

Data Privacy Directive

Issued by:	Executive Team
Place, Date of Introduction:	Baar-Zug, 29 October 2007
Last update:	12 May 2023
Last review:	12 May 2023
Area of validity:	Partners Group worldwide

Table of contents

1.	Introduction, Scope and Applicability	3
1.1.	Introduction	3
1.2.	Scope and Applicability	3
2.	Data Privacy Principles.....	3
3.	Legal Bases for Processing Personal Data.....	4
4.	Privacy by Design and Privacy by Default.....	4
5.	Sharing of Personal Data	4
6.	Privacy Notices	4
7.	Data Retention and Deletion	5
8.	Data Subject Request.....	5
9.	Reporting a Personal Data Breach.....	5
10.	Training.....	5
11.	Security Measures	5
12.	Data Protection Officer	6
13.	Contact	6
	Appendix I: Definitions.....	7

1. Introduction, Scope and Applicability

1.1. Introduction

The proper handling of Personal Data is legally required and fundamental to maintaining trusted relationships with Partners Group's clients, business partners and employees. The Directive sets out Partners Group's approach to data privacy compliance in accordance with the GDPR and other applicable data privacy laws.

This Directive is supplemented by additional policies and procedures dealing with specific data privacy requirements, such as, local data privacy directives, the Data Record Retention Directive, and the Information Security End User Policy.

Capitalized terms are defined in Appendix 1.

1.2. Scope and Applicability

This Directive applies to all Personal Data that is Processed by (a) Partners Group Holding AG and its wholly owned subsidiaries, and (b) products for which a Partners Group entity is acting as general partner. It does not apply to products for which a Partners Group entity is acting only as a portfolio manager.

All Partners Group Personnel must comply with this Directive. When Partners Group Personnel become aware of any impediments to compliance with this Directive, such as a conflicting legal or regulatory requirement, or any potential violation of data privacy law, they must immediately inform the Data Privacy Team.

2. Data Privacy Principles

Partners Group complies with the following data privacy principles when Processing Personal Data.

- a) **Lawfulness, fairness and transparency.** Personal Data shall be processed lawfully, fairly and in a transparent manner;
- b) **Purpose limitation.** Personal Data shall be collected for a specified, explicit and legitimate purposes and not processed in a manner that is incompatible with that purposes;
- c) **Data minimization.** Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) **Accuracy.** Personal Data shall be accurate and up to date; and reasonable steps must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) **Storage limitation.** Personal Data shall not be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the Personal Data are processed; and
- f) **Integrity and confidentiality.** Personal Data shall be processed in a manner that implements reasonable and appropriate security measures (technical and organizational measures) to ensure the integrity and confidentiality of the Personal Data.

Partners Group is accountable for demonstrating and documenting its compliance with these principles.

3. Legal Bases for Processing Personal Data

Partners Group Processes Personal Data based on one or more specific legal bases. For example, Partners Group may lawfully Process Personal Data where the Processing is: (a) necessary for the performance of a contract, (b) required to comply with an applicable legal or regulatory requirement, (c) necessary for the purposes of Partners Group's legitimate interests, unless such interests are outweighed by the rights and interests of the Data Subject, or (d) performed with the Data Subject's consent.

The Processing of Sensitive Personal Data is subject to additional scrutiny and must be limited to only what is necessary for the purpose. If you plan to Process Sensitive Personal Data, please contact the Data Privacy Team.

4. Privacy by Design and Privacy by Default

Partners Group applies privacy by design and privacy by default approaches to promote data privacy compliance whenever a project or process uses Personal Data. Privacy by design means that Partners Group considers data privacy and data protection from the outset and throughout the lifecycle of a project or process. Privacy by default means that Partners Group operations and processes limit the amount of Personal Data collected, the extent of Processing, and access to Personal Data.

Partners Group Personnel conduct assessments concerning the Processing of Personal Data, where appropriate, such as a data privacy review or a data protection impact assessment as described in processes which can be found on the Data Privacy Team webpage.

5. Sharing of Personal Data

Partners Group shares Personal Data to the extent necessary to fulfill the purposes for which the Personal Data will be Processed.

Partners Group will only share Personal Data if there is a written contract. Where applicable data privacy laws require specific data privacy provisions, Partners Group will include such provisions to ensure that the Personal Data is handled in compliance with applicable data privacy laws.

