

DATA PROTECTION DIRECTIVE

AT ACTIVE SPORTS REISEN GMBH (FN 207194Y), JUNS 512, 6293 TUX
(hereinafter referred to as the "Directive")

GENERAL DEFINITION OF RIGHTS AND OBLIGATIONS UNDER GDPR

1. INTRODUCTION

Active Sports Reisen GmbH (FN 207194y), Juns 512, 6293 Tux, Austria (hereinafter also referred to as "Active Sports Reisen") issues this internal regulation (Directive), which sets out the rules regarding the protection of personal data of individuals in connection with the processing of personal data by various subjects within the business activities of Active Sports Reisen.

Active Sports Reisen issues this Directive in accordance with the Austrian Data Protection Act (Datenschutzgesetz) and EU Regulation 2016/679 (hereinafter referred to as "GDPR"), which governs the procedures for the protection of personal data of data subjects by Active Sports Reisen, its employees, and data processors.

Since Active Sports Reisen is required by law to collect and process personal data of its customers in the course of its business activities, the company places great emphasis on the protection of the personal data it collects and processes.

Personal data, defined as any information relating to an identified or identifiable natural person, is collected by Active Sports Reisen both in physical documents and through electronic data. Given the sensitivity of this information, the personal data of individual customers is protected in accordance with this Directive.

2. GENERAL PRINCIPLES FOR HANDLING PERSONAL DATA

Active Sports Reisen and the designated controller are obliged to ensure the protection of personal data in accordance with this Directive and GDPR concerning its customers and third parties from whom Active Sports Reisen receives data subject to data protection under GDPR and the Directive.

Active Sports Reisen and the controller must ensure that employees are familiar with the Directive and that they follow it when handling personal data obtained in the course of their duties.

Employees who come into contact with third-party personal data, particularly that of customers or other third parties, are required to familiarize themselves with the content of the Directive and act in accordance with it. A similar obligation applies to external collaborators of Active Sports Reisen (legal or natural persons engaged in business) who are not in an employment relationship. If the Directive mentions employees, the rights and obligations also apply proportionately to these persons when they handle personal data of individuals based on their activities for Active Sports Reisen.

3. DEFINITION OF TERMS IN THE DIRECTIVE

A DATA SUBJECT is any natural person whose data is subject to data protection. For Active Sports Reisen purposes, the data subject is primarily the customer, employee, or external collaborator of Active Sports Reisen, or any third party whose data is obtained by Active Sports Reisen during its operations.

PERSONAL DATA refers to any information relating to an identified or identifiable natural person who can be identified, directly or indirectly (e.g., by name, personal details, identification number, location data, economic identity, photograph, or visual recording). Active Sports Reisen receives so-called personal data from the data

subjects.

PROCESSING refers to any operation or set of operations performed on personal data, such as collection, recording, organization, storage, adjustment, alteration, retrieval, viewing, disclosure, arrangement, deletion, or destruction of personal data.

The set of all personal data collected by Active Sports Reisen is considered a RECORD. The record shows whose personal data is collected and to what extent.

A CONTROLLER is a natural person who, alone or jointly with other controllers, determines the purposes and means of personal data processing and who is responsible for processing personal data within Active Sports Reisen.

A PROCESSOR is considered to be an external service provider, which may include, in particular, payroll and accounting services, tax advisors, financial auditors, IT network administrators, occupational safety personnel, law firms, occupational health service providers, etc., who may come into contact with personal data obtained from Active Sports Reisen.

A RECIPIENT is defined as a natural or legal person, public authority, agency, or other body to whom personal data is disclosed. When providing data to recipients, the controller must act in accordance with this Directive and GDPR.

A THIRD PARTY is a natural or legal person, public authority, agency, or other body that is not the data subject, controller, processor, or person under the direct authority of the controller or processor, and is authorized to process personal data.

A SECURITY BREACH is an incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data that is transmitted, stored, or otherwise processed.

EMPLOYEES of Active Sports Reisen are individuals who perform work tasks for Active Sports Reisen under an employment contract, an agreement on work performed, or employment services.

A BUILDING, for the purposes of this Directive, refers to the property at Juns 512, 6293 Tux, Austria.

4. PRINCIPLES OF PERSONAL DATA PROCESSING

Personal data must be processed fairly and in a lawful and transparent manner.

Active Sports Reisen complies with the principle of lawfulness when:

- a) It obtains the data subject's consent for the processing of personal data for one or more specific purposes; or
- b) The processing of personal data is necessary for the performance of a contract to which the data subject is a party or for pre-contractual negotiations; or
- c) The processing is necessary for compliance with a legal obligation of the controller (e.g., the controller's obligation to make social security payments for its employee); or
- d) The processing is necessary to protect the vital interests of the data subject or another natural person (e.g., determining fitness for work); or
- e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- f) The processing is necessary for the purposes of legitimate interests pursued by the controller or a third party.

