

Datenschutzhandbuch der FH Vorarlberg

INHALT

PRÄAMBEL	3
1. Allgemeine Grundsätze	4
1.1 Ziel des Datenschutzhandbuches	4
1.2 Geltungsbereich	4
1.3 Verantwortlichkeiten	4
1.4 Definition Personenbezogene Daten	5
1.5 Definition Datenverarbeitung	5
2. Grundlagen des Datenschutzrechtes	5
2.1 Rechtmässigkeit/Transparenz	5
2.2 Zweckbindung/Datenminimierung	5
2.3 Datensparsamkeit	5
2.4 Richtigkeit/Datenaktualität	5
2.5 Speicherbegrenzung	6
2.6 Integrität und Vertraulichkeit	6
3. Datenverwendung und -verarbeitung	6
3.1 Rechtmässigkeit der Verarbeitung	6
3.2 Anweisung Datenverwendung und -verarbeitung	7
3.3 Auftragsdatenverarbeitung	7
3.4 Prüfung Verarbeitungstätigkeiten	7
3.5 Rechtskonforme Einwilligungserklärung	7
4. Rechte von Betroffenen	8
4.1 Auskunftsrechte	8
4.2 Informationsrechte	8
4.3 Berichtigungsrecht	8
4.4 Lösungsrecht	8
4.5 Widerspruchsrecht:	9
4.5 Abwicklung von Datenschutzanfragen	9
5. Erforderliche Massnahmen	9

5.1.	Zutritts- und Zugriffsschutz.....	9
5.2.	Protokollierung von Verwendungsvorgängen.....	9
5.3.	Messenger-Dienste	9
5.4.	E-Mail-Kommunikation und Datenübertragung.....	9
5.5.	Datenklassifizierung	10
5.5.1.	Zur Notwendigkeit des Schutzes von personenbezogenen oder vertraulichen Daten..	10
5.5.2.	Zur Anwendung des Datenklassifikationsschemas der FH Vorarlberg	11
5.5.3.	Datenklassifikationsschema	12
5.6.	Sicheres Entsorgen von Daten – Löschkonzepte	13
5.6.	Abwesenheitsnotiz mit Vertretung	14
5.7.	Haftung Nutzer/Urheberrecht.....	14
5.8.	Verwendung von privaten Geräten im Zusammenhang mit Daten und IT-Betriebsmitteln der FH Vorarlberg.....	14
5.9.	Weitere Regelungen	15
5.9.1.	Plagiatsprüfung mit Turnitin.....	15
5.9.2.	Software zur Terminfindung.....	16
5.9.3.	Betreuung von Bachelor- und masterarbeiten.....	16
6.	Meldepflichtige Datenschutzvorfälle.....	16
6.1.	Meldung von Datenschutzverletzungen („DATA BREACH“)......	16
6.2.	Meldewege	17
7.	Weiterführende verbindliche Regelungen und Informationen	17
7.1.	IT-Sicherheitsrichtlinien für MitarbeiterInnen der FH Vorarlberg.....	17
7.2.	Befragungen, Berichte und Statistiken.....	17
7.3.	Arbeitsbehelf zu Compliance Anforderungen an Homepages, Facebook & Co	17
7.4.	Richtlinie Social Media	17
7.6.	Anleitung zur verschlüsselten Datenübermittlung in E-Mails	17
7.7.	Betriebsvereinbarung „Automationsunterstützte Evaluation Lehre durch die Studierenden“	17
7.8.	Betriebsvereinbarung Automationsunterstützte Verarbeitung personenbezogener Daten der Mitarbeiterinnen und Mitarbeiter	18

PRÄAMBEL

Die FH Vorarlberg steht für höchste Standards in Lehre und Forschung. Als öffentlich finanziertes Unternehmen unterliegen wir auch den gesetzlichen Grundsätzen der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit auf der Grundlage der Ordnungsmäßigkeit und Rechtmäßigkeit. Diesen Ansprüchen genügen wir ebenso bei der Einhaltung der geltenden Verordnungen, Richtlinien und Gesetze hinsichtlich des Datenschutzes.

In diesem Handbuch haben wir Voraussetzungen für die Verarbeitung personenbezogener Daten von StudentInnen, InteressentInnen, Partnern und MitarbeiterInnen geregelt. Dadurch setzen wir den Datenschutz- und Datensicherheitsstandard in unserer Organisation.

Unsere MitarbeiterInnen sind verpflichtet, diese Richtlinie zum Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze und -verordnungen zu beachten.

Dieses Handbuch ist kein statisches Dokument, sondern wird laufend weiterentwickelt und an veränderte gesetzliche Vorgaben oder technische Veränderungen angepasst.

