



Data Protection Policy


Edition: 1

Revision: 0

Approved by:

Date: 25/8/2018


<b>1. Introduction</b>	4
<b>2. Objective</b>	5
<b>3. Scope</b>	6
<b>4. Terminology</b>	8
<b>5. Abbreviation</b>	10
<b>6. Personal data processing rules</b>	11
<b>7. Responsibilities</b>	19
<b>8. Data subject rights</b>	23

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

## 1. Introduction

Vienna International School, hereinafter "**VIS**", by the nature of the activities performed, collects and uses certain personal data from individuals who may be parents, students, suppliers, business contacts, employees and other individuals the organization has a relationship with or may need to contact.

The Data Protection Policy (hereinafter "**policy**") describes how personal data must be collected, handled and stored to meet the VIS' data protection standards and to comply with the Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**").

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018


## 2. Objective

The policy aims to provide the general framework for ensuring an adequate level of protection for personal data of students, parents or legal guardians of students, employees, and contractual partners processed by VIS.

In addition, the policy provides guidelines to ensure that VIS:

- a) complies with data protection law, with GDPR and follows good practice;
- b) protects the rights of employees, students and parents and other contractual partners;
- c) is transparent about how it stores and processes individuals' personal data;
- d) adequate safeguards are implemented to protect itself and individuals whose personal data it processes from the risks associated to personal data processing activities, such as:
  - **Breaches of confidentiality.** For instance, disclosure of personal data to third parties due to lack of/ ineffective implementation of security controls or resulting from inappropriate given out of information.
  - **Reputational damage.** For instance, VIS could suffer if hackers successfully gained access to sensitive data or individuals who are affected by how VIS uses their personal data.
  - **Failing to offer choice.** For instance, all individuals should be free to choose how VIS uses data relating to them.

In order to prevent and reduce the risks associated with the collection and processing of personal data, it is mandatory for all staff who have access to any type of personal data to ensure that all their actions comply with the guidelines set out by this policy. The policy will be communicated to all employees via email and / or displayed on the Intranet (internal electronic information system).

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

### 3. Scope

The policy applies to:

- a) All staff and volunteers of VIS.
- b) All contractors, suppliers and other people working on behalf of VIS.
- c) All client data – student / parents


#### **Employee data include, but are not limited to:**

- Employees' status and education (i.e. name, surname, address, date of birth, family details, telephone number, pictures, identification number, education certificates and diplomas, visa and other residency permits);
- Employees' job history and current job data (i.e. job certificates issued by ex-employers, curriculum vitae, offer letter, compensation, promotions, awards and benefits, disciplinary records, performance appraisals, employer feedback, absence form);
- Employees' training courses, professional certificates; skills inventory (including industry and service line specializations);
- Employees' time and expenses;
- Employees' information regarding insurances (i.e. medical claims; medical certificate; travel insurance; pension insurance);
- Employees' financial information (i.e. bank number; pension funds; investments);
- Employees' electronic correspondence and telephone communications.

The collection of the above-mentioned employee data is mandatory since it is needed for the contractual agreement of the employment relationship and the legitimate interest of VIS. If the employee refuses to provide the personal data without any reason or provides false personal data, the employee shall be subject, after prior assessment of the situation, to disciplinary procedures according to applicable local law.

#### **Client/student data include, but are not limited to:**

- Clients' contact details (i.e. name, surname, business or residential address, telephone number, e-mail address) for marketing purposes;
- Student exam results, date of birth, evaluations results, grade, pictures and movies, health data;
- All client data that has been obtained from the client in the course of discussing or performing professional services and data obtained from any sources that are necessary for the performance of professional services and consequently for invoicing purposes as per the requirements of the applicable laws – including various financial data, personal identification numbers etc.;

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

- All client data required by the applicable laws regarding the scope of an agreement concluded with the client or applicable anti-money regulations.

All client data obtained from a client in the course of provision of services.

This list is not exhaustive and can be amended subject to changes in the applicable laws.