Partners Group will only share Personal Data internationally if the Personal Data is subject to appropriate safeguard to ensure an adequate level of protection for the Personal Data. For example, Partners Group shares Personal Data between its operating entities and management companies under the terms of its intra-group data transfer agreement, which uses the EU standard contractual clauses as its safeguard to transfer internationally Personal Data.

6. Privacy Notices

Partners Group provides privacy notices to relevant Data Subjects (e.g., employees, clients, service providers) about the Processing of their Personal Data. Privacy notices describe how Partners Group

Processes Personal Data, such as what Personal Data is collected, why it is being collected, the legal bases for processing it, and with whom it is shared. Privacy Notices are reviewed and updated on a regular basis.

7. Data Retention and Deletion

Partners Group retains and deletes Personal Data in accordance with its [Data Records Retention Directive](#).

8. Data Subject Request

A DSR is a request by a Data Subject or its representative about the Data Subject's Personal Data. Data Subjects may have certain rights under applicable data privacy laws to their Personal Data, such as, (a) the right to access or know about Personal Data collected about them, (b) the right to correct such Personal Data, or (c) the right to request its deletion. These rights may be subject to limitations and/or restrictions.

Partners Group has processes for responding to a DSR. Partners Group's Personnel must immediately report any suspected or confirmed DSRs to the Data Privacy Team, and adhere to the processes that can be found on the [Data Privacy Team](#) wikipage.

9. Reporting a Personal Data Breach

A PDB is a breach of security measures leading to the accidental or unlawful loss, misuse, destruction, alteration or unauthorized disclosure of, or access to, Personal Data, transmitted, stored or otherwise processed by Partners Group or any other incident that compromises the security, confidentiality, integrity, or availability of Personal Data processed by Partners Group or third parties.

Partners Group has processes for responding to a PDB. Partners Group's Personnel must immediately report any suspected or confirmed PDB to the IT Service Desk, and adhere to the processes which can be found on the [Data Privacy Team](#) wikipage.

10. Training

Partners Group provides data privacy training on a regular basis for the purposes of informing its Personnel of their data privacy obligations, of improving its Personnel's understanding of their obligations, and of improving Partners Group's compliance with applicable data privacy laws. The Data Privacy Team will review and update the data privacy training materials to ensure they are consistent with this Directive and applicable data privacy laws. Partners Group Personnel are required to complete all required data privacy trainings.

11. Security Measures

Partners Group maintains reasonable and appropriate security measures to protect the security, confidentiality, and integrity of Personal Data. Partners Group's Personnel are responsible for being familiar with and complying with its security policies, such as its Information Security End User Policy.

Service providers that are Processors of Partners Group's Personal Data must comply with Partners Group's technical and organizational measures or have equivalent measures approved by Partners Group.

12. Data Protection Officer

The DPO is responsible for (a) monitoring Partners Group's compliance with data privacy laws, (b) advising Partners Group of its data privacy obligations, and (c) acting as a contact point for Data Subjects and the relevant supervisory authority.

Partners Group has appointed a group level DPO and country DPOs where required by applicable data privacy law. More information about the group level DPO and country DPOs can be found on the [Data Privacy Team](#) webpage.

13. Contact

Any queries concerning this Directive, applicable data privacy laws, or the Processing of Personal Data may be addressed to the Data Privacy Team (dpo@partnersgroup.com).

Appendix I: Definitions

Term	Definition
Controller	A 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
Data Privacy Team	Consists of Partners Group's Data Protection Officer and its Data Privacy Counsels
DPO	Means Data Protection Officer
Data Subject	An identified or identifiable natural person
DSR	Means Data Subject Request
Directive	Means the Data Privacy Directive
GDPR	Means the EU's General Data Protection Regulation
Personal Data	Means any information relating to a Data Subject 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
PDB	Means Personal Data Breach
Personnel	Any person employed or engaged by Partners Group (i.e., employees, interns, apprentices, contingent workers)
Process/Processing	Any operation performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Processor	A natural person or entity, public authority, agency or other body which processes Personal Data on behalf of a Controller
Sensitive Personal Data	Is defined by applicable data privacy law (e.g., under the GDPR, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, biometric data, data concerning health or sex life and sexual orientation)