FH Vorarlberg
University of Applied Sciences

Data Protection Handbook of FH Vorarlberg

TABLE OF CONTENTS

PREAMBLE

FH Vorarlberg embodies the highest standards of teaching and research. As a publicly funded company, we are also bound by the legal principles of economy, efficiency, and fitness for purpose, underpinned by the foundations of good conduct and lawfulness. We must continue to uphold these standards in how we comply with data protection regulations, guidelines, and legislation.

This handbook outlines the conditions that must be met when processing the personal data of students, (potential) applicants, partners, and employees. This defines the data protection and security standards that must be followed at every level of our organization.

Our employees are responsible for following this data protection policy and complying with any applicable data protection laws and regulations.

This handbook should not be viewed as a static document. It is constantly being revised and adapted to changes in the legislative requirements and our technical systems.

1. GENERAL PRINCIPLES

1.1 PURPOSE OF THE DATA PROTECTION HANDBOOK

FH Vorarlberg has an obligation to implement all data protection legislation. The regulations established below are guidelines intended to guarantee data protection at the University.
To comply with data protection regulations, it must be ensured that any individual entrusted with the processing of personal data at FH Vorarlberg is properly informed and instructed about the relevant issues. The data protection officer (DPO) is responsible for monitoring compliance with data protection measures.
This handbook aims to highlight the importance of data protection at FH Vorarlberg.

1.2 SCOPE

This data protection handbook defines measures for compliance with legal data protection regulations. The handbook is applicable to every process at FH Vorarlberg and represents a binding basis for the professional activities of every employee (project staff, part-time lecturers, etc.). The handbook applies to every current and future place of business of FH Vorarlberg, as well as every department and division.

1.3 RESPONSIBILITIES

All executive staff at FH Vorarlberg are responsible for the data processing performed within their respective areas of responsibility. Accordingly, they must ensure that the data protection measures outlined in this data protection handbook are properly observed.
Any individual conducting data processing at FH Vorarlberg is obliged to comply with the measures defined in this data protection handbook. The data protection officer of FH Vorarlberg must be immediately notified of any incident (or suspected incident) that may jeopardize the security of processed data. This duty of notification is essential, since any misuse or loss of data may incur serious consequences for FH Vorarlberg according to the current legislation.
The data protection officer is required to inform and advise executive management and their employees about their data protection duties, sensitize and train employees about data protection legislation, monitor and verify compliance with data protection regulations, and assist with data protection impact assessments. The data protection officer coordinates with the authorities and serves as their first point of contact.
The Information Services Department is responsible for implementing the appropriate technical and organizational measures to ensure compliance with the obligations which arise from the GDPR. In particular, compliance must be ensured by both technological means (data protection by design) and privacy-friendly default settings (data protection by default). The data protection officer must be notified and consulted whenever new systems are introduced.

1.4. DEFINITION OF PERSONAL DATA

“Personal data” refers to any information which relates to an identified or identifiable natural person. A natural person is identifiable if they can be identified by associating their data with an identifier such as a name, an identification number, location data, online identifiers, or one or several characteristic features which express their physical, physiological, genetic, mental, economic, cultural, or social identify.

1.5. DEFINITION OF DATA PROCESSING

Data processing is defined as any process or series of operations involving personal data performed with or without the aid of automated procedures. Examples of data processing operations include collecting, recording, organizing, ordering, storing, modifying or updating, reading, querying, using, disclosing via transfer, publishing or otherwise making accessible, comparing or consolidating, restricting, erasing, or destroying data.

2. PRINCIPLES OF DATA PROTECTION LAW

2.1. LAWFULNESS/TRANSPARENCY

When processing personal data, the personal rights of the data subjects must be respected. Personal data must be collected and processed in a lawful and understandable manner. Information on the processing of personal data must be provided in a precise, easily accessible and comprehensible form.

