

## AIS-Salzburg Data Protection Policy

### I. Introduction

This Data Protection Policy describes how personal data must be collected, handled and stored to meet the data protection standards established by the European Union (EU) Regulation 2016/679 with regard to the processing of personal data and on the free movement of such data. This regulation is referred to as the GDPR.

This policy is to provide a general framework whereby an adequate level of protection of personal data of students, parents and legal guardian of students, employees, and contractual partners of AIS-Salzburg is ensured in its processing.

This policy provides guidelines to ensure that AIS-Salzburg:

1. complies with the EU data protection laws (GDPR);
2. protects the rights of employees, students and parents and other contractual partners;
3. is transparent about how it stores and processes individuals' personal data;
4. adequate safeguards are in place to protect itself and others whose personal data is processed from risks such as breaches of confidentiality, reputational damage and appropriate choice of data usage.

To these ends, the actions of all staff who have access to any type of personal data must comply with this policy.

### II. Types of Client Data Collected at AIS-Salzburg

Client/Student data include but are not limited to:

1. Client's contact details (i.e., name, surname, business or residential address, telephone number, e-mail address) for marketing purposes.
2. Student exam and other academic results, date of birth, evaluations results, grade, pictures, and movies, social/behavioral commentary and health/medical data.
3. All client data that has been obtained by the client in the course of discussing or performing professional educational services and data obtained from any sources that are necessary for the performance of professional educational services and consequently for invoicing purposes as per the requirements of the applicable laws, including financial data, personal identification numbers, etc.
4. All client data obtained from a client in the course of provision of professional educational services.

This information is required in carrying out the duties of the school and its educational mission.

Examples of personal data collected (not exhaustive):

- a. name and surname
- b. full name of family members
- c. address (home/residence)
- d. profession/job title
- e. training/diplomas/studies
- f. date and place of birth
- g. citizenship
- h. passport/identity documents
- i. birth certificate data
- j. health data
- k. telephone/fax
- l. e-mail address
- m. image
- n. gender
- o. physical data
- p. habits, preferences, behavior
- q. economic and financial situation
- r. family status
- s. military status
- t. civil status data
- u. bank data
- v. voice
- w. signature
- x. academic background, evaluations, results, and details of experience
- y. CCTV images and recordings of staff, personnel, students, and visitors to the school

### **III. Data Processing Requirements and Purposes**

The principles of lawfulness, fairness, and transparency are fundamental to all data collection and processing at AIS-Salzburg. There must be a legitimate, defensible basis for which the processing of all personal data occurs, including consent from the data subject and clear necessity for compliance with legal obligations to which the school must adhere. All data collection processing and its purpose must also be clearly explained in understandable communication with the clients of AIS-Salzburg.

The processing of personal data must comply with all applicable laws and in conformity with the following principles:

1. Processed fairly, lawfully and in a transparent manner;
2. Processed only for limited, specified and lawful purposes;
3. Adequate, relevant and limited to what is necessary in relation to purposes;
4. Accurate and kept up-to-date;
5. Not kept longer than necessary;
6. Processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;
7. Disclosed only if required by the data subject, applicable law or regulation;
8. Transferred only to countries with adequate protection or to entities offering adequate protection.

AIS-Salzburg will collect personal data for specified, explicit and legitimate purposes and not process the data further than for the purpose, for which it was collected. AIS-Salzburg can process personal data only if one of the following circumstances is met:

1. With the explicit and unambiguous consent of the individual to whom the data relate;
2. Where necessary, to execute a contractual relationship
3. When necessary, to protect the legitimate interests and rights of the individuals;
4. Where necessary, for the purposes of the legitimate interests of AIS-Salzburg without prejudicing the rights, freedoms or legitimate interests of the persons to whom the data relates;
5. Where necessary to fulfill applicable laws.

AIS-Salzburg will process only data that is adequate, relevant, limited to and necessary for the purposes of professional education in a boarding setting.

AIS-Salzburg is obliged to ensure that all personal data is accurate and up-to-date where required.

AIS-Salzburg will not retain personal data for a longer period than what is necessary for the purposes for which it was collected and processed.

AIS-Salzburg will only transfer personal data outside the European Economic Area where there are appropriate safeguards in place, such as the right contractual framework.

Data subjects rights will be adhered to by AIS-Salzburg. All data subjects have the right to access a copy of the personal data we hold on them.