1. ALLGEMEINE GRUNDSÄTZE

1.1 ZIEL DES DATENSCHUTZHANDBUCHES

Die Fachhochschule ist an die Einhaltung der gesetzlichen Datenschutzregelungen gebunden. Die nachfolgenden Regelungen sind Richtlinien, die den Datenschutz an der Fachhochschule gewährleisten.

Die Einhaltung der Datenschutzbestimmungen wird an der FH Vorarlberg sichergestellt, indem die mit der Verarbeitung von Daten betrauten Personen entsprechend aufgeklärt bzw. geschult werden und die Einhaltung der Bestimmungen durch die bzw. den Datenschutzbeauftragten (DSB) kontrolliert wird. Mit Hilfe dieses Handbuches soll die Bedeutung des Datenschutzes an der FH Vorarlberg betont werden.

1.2 GELTUNGSBEREICH

Das vorliegende Datenschutzhandbuch definiert die Vorgaben zur Einhaltung der rechtlichen Datenschutzbestimmungen. Es gilt für alle Prozesse und stellt für alle MitarbeiterInnen (ProjektmitarbeiterInnen, nebenberuflich Lehrende, etc.) der FH Vorarlberg eine verbindliche Arbeitsgrundlage dar. Es erstreckt sich auf alle aktuellen und künftigen Geschäftsstandorte, Abteilungen und Unternehmensbereiche der FH Vorarlberg.

1.3 VERANTWORTLICHKEITEN

Die Führungskräfte der FH Vorarlberg sind verantwortlich für die Datenverarbeitung in ihrem jeweiligen Verantwortungsbereich. Damit sind sie verpflichtet, sicherzustellen, dass die gesetzlichen und die im Datenschutzhandbuch enthaltenen Anforderungen des Datenschutzes berücksichtigt werden.

Alle Datenverarbeitenden an der FH Vorarlberg sind verpflichtet, die im vorliegenden DS- Handbuch definierten Bestimmungen einzuhalten und die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten der FH Vorarlberg bei jedem Vorfall durch den die Sicherheit der verarbeiteten Daten gefährdet ist (auch bei Verdacht), unverzüglich zu kontaktieren. Dies ist insofern wichtig, als dass der Missbrauch, aber auch der Verlust von Daten für die FH Vorarlberg nach geltendem Recht teilweise schwerwiegende Konsequenzen nach sich ziehen kann.

Die/der Datenschutzbeauftragte ist verpflichtet, die Geschäftsführung und die MitarbeiterInnen hinsichtlich ihrer Pflichten nach dem Datenschutzrecht zu unterrichten und zu beraten, die MitarbeiterInnen hinsichtlich der Einhaltung der Datenschutzbestimmungen zu sensibilisieren und zu schulen, die Einhaltung der Datenschutzvorschriften zu überwachen und zu überprüfen, sowie im Zusammenhang mit Datenschutz-Folgenabschätzungen zu beraten. Darüber hinaus arbeitet sie/er mit der Aufsichtsbehörde zusammen und ist Anlaufstelle für diese.

Der Abteilung Information Services hat die Aufgabe, geeignete technische und organisatorische Maßnahmen zu treffen, die die Einhaltung der sich aus der DSGVO ergebenden Verpflichtungen gewährleisten. Insbesondere soll die Einhaltung der Grundsätze des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) berücksichtigt werden. Bei der Einführung neuer Systeme ist die/der Datenschutzbeauftragte zu informieren und beratend hinzuzuziehen.

1.4. DEFINITION PERSONENBEZOGENE DATEN

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der Person sind.

1.5. DEFINITION DATENVERARBEITUNG

Datenverarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

2. GRUNDLAGEN DES DATENSCHUTZRECHTES

2.1. RECHTMÄSSIGKEIT/TRANSPARENZ

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte der betroffenen Personen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und nachvollziehbar erhoben und verarbeitet werden. Die Informationen zur Verarbeitung von personenbezogenen Daten sollten in präziser, leicht zugänglicher und verständlicher Form bereitgestellt werden.

2.2. ZWECKBINDUNG/DATENMINIMIERUNG

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden. Die Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Sie müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

2.3. DATENSPARSAMKEIT

Die Datenverarbeitung muss auf das zweckgebundene, notwendige Maß beschränkt werden. Es dürfen folglich keine Daten verarbeitet werden, die zur Erfüllung des angegebenen Verwendungszwecks nicht erforderlich sind. Daten sollten nach Möglichkeit anonymisiert oder pseudonymisiert werden.

2.4. RICHTIGKEIT/DATENAKTUALITÄT

Personenbezogene Daten sind sachlich richtig und soweit erforderlich auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, damit unrichtige Daten gelöscht oder berichtigt werden.

2.5. SPEICHERBEGRENZUNG

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher sollte der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen. Dabei ist das allgemeine Löschkonzept der FH Vorarlberg zu beachten.