2.2. STATEMENT OF PURPOSE/DATA MINIMIZATION

Personal data must be processed lawfully, in good faith, and in a manner that can be reasonably understood by the data subjects. Data may only be collected for explicitly specified and legitimate purposes and may not be further processed in a manner incompatible with these original purposes. The data collected must be appropriately and materially limited to the extent required for the stated purpose of processing.

2.3. DATA MINIMISATION

Data processing must be limited to the specific required extent. Thus, no data processing may take place that is not required to fulfil the specified purpose. Where possible, data should be anonymised or pseudonymised.

2.4. ACCURACY/UP-TO-DATENESS

Personal data must be factually accurate and kept up-to-date wherever necessary. Appropriate measures must be adopted to ensure that incorrect data is erased or corrected.

2.5. STORAGE LIMITS

Personal data must be stored in a form that only allows data subjects to be identified for as long as necessary according to the stated purpose of processing. In particular, the retention periods of personal data must be set to the absolute minimally sufficient levels. The controller must define appropriate time frames for the deletion of data, as well as periodic reviews. The overall deletion policy of FH Vorarlberg must be followed.

2.6. INTEGRITY AND CONFIDENTIALITY

Personal data must be treated confidentially and secured against unauthorized access, unlawful processing, disclosure, loss, and damage by adopting appropriate organizational and technical measures. To ensure compliance with the confidentiality, all employees of FH Vorarlberg are obliged to keep confidential personal data that has been entrusted or become accessible to them solely on the basis of their professional capacity. This duty of confidentiality remains in effect even after conclusion of the employment agreement. In addition, all business partners are bound by a duty of confidentiality.

3. DATA USAGE AND DATA PROCESSING

3.1. LAWFULNESS OF THE PROCESSING

Personal data must be **lawfully** and transparently collected and processed. Processing is also subject to **purpose limitation** and may therefore be processed only for specified, clear and legitimate purposes. In addition, data should always be stored **properly and in an up-to-date state** and the **storage period** should be limited to the absolute minimum required (deletion periods).
In principle, data processing is legal if one of the following conditions is met (see Art. 6 EU GDPR)

- Consent (the data subject gives consent to processing for one or more specific purposes, such as taking photographs/videos)
- Contract fulfilment or for pre-contractual measures (e.g. student training contract)
- Fulfilment of a legal obligation to which FH Vorarlberg is subject (e.g. mandatory notifications to the Ministry, Statistics Austria etc.)
- Protection of public interests or
- Protection of the legitimate interests of FH Vorarlberg, unless the interests or fundamental rights and freedoms of the data subject that require protection of personal data prevail.

3.2. INSTRUCTIONS FOR DATA USAGE AND DATA PROCESSING

Personal data may only be used and processed on the instruction of a properly authorized person. A transparent allocation of responsibilities must be established by the head of each organizational unit. The instruction to perform a task may be given verbally, in writing, implicitly, and prior instructions may already exist.

3.3. CONTRACT PROCESSING

Contract processing refers to the situation where a contractor is commissioned to process personal data without taking on responsibility for the corresponding process. This could for example include external IT service providers, Digibon, hosting companies, but also includes services such as hired photographers. In any such case, a contract data processing agreement must be concluded with the external contractor.
The legal department of FH Vorarlberg offers support for this process (Edna Fitz, edna.fitz@fhv.at) and can be contacted whenever necessary. Any agreements concluded with the contractor must be scanned and forwarded to the person responsible for data protection (Edna Fitz, edna.fitz@fhv.at).
The contractor may only process personal data in accordance with the instructions of the client. The ability of a contractor to implement the necessary technical and organizational measure for data protection must be taken into account in the selection process.

3.4. MONITORING OF PROCESSING ACTIVITIES

All executive staff employed by FH Vorarlberg are responsible for any data processing activities performed within their respective areas of responsibility. These activities must be reviewed at regular intervals and adapted whenever necessary to reflect the latest requirements.
Whenever new business processes or research contracts are introduced or established, any processing activities must be identified and the key issues (controller, data types, data origins, data transfers, etc.) must be clarified. The results must be reported to the data protection officer, who records them in the directory of processes.
The procedure for updating existing processing activities and reporting any new activities is governed by the FHV internal procedure "OA-024 Reporting and maintenance of processing activities involving personal data".
This procedure represents a binding basis for every employee of FHV (https://inside.fhv.at/pages/viewpage.action?pageId=163732368).