Personal data examples	
<ul style="list-style-type: none"> <li>• name and surname</li> <li>• full name of family members</li> <li>• address (home/residence)</li> <li>• profession/job title</li> <li>• training/diplomas/studies</li> <li>• date and place of birth</li> <li>• data on owned assets</li> <li>• Pension file no.</li> <li>• telephone / fax</li> <li>• nickname / alias</li> <li>• e-mail</li> <li>• image</li> <li>• gender</li> </ul>	<ul style="list-style-type: none"> <li>• geolocation data</li> <li>• data from driver's license / certificate of registration</li> <li>• physical / anthropometric data</li> <li>• habits / preferences / behavior</li> <li>• economic &amp; financial situation</li> <li>• family status</li> <li>• military status</li> <li>• civil status data</li> <li>• bank data</li> <li>• voice</li> <li>• citizenship</li> <li>• signature</li> </ul>

This policy was adopted by the VIS Board of Governors and shall enter into force as of the 25th of May 2018 ("Effective Date") and shall be published on the VIS intranet and be made available to employees, clients or business partners upon request.

The policy shall apply only where it provides supplemental protection for personal data processed by VIS. Where applicable local law provides more protection than this policy, local law shall prevail.


#### CREDITORS

##### Categories of data:

the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- Name and address and contact details
- PPS number and tax details
- bank details and amounts paid

Purposes:

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

Lawful basis for processing:

For the performance of a contract for certain types of information. Legal basis where the College is required to act as Principal Contractor under Relevant Contracts Taxation regulations set out by the Revenue Commissioners.

Location:

In a secure, locked office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security:

In a secure, locked filing cabinet for paper files. In a secure locked server room for computer files. Computer records are password protected and firewall protected.

Is any of this data passed on? If yes, to what purpose?

Relevant data is passed onto the Revenue Commissioners and may be passed to our Auditors where relevant in the performance of their duties.

How long do we keep the information?

Data Retention Policy.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

## CCTV images/recordings

CCTV is installed in some external areas of the schools, as detailed in the CCTV Policy. These CCTV systems may record images of staff, pupils and members of the public who visit the premises.

### Purposes:

Safety and security of staff, pupils and visitors and to safeguard school property and equipment.

### Lawful basis for processing:

Legitimate interests.

### Security:

Only the system administrators (Technical Support Team) have access to the recorded video data.

Any use of recorded data such as viewing or transmission can take place only in specific cases of suspicion and at the explicit directive of the Director or Business Manager of the Vienna International School. The Betriebsrat shall be informed of any such planned access to the recorded data. Access can take place only in the presence of a Betriebsrat member.

In any case it will be deleted seven days after being recorded, except in cases where VIS has a legal obligation to keep the recorded data.

### Is any of this data passed on? If yes, to what purpose?


- no

### How long do we keep the information?

- See Data Retention Policy.

## 4. Terminology


- a) 'client' - the existing or potential clients (i.e. parents, students, visitors) of VIS and employees, partners, directors, agents of legal entities who are considered to be "data subject(s)" for the purpose of this policy.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

- b) **'employee(s)'** – any individual hired, formerly hired, including administrative staff, self-employed or contract personnel, temporary or seconded staff, voluntary workers and retirees.
- c) **'personal data'** - any information relating to an identified or identifiable natural person; 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;
- d) **'processing'** - 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;
- e) **'restriction of processing'** - the marking of stored personal data with the aim of limiting their processing in the future;
- f) **'controller'** - the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- g) **'processor'** - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- h) **'recipient'** - a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 L 119/33 Official Journal of the European Union EN framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- i) **'third party'** - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- j) **'consent'** - 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;
- k) **'personal data breach'** - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- l) **'representative'** - a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;


Any additional terms related to data protection shall have the meaning designated to them under article 4 of the GDPR.