Active Sports Reisen must ensure that personal data is primarily collected on legal grounds specified in points (b) through (f) of this paragraph.

If such legal grounds for processing personal data do not exist, Active Sports Reisen is only authorized to process personal data based on the data subject's consent under point (a).

5. PURPOSE OF PERSONAL DATA PROCESSING

Active Sports Reisen processes personal data of data subjects mainly for the following purposes:

- a) Performance of contractual obligations, including pre-contractual arrangements (order processing, order fulfillment, invoice delivery, contract management, etc.);
- b) Compliance with employment relationships with employees and related matters;
- c) Fulfillment of legal obligations arising from applicable laws – legal compliance by Active Sports Reisen;
- d) Archiving of customer data for the period prescribed by special regulations;
- e) Protection of Active Sports Reisen's interests in the event of claims enforcement.

Active Sports Reisen is obliged to inform each data subject that their data is being processed for specified purposes. Active Sports Reisen fulfills this obligation by providing the data subject with access to this Directive so that the data subject can familiarize themselves with their rights arising from the Directive and GDPR.

Active Sports Reisen is authorized to retain personal data only for the period necessary to maintain the purpose outlined in this article, regardless of whether the data subject has requested the deletion of the data. If the reason for retaining personal data ceases (the retention of personal data loses its purpose), Active Sports Reisen is obliged to delete the personal data without further delay.

6. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The processing of personal data revealing racial or ethnic origin, political opinions, religious beliefs, or union membership is prohibited. The processing of genetic data, biometric data for the unique identification of a person, health data, or data concerning a person's sexual life or orientation is also prohibited, except for the provided exceptions.

Active Sports Reisen is authorized to know the health status of its employees, i.e., personal data related to the physical or mental health of an individual, including data on medical services provided to that person, which reveal their health status (results of entry and periodic health examinations), but only for the purpose of assessing fitness for work and health risks. This health data is not considered a special category of personal data.

7. DATA PROTECTION OFFICER

Since Active Sports Reisen does not meet the conditions for the mandatory appointment of a data protection officer, it will not appoint one. Active Sports Reisen may obtain special category personal data (as mentioned in section 6) from data subjects during its operations; however, collecting such data is not its primary activity, nor does it process such data extensively. Therefore, it does not require a dedicated data protection officer.

8. CONTROLLER

Active Sports Reisen must ensure and be able to demonstrate that processing is carried out in compliance with GDPR; it will implement appropriate technical and organizational measures, taking into account the nature, context, and purposes of the processing, as well as the varying likelihood and severity of risks to the data subjects. One element by which Active Sports Reisen can demonstrate compliance with its obligations is adherence to this Directive and the mechanisms provided therein, by the controller, employees, and processors.

Active Sports Reisen is obliged to appoint one or more joint controllers who will be responsible for implementing appropriate measures and whom data subjects can contact with their requests.

If Active Sports Reisen appoints two or more controllers, they are joint controllers. In such cases, joint controllers are jointly responsible for fulfilling the obligations under the Directive. The data subject may exercise their rights under this Directive with any or all of the controllers.

9. **PROCESSOR**

Processors are considered external service providers. The activities of these processors are not primarily aimed at handling personal data; however, while providing services for Active Sports Reisen, they may come into contact with personal data of data subjects.

Active Sports Reisen must ensure that each processor provides sufficient guarantees to implement appropriate technical and organizational measures so that processing complies with the Directive and GDPR and that the protection of the rights of data subjects is ensured.

Active Sports Reisen must ensure that it enters into a written contract (processor clause) with each processor, obliging them to comply with the obligations under the Directive and GDPR.

10. **BASIC RIGHTS OF DATA SUBJECTS**

10.1. **Right of access to personal data**

A data subject has the right to obtain confirmation from the controller as to whether or not personal data concerning them is being processed. If it is, they have the right to access such personal data and the following information:

- a) The purposes of the processing; the categories of personal data concerned;
- b) The recipients or categories of recipients to whom personal data has been or will be disclosed (in particular, recipients in third countries or international organizations);
- c) The planned retention period for personal data or, if that is not possible, the criteria used to determine that period;
- d) The data subject's right to request the rectification or erasure of personal data, restriction of processing, or to object to the processing;
- e) All available information regarding the source of the personal data if it was not obtained from the data subject.