3.5. LEGAL DECLARATION OF CONSENT

A declaration of consent is required whenever the collected data are not required to fulfil a contract or the processing activities performed by FH Vorarlberg do not arise from a statutory requirement, are not performed on the basis of a contractual relationship, or are not in the overriding legitimate interest of FH Vorarlberg.
A declaration of consent is valid only if the data subject was informed of his/her right to withdraw consent and are informed of who is responsible for processing the personal data and for what purposes the data is being processed.
Consent must be informed, voluntary, and unambiguous. For the sake of evidence, it is recommended to seek written consent (template).

Previously received consents continue to apply if they meet the requirements of the GDPR. It must be verified that the purpose of the data processing has been specified and that instructions on the right of withdrawal have been provided and that the consent is verifiable. Otherwise, new consent must be obtained.

4. RIGHTS OF DATA SUBJECTS

4.1. RIGHT OF ACCESS

Data subjects have the right to request information about whether the FH Vorarlberg is processing any of their personal data and, if so, which data. Any contact with the person requesting this information is the sole responsibility of the named data protection officer or their representative.
Every employee must refer any persons with requests relating to data protection exclusively to the dedicated point of contact for such requests at datenschutz@fhv.at. The person responsible for these requests (currently the legal department) must nevertheless be informed of any such request without delay.

4.2. RIGHT OF INFORMATION

If person data are collected from a data subject, the latter must be informed of the storage terms and purpose of the data collection, processing, or usage when the data are collected. Furthermore, the data subject must be informed of any party to whom the personal data will be disclosed and the purpose of disclosure, as well as the contact details of FH Vorarlberg (if the data subject does not already have them) and the details of the person of contact for data protection (datenschutz@fhv.at).

4.3. RIGHT OF RECTIFICATION

Data subjects have the right to demand the immediate rectification of any inaccuracies in their personal data, as well as the completion of any incomplete data.

4.4. RIGHT OF DELETION

Data subjects have the right to demand the deletion of their personal data. FH Vorarlberg will review any such requests together with the affected departments. Data may only be deleted if FH Vorarlberg no longer has a legitimate interest in continuing to keep them.

4.5. RIGHT OF OBJECTION

Data subjects have the right to object at any time to the processing of their personal data, which is based on the legal basis of the overriding legitimate interest of FHV.

4.6. HANDLING OF DATA PROTECTION REQUESTS

The FHV internal procedure "VA-057 Handling data protection requests" (https://inside.fhv.at/display/kompakt/VA-057+Datenschutzanfragen+abwickeln) outlines how access, rectification, and erasure requests should be processed in a standardized and timely manner. This procedure represents a binding basis for every employee of FHV.

5. NECESSARY MEASURES

5.1. PHYSICAL AND USER ACCESS PROTECTION

If a workstation is left unattended for an extended period of time, all sensitive and confidential documents must be securely stored in the desk (including storage media such as USB drives) and any computer terminals must be locked (e.g. using "Windows key + L" on PCs).
Any unoccupied office spaces must be kept locked. This is intended to prevent unauthorized persons from gaining access to the documents and IT equipment inside these spaces. For any work performed in a home office setting, appropriate measures must also be taken to ensure that documents concerning FH Vorarlberg are protected against unauthorized access.

5.2. LOGGING OF USAGE OPERATIONS

Wherever possible, records must be kept of any usage operations that have been performed, such as modifications, queries, and transfers, to allow retrospective verification that these operations were properly authorized.