	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

## 5. Abbreviation

- a) DPO - Data Protection Officer
- b) GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and follows good practice;

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

## 6. Personal data processing rules

VIS is committed to adhering to the data protection principles set out by the GDPR. These principles are:

**Lawfulness, fairness and transparency;** this means that we should have a legitimate basis for which we are processing personal data, for example consent from the data subject, or that the processing is necessary for compliance with a legal obligation to which we are subject. It also means that we should inform the data subject about the processing in accessible and easy to understand communication.

The processing of personal data shall comply with the applicable laws and with the below-mentioned principles:


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

**Purpose Limitation;** we should only collect personal data for specified, explicit and legitimate purposes and not process the data further than for the purpose, for which it was collected. VIS can process personal data only if one of the following circumstances is met:

- With the explicit and unambiguous consent of the individual to whom the data relate;
- Where necessary, to execute a contractual relationship or the pre-contractual (employment contract included);
- When necessary, to protect the legitimate interests and rights of the individuals;
- Where necessary, for the purposes of the legitimate interests of VIS; however, if doing so would materially prejudice the rights, freedoms or legitimate interests of the persons to whom the data relate, VIS will not process employee data purely for the purposes of their own legitimate interests;
- Where necessary, to fulfill applicable laws;

**Data Minimisation;** the personal data processed should be adequate, relevant and limited to what is necessary in relation to the purposes.

**Accuracy;** we have an obligation to ensure that personal data is accurate and to keep personal data up to date, where required.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

**Storage Limitation;** we should not retain personal data for a longer period than what is necessary for the purposes for which it was processed. We should set retention periods for the personal data we process.

**Integrity and Confidentiality;** we should have the right security controls in place to protect against unauthorised and unlawful processing and against accidental loss or destruction of, or damage to personal data. This includes both technical and organisational measures such as defined processes and training and awareness.

**Lawful transfer outside the European Economic Area;** we should only transfer personal data outside the European Economic Area where there are appropriate safeguards in place, such as the right contractual framework.

**Data Subject Rights;** data subjects have a number of rights that we should adhere to, for example the right to access a copy of the data we hold on them, and the right to opt out of direct marketing, which they have previously opted into.

Both the VIS and any data processor authorized by VIS, 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. Furthermore, data processors authorized by VIS shall disclose personal data only with the VIS's authorization, unless a legal obligation imposes data processors to act otherwise.


VIS has in place policies and procedures, which define the fundamental principles and practices of VIS in order to ensure confidentiality, integrity and availability of information in electronic and hard copy format, and security of operating processes.

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

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised can access the data.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Full details of our security policies can be found in the organisation's suite of IT guidelines and procedures.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

## 6.1 Processing sensitive data

VIS prohibits the processing of personal 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:

- The individual has given his explicit consent to the processing thereof
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protections law in so far as authorized by the European Union or member state law or a collective agreement pursuant to member state law
- 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
- Processing of personal data relates to data which are manifestly made public by the data subject
- Processing is necessary for the preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, 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.


## 6.2 Consent

The consent is defined at Art. 4 (11) of 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*”.

### 6.2.1 Principles

**Consent must be freely given:** should reflect the data subject's genuine and free choice without any element of compulsion, or undue pressure put upon the data subject, avoiding any negative consequences in the case of refusal to give it.

- Consent must be specific: VIS must clearly and precisely explain the scope and the consequences of the data processing.
- Consent must be informed: the nature of the processing should be explained in an intelligible and easily accessible form, using clear and plain language which does not contain unfair terms. The data subject should be aware at least of the identity of the controller and the purposes for which the personal data will be processed.
- Consent must be explicit: VIS uses written declarations, e-mail responses, and active checkboxes.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

### 6.2.2 Individual specific consent

Explicit consent is necessary when VIS processes sensitive categories of data (e.g., medical, genetic, biometric data, 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).

In order to obtain explicit consent, VIS accepts a written statement signed by the data subject. Additionally, controllers are required to keep records in order to demonstrate that a valid consent has been given and that the data subject has been informed.