Both AIS-Salzburg as well as any data processor authorized by AIS-Salzburg, shall keep the confidentiality of the personal data, under the requirements of the law, will not disclose, publish or otherwise reveal any information relating to personal data and operations performed without an appropriate legal basis allowing them to do so. Data processors authorized by AIS-Salzburg shall disclose personal data only with AIS-Salzburg authorization, unless a legal obligation imposes data processors to act otherwise.

In case of loss or leakage of personal data or suspicions of potential loss or leakage of personal data to unauthorized persons, AIS-Salzburg shall inform the competent authorities and the relevant persons accordingly.

AIS-Salzburg will maintain data security by protecting the confidentiality, integrity and availability of the personal data. Confidentiality will be maintained by limiting access only to those authorized to access it. Integrity will be protected by ensuring that the personal data is accurate and suitable for the purposes for which it was collected and processed. Personal data will be made available to authorized users if they require it for authorized purposes.

### **IV. Sensitive Data Processing**

AIS-Salzburg prohibits the collection or processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, physical or mental health data, trade-union membership, and the processing of data concerning health or sex life, unless:

1. The individual has given explicit consent of the processing thereof.

2. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
3. Processing of personal data relates to data which are manifestly made public by the data subject.
4. Processing is necessary for preventative medicine, for the assessment of the appropriateness of participation in educational programming, for medical diagnosis, for the provision of health or social care or treatment or the management of health or social care systems and services on the basis of the European Union or member state law or pursuant to contract with a health professional.

## **V. Individual Notification**

AIS-Salzburg will inform individuals of this data protection policy with notice concerning:

1. the purposes for which their personal data are processed.
2. other relevant information: the nature and categories of the processed personal data, the categories of third parties to which the personal data are disclosed and how and when individuals can exercise their rights.

## **VI. Consent**

The consent of the client is defined by the GDPR as '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.' AIS-Salzburg will keep records of valid consent throughout the enrollment period of any client.

## **VII. Withdrawal of Consent**

Data subjects have the right to withdraw his or her consent at any time. AIS-Salzburg accepts a written statement signed by the data subject which specify the exercise of the right of withdrawal of the consent. It should be forwarded to office@ais-salzburg or by mail using the school's street address: Moosstrasse 106, 5020 Salzburg, Austria.

## **VII. Data Use**

1. When working with personal data, authorized employees of AIS-Salzburg will ensure that the screens of their personal computers are always locked when left unattended.
2. Personal data will not be shared informally and never sent by e-mail.
3. Data will be encrypted before being sent electronically.
4. Authorized employees will not save copies of personal data on their own computers; they will only access and update the central copy (PowerSchool).
5. Personal data will not be disclosed to unauthorized persons, either within AIS-Salzburg or externally.
6. Data will be regularly reviewed and updated if it is found to be out-of-date. If no longer required, it will be deleted.
7. Only those authorized employees who require access to personal data in the functioning of their responsibilities will be granted access by the Data Protection Officer.

## **VIII. Data Storage**

Personal data will be stored at AIS-Salzburg in such a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods so far as the data will be processed solely for archiving purposes in the client's or public interest or for scientific, historical, or statistical purposes with appropriate safeguards.

All personal data stored will be in such a manner that ensures appropriate security against unlawful processing and accidental loss, destruction or damage.

Security measures in place at AIS-Salzburg:

1. Users will always lock their laptop/desktop when moving away from the computer.
2. Users will never attempt to circumvent computer or server security or gain access to a system for which they have no authorization.
3. Servers and workstations will be protected by using security software and firewall rules.
4. Servers are located in places specially equipped with access and environmental controls and will be inaccessible to unauthorized individuals.
5. Data will be frequently and regularly backed up.
6. Employees of AIS-Salzburg must use strong passwords which are frequently changed. All passwords must be kept confidential by all employees.
7. Access to the IT systems at AIS-Salzburg are granted on a 'need to know' basis, based upon privileges required to perform specific duties.

Security for printed data at AIS-Salzburg:

1. Users working in departments that handle confidential information will lock and secure all information and equipment when they are away from their desk areas.
2. Access controls are implemented throughout the school and are applied to all employees, clients, contracted partners, and visitors to the school.
3. Retention and disposal schedules are in place to ensure legal compliance with GDPR as well as protect personal and intellectual property.