5.3. MESSENGER SERVICES

Messenger services such as WhatsApp automatically involve the processing of personal data. For grounds of data protection, the use of WhatsApp must therefore be prohibited for official communications or communications with students.
This also applies to any other messenger services involving a transfer of contact data from the user's address book to the service provider, or which violate any other data protection measures.
The existing internal communication channels must be used for official communications.

5.4. E-MAIL COMMUNICATION AND DATA TRANSFER

a) No special precautions are necessary for e-mails between internal recipients (fhv.at, students.fhv.at and schlosshofen.at), as we have arranged special precautions for the protection of such data within the university.

b) Transmission to external recipients of e-mails that contain personal data already within the text or business and company secrets is permitted only if the messages themselves are encrypted.
Please note that recipients must also use the technical requirements for e-mail encryption and must apply them correctly. Another prerequisite is a proper digital signature exchanged in advance (by sending signed e-mails between the partners).

FH Vorarlberg typically provides each user with a personal certificate. For more information, please see https://inside.fhv.at/display/is/TCS+-+Persoenliche+Zertifikate (NB: PGP can also be used).

c) Transmission to external recipients of e-mails that contain personal data only in attachments is also permitted but only if the attachments are encrypted. For more information, please see https://inside.fhv.at/display/is/TCS+-+Persoenliche+Zertifikate.

Please note that the exchange of personal data with third parties is permitted only within the framework of corresponding contractual agreements (e.g. order processing agreement, an agreement pursuant to Art. 26 GDPR, confidentiality agreement). Transmission of content with special categories of personal data, as well as of confidential and secret information (business and trade secrets, data classifications C and D) should not take place via e-mail but should use another technical system. As part of arranging such data exchange, FH Vorarlberg strongly recommends establishing suitable teams on DropBox FHV and completely refraining from transmission via e-mail. For more information, please see https://inside.fhv.at/display/is/Dropbox+FHV.

5.5. DATA CLASSIFICATION

5.5.1. REGARDING THE NEED TO PROTECT PERSONAL OR CONFIDENTIAL DATA

The necessity to classify personal data arises from the EU GDPR. Data can be classified as "personal", "non-personal" and "special categories of personal data" (previously "sensitive data" in the Data Protection Act (DSG 2000)).

On this basis, personal data must be treated with the required confidentiality and integrity with regard to the general data protection regulations, regardless of whether the data belongs to students, employees, individuals taking part in events, contact persons, legal person or other persons with whom employees of FH Vorarlberg have contact. The requirements of data minimisation, transparency, correctness and storage limits must be observed.

In this regard, a protection level strategy for personal data is helpful.

In addition to documentation containing personal data, other internal documents with internal confidential information (business and trade secrets) are also subject to corresponding confidentiality obligations and the protection level strategy must be applied here as well.

5.5.2. REGARDING THE APPLICATION OF THE FH VORARLBERG DATA CLASSIFICATION SCHEME

Dealing with legacy data

The FH Vorarlberg data classification scheme was implemented in the fall of 2019. Data that were created or altered prior to this date are classified as “B: intern/internal”, unless they fall under the classifications “C: vertraulich/ confidential” or “D: geheim/secret” or they are already publically accessible.

Dealing with public data (data classification A: öffentlich/public)

Public data do not require separate classification.

In addition to conventional information accessible without special permission, (e.g. in printed media or on websites), public data also includes publications on social media.

It should be noted that all information that is transmitted to all or to a large group of students is also considered public within the meaning of this data classification scheme.

Dealing with restricted data (data classification B: intern/internal)

Restricted data do not require separate classification.

By definition, unclassified documents are classified as B: intern/internal if they are accessible only to employees or to a specific group of employees. The purpose of this regulation is to simplify the data classification.

In principle, by selecting the place of publication or specifying the explicit authorisation settings, the author must stipulate that data is accessible only to authorised and necessary individuals.

Dealing with confidential or secret data (data classification C: vertraulich/confidential and D: geheim/secret)

Documents of a confidential or secret nature must be explicitly classified by the author as "C: vertraulich/confidential" or "D: geheim/secret" and may be made accessible only to the directly necessary and entitled individuals.

