Scope and purpose

This Data Protection and Privacy Policy ("**Policy**") applies to Reist Telecom AG ("**Reist**") when it processes personal data of partners, contractors, agents and other third parties ("**Partner**" or "**you**").

This Policy sets out the obligations of Reist regarding data protection and the rights of the Partners in respect of their personal data under the Swiss Data Protection Act ("**DPA**") and General Data Protection Regulation ("**GDPR**"), as amended from time to time (collectively "**Regulation**").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a Partner); 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.

This Policy sets out the procedures that are to be followed when dealing with personal data of Partners.

2 How to contact us?

Please contact us if you have any questions relating to this Policy or the personal data we hold about you. Either contact us by e-mail dataprivacy@reist.swiss.

3 Why do we process your personal data and on what legal basis?

We process your personal data in order to perform our obligations under the respective contract concluded with you, or for the purpose of other legitimate interests, or in order to comply with a legal duty imposed on Reist in connection with the respective contract.

4 What information do we collect about you?

The following personal data may be collected, held, and processed by Reist:

- a. your name, ID or passport, telephone number(s), mailing address, email address and any other information relating to you which you have provided us;
- b. you are able to configure any kind of datafield to collect any kind of information within the configuration of your tenant. So all these information the users then type in to your mandatory or optional datafields are subject to be collected, held and processed.

5 How do we collect personal data about you?

Generally, Reist may collect your personal data in the following ways:

- a. when you submit forms or applications to us;
- b. when you submit requests to us;
- c. when you ask to be included in an email or other mailing list;
- d. when you respond to our initiatives; and
- e. when you submit your personal data to us for any other reason

6 The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

- a. processed lawfully, fairly, and in a transparent manner in relation to the Partner;
- b. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- e. kept in a form which permits identification of the Partner for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the Regulation in order to safeguard the rights and freedoms of the Partner;
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7 What are your Rights?

You have the following rights under the Regulation:

- a. the right to be informed about the collection and use of personal data by Reist;
- b. the right of access to the personal data Reist holds about you;
- c. the right to rectification if any personal data Reist holds about you is inaccurate or incomplete;
- d. the right to be forgotten – i.e. the right to ask Reist to delete any personal data it holds about you;
- e. the right to restrict (i.e. prevent) the processing of the personal data;
- f. the right to data portability (obtaining a copy of the personal data to re-use with another service or organization);
- g. the right to object to Reist using the personal data for particular purposes; and
- h. rights with respect to automated decision making and profiling (where applicable).

8 Technical and Organizational Measures

Reist shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply and implement the appropriate technical and organization measures which are set out in Reist's Data Processing Agreement, Appendix 3: [\[Link\]](#).

9 Transferring personal data to a country outside the EEA

- 9.1 Reist generally processes all personal data in Switzerland.
- 9.2 Reist may from time to time transfer ("transfer" includes making available remotely) personal data to countries outside of Switzerland or the EEA (the UK included in the term "EEA" for the purposes of this Policy). These countries outside the EEA are listed here: [\[Link\]](#).
- 9.3 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
 - a. the transfer is to a country, territory, or one or more specific sectors in that country (or an international organization), that the Swiss Federal Council or the European Commission has determined ensures an adequate level of protection for personal data;
 - b. the transfer is to a country (or international organization) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data

protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorized by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorized by the competent supervisory authority;

- c. the transfer is made with the informed consent of the relevant Partner(s);

10 Data Breach Notification

- 10.1 All personal data breaches must be reported immediately to Reist's data protection officer.
- 10.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of the Partner (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the FDPIC and where applicable the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. With regard to data security breaches the FDPIC must be informed immediately.
- 10.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of the Partner, the data protection officer must ensure that all affected the Partners are informed of the breach directly and without undue delay.

11 Withdrawal of Consent

In the event a consent was given, Partners have the right to withdraw such consent given at any time by sending a written notice or e-mail to Reist's data protection officer.

12 Changes to this Policy

Reist reserves the right to amend this Policy from time to time. The latest version is published on Reist's website(s).