#### **IX. Data Accuracy**

Personal data stored and processed at AIS-Salzburg will be updated to be kept as accurate as possible. Inaccurate data will be discarded or deleted immediately. All employees at AIS-Salzburg will maintain vigilance in an effort to ensure that all stored data is accurate.

#### **X. Transfer of Data to Third Parties**

Authorized employees of AIS-Salzburg will remain vigilant in their transferral of personal data for purposes specifically required by professional educational practice and supported by the school's mission. In all cases where possible, authorized employees will evaluate, with the assistance of the IT Coordinator, the security of all transfers in or outside of the EU and implement appropriate safeguards as required by the GDPR.

The AIS-Salzburg college counselor will require that third parties in reception of personal data (e.g., universities, medical officials) prove that appropriate security measures are in place for the transfer of such data as well as the submission of further data that relies upon stored and processed personal data from clients of AIS-Salzburg.

The AIS-Salzburg office administration will ensure that all contracted partners and clients with which personal data is transferred prove secure systems are in place for such transferral. In all such cases, such transfers will take place only through transparent necessity in meeting the school's professional educational goals and mission.

#### **XI. Data Protection Officer (DPO) at AIS-Salzburg**

The Data Protection Office at AIS-Salzburg is Mr. Paul McLean, [pmclean@ais-salzburg.at](mailto:pmclean@ais-salzburg.at), AIS-Salzburg, Moosstrasse 106, 5020 Salzburg, Austria. The DPO is required to:

1. keep the administration of AIS-Salzburg updated about all data protection responsibilities, risks and other issues.
2. Review all data protection procedures and related policies.
3. Arrange data protection training and advice to employees responsible for processing personal data.
4. Deal with requests from individuals to see the data AIS-Salzburg stores on them ('subject access requests')
5. Checking and approving any contracts or agreements with third parties that may handle our sensitive data.
6. Control and monitor all data protection procedures.
7. Stay informed of all data protection laws and procedures.

#### **XII. Employees with Access to Personal Data at AIS-Salzburg**

1. Only access personal data to the extent necessary to serve the applicable legitimate purposes for which AIS-Salzburg processes personal data and to perform their job.
2. Report any incident or issue relating to the security of personal data to the DPO.
3. Never discuss confidential information in public areas or with individuals who do not have the need to know.
4. Dispose of sensitive documents properly.
5. Power off computing devices when not in use for extended periods.
6. Lock and secure all information and equipment when they are away from their desk areas.
7. Keep all secure information out of sight or view when away from their desks.
8. No storage of passwords in plain text.
9. Promptly report and suspected breach of security that comes to their attention.
10. Consult the DPO whenever they have concerns about data privacy.

#### **XIII. IT Manager at AIS-Salzburg with Access to Personal Data**

1. Ensure that all systems, services and equipment used for storing data meet acceptable security standards.
2. Perform regular checks and scans to ensure security hardware and software is functioning properly.
3. Evaluate any third-party services AIS-Salzburg is considering using to store or process data in order to ensure the integrity, confidentiality and availability of processed data.
4. Identify and implement technical measure to ensure the security of personal data stored.
5. Provide support for investigating potential breaches of security.
6. Provide personnel assistance on technical and security standards for the processing and protection of personal data.

#### **XIV. Admissions and External Relations**

1. Ensuring that the marketing strategies comply with the principles of this policy.
2. Ensure that personal data databases used for marketing purposes is accurate and up-to-date.
3. Work with other organization representatives to ensure that marketing initiatives respect the principles of personal data protection.
4. Coordinate any requests of media regarding the protection of personal data.
5. Ensure any statement of personal data that accompanies advertising material, or is used in communication channels (e-mail, letters).

#### **XV. Data Subject Rights**

In the collection of personal data directly from the data subjects to whom it relates, AIS-Salzburg will make sure that those persons are aware of the following at the time when personal data are obtained:

1. The identity and the contact details of the DSO.
2. The purposes of the processing and legal basis
3. The legitimate interests pursued by the school or a third party, where applicable.
4. The recipients or categories of recipients of the personal data, if any.
5. The fact that the school intends to transfer personal data abroad and the existence or absence of an adequacy decision, where applicable.
6. The period for which the personal data will be stored, or criteria used to determine that period.
7. The existence of the rights of the data subject: to request access to and rectification or erasure of personal data, or a restriction on processing or to object to processing, the right to data portability, the right to withdraw consent at any time, and the right to lodge a complaint with a supervisory authority.
8. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data, and the possible consequences of failure to provide such data.