The author must classify the data in such a way that the recipient immediately recognises this (e.g. at the beginning of a document or in the subject line of an e-mail).

Due to rapid technological progress, the documentation at https://inside.fhv.at/pages/viewpage.action?pageId=190291547 is binding.
The obligations regarding the role of the responsible person cannot be delegated but a substitute can be nominated.

5.5.3. DATA CLASSIFICATION SCHEME

Data classification	Definition	Application and examples
Data classification A: öffentlich/public	Data that are not subject to particular restrictions or that have already been published. Data is classified as public within the meaning of this scheme if it is made available to all internal users (employees and students) or a majority of them. Due to the large number of recipients, data on the intranet is also classified as public if the user group has not been explicitly restricted by the author to a specific group.	Data on the Internet, data in the company register, data available throughout FHV
Data classification B: intern/internal	Data for which no restrictions are required within an organisational unit but which require restrictions regarding access rights, processing and disclosure outside of the organisational unit.	e.g. in-house communication and other documents with no confidentiality
Data classification C: vertraulich/confidential	Data available only to a certain group of people and whose improper handling or dissemination could impair the persons concerned or FH Vorarlberg in terms of social position or economic situation ("reputation")	Data available only to a certain group of people; with regard to access, processing and transfer rights, the data are subject to corresponding restrictions. e.g. income data, data on social benefits
Data classification D: geheim/secret	Data available only to a very limited group of people and whose improper handling or dissemination could have a very negative impact on the people concerned or FH Vorarlberg in terms of social position or economic situation ("existence"). The data are subject to legal duty of confidentiality.	Only a very limited group of people has access, processing and transfer rights. e.g. official assessments, health records, debts/executions, research results to which confidentiality agreements apply

5.6. SECURE DISPOSAL OF DATA – DELETION POLICIES

Deletion policies for the deletion of personal data and the disposal of paper documents are required for all processing activities.

Deletion and disposal of paper documents must follow the deletion policies.

There are various means of disposing of paper documents, based on the information they contain.

Type of document	Data classification	Security level	Method of disposal/Security level according to Austrian standard (ÖNORM)
Data that are not subject to any particular restrictions and have already been published and **do not contain any personal information**.	Partial data classification A: öffentlich/public e.g. brochures, advertising material, newspapers, non-personalised invitations to events	P-1	Cardboard box
Data that are not subject to any **particular restrictions** and have already been published **and contain any personal information**.	Data classification A: öffentlich/public e.g. personalised advertising	P-1 to P-3	Document destruction box
Data for which no restrictions are required within an organisational unit but which require restrictions regarding access rights, processing and disclosure outside of the organisational unit.	Data classification B: Intern/internal e.g. in-house communication and other documents without high confidentiality	P-2 to P-5	Document destruction box or document shredder with P-2 security level (strip width max. 6 mm)
Data available only to a certain group of people and whose improper handling or dissemination could impair the persons concerned or FH Vorarlberg in terms of social position or economic situation ("reputation")	Data classification C: Vertraulich/confidential e.g. income data, data on social benefits, inquiries, quotations, personal data and files, student data other than those that fall under data classification D	P-4 to P-5	Document destruction box or document shredder with P-4 security level (max. 160 mm² particle area)
Data available only to a very limited group of people and whose improper handling or dissemination could have a very negative impact on the people concerned or FH Vorarlberg in terms of social position or economic situation ("existence"). The data are subject to legal duty of confidentiality.	Data classification D: Geheim/secret e.g. official assessments, health records, debts/executions, research results to which confidentiality agreements apply, secret R & D data, financial data, company management documents	P-5	document shredder with P-5 security level (max. 30 mm² particle area)

Any paper waste that contains personal information must be disposed of securely.

If an electronic data carrier is to be forwarded or discarded, the data contained on it must be first be deleted.

If Excel lists with personal data are used as work tools, these data must be deleted when the work is completed and the purpose is fulfilled, provided that this data is no longer required. The deletion policy must be observed.