10.2. **Right to rectification**

The data subject has the right to obtain from the controller the rectification of inaccurate personal data concerning them without undue delay. They also have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

10.3. **Right to erasure**

The data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay, and the controller has the obligation to erase personal data without undue delay if one of the following grounds applies:

- a) The personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
- b) The data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;

- c) The data subject objects to the processing under Article 12 of the Directive, and there are no overriding legitimate grounds for the processing;
- d) The personal data has been unlawfully processed;
- e) The personal data must be erased to comply with a legal obligation under Union or Member State law to which the controller is subject;
- f) The personal data has been collected in relation to the offer of information society services.

If the controller has made the personal data public and is obliged to erase it, they will take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested the erasure of any links to, or copies or replications of, the personal data.

The aforementioned rules do not apply if the processing is necessary:

- a) For exercising the right of freedom of expression and information;
- b) For compliance with a legal obligation that requires processing under Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) For reasons of public interest in the area of public health;
- d) For the establishment, exercise, or defense of legal claims;
- e) For the protection of the legitimate interests of the controller;
- f) Where Active Sports Reisen is required to retain data under a specific regulation.

10.4. Right to restriction of processing

The data subject has the right to obtain from Active Sports Reisen the restriction of processing in the following cases:

- a) The data subject contests the accuracy of the personal data, for a period enabling the controller to verify the accuracy of the personal data;
- b) The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of its use instead;
- c) The controller no longer needs the personal data for the purposes of processing, but the data subject requires it for the establishment, exercise, or defense of legal claims;
- d) The data subject has objected to processing pending verification of whether the legitimate grounds of the controller override those of the data subject.

If the processing has been restricted under paragraph 1 of this article, such personal data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest.

10.5. Right to object

The data subject has the right to object at any time to the processing of personal data concerning them for reasons related to their particular situation. The controller will no longer process the personal data unless they can demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

11. ISSUANCE AND UPDATING OF THE DIRECTIVE

The controller is obliged to familiarize the employees of Active Sports Reisen with this Directive. The Directive is accessible to every employee in electronic form via the intranet on the network drive in the GDPR folder. The most up-to-date version of the Directive will always be in this folder, and employees are obliged to regularly familiarize themselves with it. The most current version of the Directive will also be

available in the Active Sports Reisen building, and the controller will allow any employee or client to familiarize themselves with the Directive. The controller will notify employees of any updates to the Directive.

SPECIFIC MEASURES TO ENSURE PERSONAL DATA PROTECTION

1. PHYSICAL RECORDS OF PERSONAL DATA

Contracts and other documents containing personal data in physical form must be stored in a locked area (drawer, cabinet, safe, file cabinet, office, storage room, etc.) in the building to prevent unauthorized access by third parties. Active Sports Reisen is required to ensure that only employees, the controller, or persons authorized by the controller, who are bound by the obligations under this Directive, have access to these areas.

If personal data is stored in physical form, the controller is required to dispose of the personal data after the purpose and legal obligation for archiving have been fulfilled. In the event of absence from the building (after working hours), it is the responsibility of the last person to leave the building that day to ensure all documents containing personal data are locked in a secure area.

The controller and employees must ensure that documents do not compromise personal data protection, especially regarding the risk of reusing previously used paper and handling used and unnecessary documents containing personal data, which cannot be discarded with regular waste but must be properly shredded.

2. ELECTRONIC RECORDS OF PERSONAL DATA

Active Sports Reisen may use external IT services to manage networks, computers, phones, mobile devices, etc., during its operations. These individuals may have access to personal data of data subjects. The controller is committed to ensuring that these individuals are bound by confidentiality regarding all information they may come across during their work.

The controller is required to implement a firewall and antivirus software to ensure data security in the computers located at Active Sports Reisen.

The controller must also ensure regular updates to programs and operating systems to maintain data security in the computers used by Active Sports Reisen.

If personal data is stored electronically on recording devices, Active Sports Reisen is required to remove this data after the purpose and legal obligation for archiving have been fulfilled.

The controller and each employee are required to use passwords on their IT equipment to prevent unauthorized access.

The controller and employees are obliged to act in a way that minimizes the risk of personal data breaches when using electronic communication, ensuring that emails are sent only to the intended recipient and not to third parties.

3. PROTECTION OF EMPLOYEE PERSONAL DATA

Employee personal data must not be used for any purpose other than for which it is intended.

The employee acknowledges that the use of their personal data is assumed to be based on a legal ground for processing personal data, contractual processing grounds. If no such grounds exist, and Active Sports Reisen wishes to use the employee's personal data, they must obtain prior written consent from the employee. Only the company's statutory body and other entities authorized by relevant

regulations to require these contracts have access to contractual documentation between Active Sports Reisen and employees. Active Sports Reisen is also authorized to provide contracts to the payroll accountant and tax advisor, particularly for recording hours worked, leave, and other employment-related matters, as well as to a person responsible for ensuring workplace safety.