### 6.2.3 Direct marketing

VIS shall engage in unsolicited commercial communication (direct marketing communication) only with the prior consent of the Individual ("opt-in"). In every direct marketing communication that is made to the individual, the individual shall be offered the opportunity to opt-out of further direct marketing communication. Personal data collected by VIS will never be disclosed to a third-party company who intends to use it for direct marketing purposes unless specific consent has been given by data subject.

### 6.2.4 Objection to direct marketing

If an individual objects to receiving marketing communications, or withdraws his consent to receive such materials, VIS will take steps to refrain from sending further marketing materials as specifically requested by the individual. VIS will do so within the time period required by applicable law.


VIS accepts a written statement signed by the data subject which specifies the exercise of the right to object to direct marketing. It should be forwarded to VIS at [dpo@vis.ac.at](mailto:dpo@vis.ac.at) or by mail using the following contact details Strasse der Menschenrechte 1, 1220 Vienna.

Additionally, VIS keeps records to demonstrate that a valid consent has been given and that the data subject has been informed.

### 6.2.5 Withdrawal of consent

Data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. VIS has the obligation to make it easy for individuals to withdraw consent.

VIS accepts a written statement signed by the data subject which specify the exercise of the right of withdrawal the consent. It will be forwarded to VIS at [dpo@vis.ac.at](mailto:dpo@vis.ac.at) or by mail using the following contact details Strasse der Menschenrechte 1, 1220 Vienna.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

Additionally, VIS keeps records in order to demonstrate that a valid consent has been given and that the data subject has been informed.

### 6.3. Individual notification

VIS must inform individuals through a data protection policy or notice about:

- the purposes for which their personal data are processed;
- other relevant information (e.g., the nature and categories of the processed personal data, the categories of third parties to which the personal data are disclosed (if any) and how individuals can exercise their rights).

For this purpose, VIS informs the data subjects at various moments of interactions with data subject such as: agreement signing, applying for a job with VIS etc.

### 6.4 Data use


Personal data is of no value to VIS unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Personal data should not be disclosed to unauthorized people, either within VIS or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their department manager or the Data Protection Officer if they are unsure about any aspect of data protection.
- The only people able to access data covered by this policy should be those who need it for their work.
- When access to confidential information is required, employees can request it from their department managers.

VIS will provide training to all employees to help them understand their responsibilities when handling data and to implement this policy.

### 6.5 Data storage

Personal data must be kept in a form that permits identification of data subjects for no longer than is 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

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

purposes in the public interest, or scientific, historical, or statistical purposes in accordance with subject to the implementation of appropriate safeguards.

Data storage is the processing operation that consists in keeping personal data collected by VIS on any support (electronic or paper).

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Security measures for the electronic data:


- User should always lock laptop/desktop by pressing Ctrl+Alt+Del while moving away from computer
- User should not circumvent computer security or gain access to a system for which they have no authorization
- Servers and workstations will be protected by using security software and implementing firewall rules;
- Servers will be located in places specially equipped with access control and environmental controls, inaccessible to unauthorized persons;
- Data must be frequently backed up and these copies must be periodically tested to ensure data recovery;
- Employees must use strong passwords for the computer applications used, in accordance with the domain password configuration rules. Passwords must be kept confidential and changed regularly;
- The access to IT systems (to personal data) will be granted by the IT department according to the "need to know" principle, based on privileges required to perform their duties.

Security measures for the printed data:

- Users working in departments that handle confidential information should lock and secure all information and equipment when they are away from their desk areas.
- Access controls are implemented as required, to monitor and restrict access for individuals to areas to which access is required for business purposes. These restrictions are applied as required to VIS employees, including contractors, visitors and other relevant identified third parties;
- VIS will establish retention or disposal schedules for specific categories of records in order to ensure legal compliance, and also to accomplish other objectives, such as preserving intellectual property and cost management.

## 6.6 Data accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

without delay. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Best practices:

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets;
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a parent's details when they call;
- VIS will make it easy for data subjects to update the information. For instance, personal data could be updated every year at re-enrolment.
- Data should be updated as inaccuracies are discovered. For instance, if a parent can no longer be reached on their stored telephone number, it should be removed from the database.