For statistical or similar purposes, authorised individuals must anonymise personal data immediately prior to storage or processing.

5.6. OUT-OF-OFFICE NOTIFICATION WITH NAMED REPRESENTATION

To ensure timely processing of data protection inquiries, employees who are absent for more than three days must set up an e-mail absence tools and furnish the notification that this e-mail will not be forwarded and whom to contact on their behalf.
If no representative among colleagues or superiors can be identified, the address info@fhv.at can be provided in justified cases.

5.7. USERS/COPYRIGHT LIABILITIES

Whenever data, media or software of any type are used, it must be ensured that any copyrights held by third parties (e.g. photos, videos, music, text) are observed. Copyright-protected content may not be used without the consent of the author or copyright-holder.
In general, processing of data is not permitted if

- this violates existing legal provisions or threatens moral integrity,
- this violates the rights of others (e.g. data privacy, personal rights),
- this hinders, harasses (spam)or frightens others or the data contain harmful components (e.g. viruses),
- processing is used to obtain unauthorised access (e.g. password scan) or
- this is intended to impair operation (e.g. network operation).

Moreover, the applicable licence terms must be observed for all activities. Please note that free software or data are also bound to certain licence terms (e.g. GPL, BSD, MIT, CC), the consequences of which must be followed.

5.8. USE OF PRIVATE DEVICES IN CONNECTION WITH DATA AND FH VORARLBERG IT RESOURCES

The following regulations apply to the access of private IT devices to FH Vorarlberg IT resources (including services, information systems, network drives, cloud services). These apply in particular to external lecturers as well as to internal employees who use their personal IT devices (e.g. smartphones) for business purposes. The provisions also apply even if the business use of personal devices has been approved by management.

In general, only absolutely necessary business data should be stored on private (mobile) devices and storage media.

However, storage of personal, confidential or secret data on private cloud services is always prohibited.

Access to FHV systems requires compliance with the following regulations:

- Blocking the device with a sufficiently secure password or PIN; additional use of other methods is recommended (e.g. biometric features, 2FA).
- Encryption of the hard drive (in particular if sensitive data are to be stored).
- The unlocked device must not be forwarded to third parties.
- Data carriers or devices or unknown origin must not be connected to the device (viruses, Trojans, malware etc.).
- Regular updates of the operating system and protection software against viruses and such.

In general, FH Vorarlberg recommends these regulations are observed as they serve to protect personal private data, regardless of whether it is used for business purposes.

If there is suspicion of a data breach or similar circumstances relating to security of FHV data, FH Vorarlberg must be immediately informed via datenschutz@fhv.at.

If a mobile device (Notebook, Smartphone, data stick etc.) that is used for business purposes is lost or stolen, a report must immediately be made to the data protection officer at datenschutz@fhv.at. In such case, a data breach is possible. This must be reported by FH Vorarlberg to the data protection authority within 72 hours. See also Item 6.

Please note: The private use of FHV IT resources is regulated in the IT Security Guidelines for Employees in the section "Compliance Anforderungen für die private Nutzung von IT Betriebsmitteln/Compliance requirements for the private use of IT resources".
(https://inside.fhv.at/pages/viewpage.action?pageId=163717136)

5.9. OTHER REGULATIONS

5.9.1. PLAGIARISM ASSESSMENT WITH TURNITIN

The title page, dedications and acknowledgements are not be imported when using Turnitin for plagiarism assessments or must be redacted prior to uploading.

5.9.1. SOFTWARE FOR SCHEDULING

Scheduling appointments, registering for training etc. that affect individuals internal to FHV is to be done via the internal Easyevent system.
In future, it is recommended that scheduling appointments with external individuals is done using Termino or the DFN personal organizer as an alternative to Doodle:
https://www.termino.gv.at/meet/,
https://www.dfn.de/dienstleistungen/dfnterminplaner/

5.9.2. SUPERVISION OF BACHELOR'S AND MASTER'S THESES

From the perspective of data protection law, students usually assume the role of the responsible person in the preparation of academic theses. However, due to the fact that academic theses are created within the framework of teaching or research projects, there is also the possibility that FHV and the students are jointly responsible or that FHV is responsible for data protection law aspects. In case of doubt, datenschutz@fhv can be contacted.