The controller must not disclose employee data to third parties except in the cases mentioned in the Directive and legal regulations. This prohibition also applies after the termination of employment.

4. PROTECTION OF CLIENT AND THIRD-PARTY PERSONAL DATA

Client personal data must not be used for any purpose other than that for which it is intended.

The client acknowledges that the use of their personal data is assumed to be based on a legal ground for processing personal data, contractual processing grounds. If no such grounds exist, and Active Sports Reisen wishes to use the client's personal data, it must obtain prior written consent from the client.

Active Sports Reisen and the controller are committed to ensuring that documentation is managed so that no third party has access to it.

Active Sports Reisen is required to archive documentation in accordance with the law and special regulations, ensuring that only the controller or an authorized employee or person has access to the documentation. After the archive period has expired, Active Sports Reisen is required to shred documents, possibly using third-party services. Active Sports Reisen is not required to shred documents if there is a reason to retain them.

Employees and authorized persons must ensure that they handle all personal data of clients or third parties that they come into contact with in the course of their work activities in accordance with the controller's instructions and the Directive.

5. RECORD OF PROCESSING ACTIVITIES

The controller is required to keep records of processing activities for which they are responsible. These records must include:

- a) The name and contact details of the controller and any joint controller, the controller's representative, and the data protection officer, if one is appointed;
- b) The purposes of the processing;
- c) A description of the categories of data subjects and the categories of personal data;
- d) The categories of recipients to whom personal data has been or will be disclosed, including recipients in third countries or international organizations;
- e) Information on any transfer of personal data to a third country or international organization, including the identification of that third country or international organization;
- f) Where possible, the planned retention periods for each category of data; where possible;
- g) Identified incidents, including the action taken.

The controller will allow customers and employees to view the Record of Processing Activities related to their data, which will be accessible in the Active Sports Reisen building. If a data subject requests access to the Record of Processing Activities, the controller will ensure its electronic delivery regarding the data concerning the subject.

The Record of Processing Activities may be kept in written or electronic form.

6. INCIDENT REPORTING

The supervisory authority is the Datenschutzbehörde Republik Österreich.

If the controller becomes aware of a personal data breach, they are required to internally record the incident in the Record of Processing Activities, including the corrective action taken.

If the incident could lead to a risk of misuse of personal data, the controller must report this to the supervisory authority within 72 hours of the incident. The notification must include:

- a) A description of the nature of the personal data breach, including, where possible, the categories and approximate number of affected data subjects and categories, and the approximate number of personal data records concerned;
- b) The name and contact details of the data protection officer or other contact point where more information can be obtained;
- c) A description of the likely consequences of the personal data breach;
- d) A description of the measures taken or proposed to address the personal data breach, including, where appropriate, measures to mitigate any adverse effects.

7. RECORD OF DATA SUBJECTS

The controller keeps an internal record of data subjects. This record may be kept in written or electronic form. Together with the Record of Processing Activities, it serves to ensure the highest level of protection for clients' and employees' personal data. This record is also used as a basis for reporting incidents in the Record of Processing Activities.

8. EMPLOYEE TRAINING

Active Sports Reisen is committed to regularly training employees on GDPR-related issues. During the training, employees will be informed about the latest GDPR issues, including the current version of the Directive. Training may also include updates to the Directive in Active Sports Reisen's internal system.

When a new employee is hired under an employment contract, work agreement, or employment service, Active Sports Reisen will familiarize them with this Directive and related documents.

9. CONFIDENTIALITY

The controller is bound by the obligation of confidentiality concerning information about data subjects and is not authorized to use this information for purposes other than those specified in the Directive.

Active Sports Reisen commits to ensuring that all employees are bound by the obligation of confidentiality regarding all personal data of third parties they encounter in the course of their work.

Active Sports Reisen also commits to ensuring that all personal information is stored in a secure location that is not accessible to external parties (e.g., a party responsible for cleaning the premises). If some information is still accessible to an external party and its security cannot be ensured, Active Sports Reisen commits to ensuring confidentiality for these external parties as well; in such cases, these parties will be informed of their obligations under the Directive.

10. SURVEILLANCE SYSTEM

Active Sports Reisen does not operate a surveillance system on the premises.

11. GPS MONITORING OF VEHICLES

Active Sports Reisen does not use GPS monitoring of company vehicles.

12. DATA SUBJECT AWARENESS

If a data subject believes that their personal data is being unlawfully processed, they may lodge a complaint with the supervisory authority, the Datenschutzbehörde Republik Österreich.

Data subjects will be informed about the possibility of familiarizing themselves with this Directive.

Madseit, as of September 1, 2024.