## 6.7 Transfer of personal data to third parties

VIS shall transfer personal data to a third-party controller to the extent necessary to serve the applicable legitimate purposes for which the personal data are processed. Transfer to a third party must be in accordance with the respective legal and regulatory requirements.

Data transfer is always allowed in the following situations:

- When the data subject has given his consent unambiguously to the proposed transfer;
- When the transfer is necessary for the performance of a contract between the data subject and VIS;
- When the transfer is necessary or legally required on important public interest grounds, such as national defense, public order or national security, for the purposes of criminal procedures or for the establishment, exercise or defense of legal claims, provided that the data to be processed is in connection with this purpose and are retained for no longer than necessary;
- When the transfer is necessary in order to protect the vital interests of the data subject (incl. life, physical integrity or health);
- When the transfer is a result of a previous request for access to official documents that are public or a request for information that can be obtained from registers or any other publicly available documents.


In addition to the cases mentioned above, as transfer are considered processing operation performed with regard to the personal data, such transfers shall be allowed whenever an appropriate legal basis for transfer is identified according to article 6 or article 9 (2) GDPR.

## 6.8 Transfer of personal data to third countries

VIS transfers personal data to the third countries, using cloud based services as follows:

- *United States of America* – to third parties that have obtain EU – US Privacy Shield certification (i.e. Faria Systems LLC as provider of the ManageBac and Open Apply applications). With other USA based providers of applications, VIS is in the process of



	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

implementing appropriate safeguards in order to ensure secure transfers of personal data by May 25, 2018.

- *India* - case in which VIS has chosen to contract with a trusted supplier and it is making all efforts to amend the agreement with this supplier in order to accommodate all the safeguards imposed by the data protection applicable legal provisions.

The appropriate safeguards put in place by VIS as regards the transfers of personal data to India or USA, can be consulted upon request made to the DPO.

In the absence of an applicable legal provision, VIS will transfer personal data only if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

VIS has published a list with systems that have been checked and can be used by school members for administrative and educational purposes. Those systems are necessary for the performance of the contract between the data subject and the controller.

## 7. Responsibilities


Any person authorized by VIS and VIS's employees that are involved in processing of personal data of data subjects or who have access to personal data in any way are required to comply with this policy.

Any VIS employee has responsibilities in terms of collecting, using and storing personal data properly. At the same time, the departments and teams are responsible for developing their own operational **rules/ procedures** to ensure that in terms of personal data the good practices are established and respected.

***It is also the responsibility of each employee to inform the VIS if any change occurs with respect to their personal data.***

### Data Protection Officer

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule;
- Arranging data protection training and advice for VIS' employees;
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data VIS holds about them (also called 'subject access requests');
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
- Have control and monitoring powers (the right to perform internal investigations and to access information);
- Have expert knowledge of data protection law and practices.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

### Employees with access to personal data


- Only access personal data to the extent necessary to serve the applicable legitimate purposes for which VIS processes personal data and to perform their job;
- Report of any (possible) incident or issue relating to personal data to their manager or to [dpo@vis.ac.at](mailto:dpo@vis.ac.at) ;
- Never discuss confidential information in public areas or with individuals who don't have a need to know;
- Dispose of sensitive documents properly;
- Computing devices should be powered off when not in use for extended periods of time (such as after work, on weekends, during holidays and so on);
- Users working in departments that handle confidential information should lock and secure all information and equipment when they are away from their desk areas;
- Users should keep their desk areas organized and keep all confidential information secured and out of view when away from their desks;
- Not sharing of passwords;
- Not storing the passwords in plain text;
- User should promptly report any suspected breach of security policy that comes to their knowledge;
- Consult the DPO and/or their direct manager whenever they have concerns regarding the data privacy.

### Board of Governors

- Establishing regular and transparent reporting mechanisms and reporting lines in order to monitor all substantial risks, including compliance risks in relation to data protection issues;
- The approval and periodic review, at least yearly, of this Policy and other data protection related policies based on the proposals / submitted by the responsible divisions.