If a Bachelor's or Master's thesis contains a data subject's personal information, the student must be advised that the rights of the data subject (obligation to provide information pursuant to Art 13f GDPR, obtaining consent if necessary) must be respected and, if applicable, a risk assessment and data protection impact assessment must be conducted; authorisation from the data protection authority may also be required. For additional important information on dealing with academic theses that contain personal data, please see
https://inside.fhv.at/pages/viewpage.action?pageId=192230106.

If there is joint responsibility or if the student is classified as the processor, it is necessary to conclude the appropriate contracts (agreement pursuant to Art. 26 or contract processing agreement).

6. REPORTABLE DATA PROTECTION INCIDENTS

6.1. NOTIFICATION IN THE EVENT OF A DATA BREACH

A data breach is defined as an incident in which an unauthorized individual obtains access to data (e.g. loss of a data carrier, hacking incident, etc.). This may result in physical, material, or immaterial harm to the data subject, including a loss of control over their personal data, a loss of confidentiality of data subject to professional secrecy, and other significant detriments.
The GDPR introduces certain reporting and notification obligations in the event of a data breach concerning personal data.
Any documents, IT systems, or data carriers that are lost or stolen must be reported **immediately**. This also applies to any private devices that have been used for business purposes.

6.2. REPORTING CHANNELS

In the event of a data protection incident, the following reporting channels must be followed:
Immediate internal report (even for suspected incidents) by telephone to the person of contact for data protection (currently the legal department: +43 5572 792 2002) or the Head of the Information Service (= Head of IS, representative of the person of contact for data protection and/or the data protection officer: +43 5572 792 2201), or by email to datenschutz@fhv.at.

7. OTHER BINDING REGULATIONS AND INFORMATION

7.1. IT SECURITY POLICY FOR EMPLOYEES OF FH VORARLBERG

This policy is binding and can be found on Inside at the following link: https://inside.fhv.at/pages/viewpage.action?pageId=163717136

7.2. SURVEYS, REPORTS, AND STATISTICS

The employees of FH Vorarlberg should be aware that various surveys that may concern them are conducted on a regular basis. The implementation of these surveys is regulated by the internal framework agreement on the automation-supported processing of employee personal data. The surveys can be accessed at the following link:
https://inside.fhv.at/display/kompakt/Befragungen%2C+Berichte+und+Statistiken

7.3. AUXILIARY DOCUMENT ON COMPLIANCE REQUIREMENTS FOR HOMEPAGES, FACEBOOK & CO

https://inside.fhv.at/pages/viewpage.action?pageId=163730730

7.4. SOCIAL MEDIA POLICY

https://inside.fhv.at/display/ds/Vorgaben+und+Informationen?preview=/163733734/169216497/Social%20Media%20Richtlinie.pdf

7.5. INSTRUCTIONS REGARDING ENCRYPTED DATA TRANSMISSION IN E-MAILS

https://inside.fhv.at/display/is/TCS+-+Persoenliche+Zertifikate

7.6. INTERNAL AGREEMENT ON THE AUTOMATION-SUPPORTED EVALUATION OF TEACHING BY STUDENTS

https://inside.fhv.at/display/br/BV+-+Evaluation+Lehre

7.7. INTERNAL AGREEMENT ON THE AUTOMATION-SUPPORTED EVALUATION OF TEACHING BY STUDENTS

https://inside.fhv.at/display/br/BV+-+Evaluation+Lehre

7.8. INTERNAL AGREEMENT ON THE AUTOMATION-SUPPORTED PROCESSING OF EMPLOYEE PERSONAL DATA

https://inside.fhv.at/pages/viewpage.action?pageId=162827196