### Director / Principal

- Ensuring that an adequate organisational structure is in place as well as effective communication and reporting channels, in order to ensure that personal data is being processed in a clear and consistent way and in compliance with the VIS's internal policies and procedures;
- Work together with and facilitate the appropriate DPO to create and maintain a framework for the development, implementation and updating of local data protection policies and procedures (including training and education);
- Ensuring the effective implementation of the required business management framework, including the establishment of mechanisms for developing and monitoring the

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

implementation of internal regulations to ensure that this policy is adequately implemented.

### Department Leaders/Managers


- Ensure that their Department will process personal data in accordance with this policy;
- Ensure that VIS staff is informed with regard to policies and procedures relevant to the protection of personal data;
- Ensure that personal data are processed in accordance with procedures and policies relevant to the protection of personal data;
- Notify the DPO and follow his/her advice on emerging risks or incidents;
- Ensure that the data inventory process is correct and complete. The data inventory of personal data must be updated periodically;
- Ensure that the staff working in his department follow the required training.

### IT Manager

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- Performing regular checks and scans to ensure security hardware and software is functioning properly;
- Evaluating any third-party services the company is considering using to store or process data in order to ensure the integrity, confidentiality and availability of processed data. For instance, cloud computing services;
- Identify and implement technical measures to ensure the security of personal data stored;
- Provide support for investigating potential breaches of security;
- Provide personnel training on technical and security standards for the processing and protection of personal data.

### Admissions & External Relations


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

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

## Human Resources

- Identifying the training and development needs of the staff in connection to the processing and protection of personal data;
- Ensures the inclusion of the training materials on personal data protection within the yearly training plan;
- Ensures support to the business units for implementing the training programmes regarding personal data processing and protection;
- Ensures that any action taken with regard to employee data is in line with the requirements of the Regulation. This applies to all processes managed by the human resources team, starting with recruitment process, implementation of the employment contract and to its termination.

In all these cases, the Human Resources Coordinator must be involved in the decision-making process and in assessing the impact of potential projects on the protection of employees' data. HR Coordinator must ensure a balance between the interests of VIS and the right to a private life of employees.

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

## 8. Data subject rights

### Right to be informed


When collecting personal data directly from the data subjects to whom it relates, VIS will make sure that those persons are aware of the following (except to the extent that it is obvious) at the time when personal data are obtained:

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the DPO, where applicable;
- The purposes of the processing and legal basis;
- The legitimate interests pursued by the controller or by a third party, where applicable;
- The recipients or categories of recipients of the personal data, if any (i.e. controllers, processors or other recipients);
- The fact that the Controller intends to transfer personal data abroad and the existence or absence of an adequacy decision, where applicable;
- The period for which the personal data will be stored, or criteria used to determine that period;
- 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 (where applicable), and the right to lodge a complaint with a supervisory authority;
- The existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- 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.

The above-mentioned information has to be provided also in case when the data have not been obtained directly from the data subject to whom it relates, with additional information from which sources the personal data originated, and if applicable, whether it came from publicly available sources. In such case the information has to be provided within reasonable period after obtaining the personal data (at the latest within one month) or at the latest at the time of the first communication to that data subject or at the latest when the personal data are first disclosed, if disclosure to another recipient is envisaged.

VIS will not provide information about processing where they reasonably consider that to do so would prejudice:

- The prevention, investigation, detection or prosecution of breaches of professional ethics or criminal offences;

	Data Protection Policy	Edition: 1
		Revision: 0
		Approved by: Date: 25/8/2018

- The material rights and freedoms of any person

### Other rights

Data subjects have the right to request access to their personal data and to obtain as appropriate the rectification or erasure of their personal data pursuant to applicable laws. Employees and clients/ students whose personal data are processed by VIS also have the following rights: right to rectification, right to erasure, right to restriction of processing or to object to processing, the right to data portability (where applicable), the right to withdraw consent at any time (where consent is the legal basis for processing). All above-mentioned rights can be enforced as provided by the "Data Subject's Rights Procedure".