2.6. INTEGRITÄT UND VERTRAULICHKEIT

Personenbezogene Daten müssen vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung, Weitergabe, Verlust oder Beschädigung gesichert werden. Zur Sicherstellung der Einhaltung des Grundsatzes der Vertraulichkeit werden alle MitarbeiterInnen der FH Vorarlberg zur Geheimhaltung von personenbezogenen Daten, welche ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, verpflichtet. Diese Geheimhaltungsverpflichtung bleibt auch nach Beendigung des Arbeitsverhältnisses aufrecht. Darüber hinaus sind auch etwaige GeschäftspartnerInnen zur Einhaltung der Vertraulichkeit zu verpflichten.

3. DATENVERWENDUNG UND -VERARBEITUNG

3.1. RECHTMÄSSIGKEIT DER VERARBEITUNG

Personenbezogene Daten müssen auf **rechtmäßige** Weise und nachvollziehbar erhoben und verarbeitet werden. Verarbeitungen unterliegen außerdem der **Zweckbindung** und dürfen daher nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden.

Weiters sollen Daten immer sachlich **richtig und aktuell** gespeichert werden und die **Speicherfrist** auf das unbedingt erforderliche Mindestmaß beschränkt werden (Löschfristen).

Datenverarbeitungen sind im Wesentlichen rechtmäßig, wenn eine der nachstehenden Bedingungen erfüllt ist (vgl. Art. 6 EU-DSGVO)

- Einwilligung (Betroffene/r gibt ihre/seine Einwilligung zur Verarbeitung für einen oder mehrere bestimmte Zwecke, z.B. Fotos/ Videos aufnehmen)
- Vertragserfüllung oder für vorvertragliche Maßnahmen (z.B. Ausbildungsvertrag der Studierenden)
- Erfüllung einer rechtlichen Verpflichtung der die FH Vorarlberg unterliegt (z.B. verpflichtende Meldungen an das Ministerium, Statistik Austria etc.)
- Zur Wahrnehmung öffentlicher Interessen oder
- Zur Wahrung der berechtigten Interessen der FH-Vorarlberg, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen

3.2. ANWEISUNG DATENVERWENDUNG UND -VERARBEITUNG

Personenbezogene Daten dürfen nur auf Anweisung von dazu berechtigten Personen verwendet und verarbeitet werden. Die transparente Aufgabenverteilung erfolgt durch LeiterInnen der Organisationseinheiten. Die Auftragserteilung kann mündlich, schriftlich oder konkludent erfolgen oder bereits erfolgt sein.

3.3. AUFTRAGSDATENVERARBEITUNG

Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. Dies können unter anderem auch externe IT-Dienstleister sein, Digibon, Hosting-Unternehmen, aber auch beauftragte Fotografen. In diesen Fällen ist mit externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschließen.

Bei der Erstellung dementsprechender Vereinbarungen ist die Rechtsabteilung der FH Vorarlberg unterstützend tätig (Edna Fitz, edna.fitz@fhv.at), die bei Bedarf zu kontaktieren ist. Die abgeschlossenen Vereinbarungen sind eingescannt an die für Datenschutz zuständige Person (Edna Fitz, edna.fitz@fhv.at) zu übermitteln.

Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

3.4. PRÜFUNG VERARBEITUNGSTÄTIGKEITEN

Die Führungskräfte der FH Vorarlberg sind verantwortlich für das Verzeichnis der Verarbeitungstätigkeiten in ihrem jeweiligen Verantwortungsbereich. Dieses ist in regelmäßigen Abständen zu überprüfen und im Falle von Änderungen entsprechend anzupassen, sodass die Aktualität gewahrt wird.

Bei der Einführung neuer Geschäftsprozesse und neuer Forschungsaufträge müssen alle Verarbeitungstätigkeiten identifiziert und zentrale Fragestellungen (Verantwortlicher, Datenarten, Datenherkunft, Datenübermittlung usw.) beantwortet werden. Die Ergebnisse müssen an den Datenschutzbeauftragten gemeldet werden, um diese ins Verzeichnissesverzeichnis zu überführen.

Das Vorgehen hinsichtlich der Aktualisierung bestehender und Meldung neuer Verarbeitungstätigkeiten regelt die FHV-interne Verfahrensanweisung „OA-024 Verarbeitungs-tätigkeiten personenbezogener Daten melden und pflegen“.

Diese Verfahrensanweisung stellt eine verbindliche Vorgabe für alle MitarbeiterInnen der FHV dar. (<https://inside.fhv.at/pages/viewpage.action?pageId=163732368>)

3.5. RECHTSKONFORME EINWILLIGUNGSERKLÄRUNG

Einwilligungserklärungen sind erforderlich, wenn die erhobenen Daten nicht zur Vertragserfüllung erforderlich sind oder die von der FH Vorarlberg vorgesehene Verarbeitungstätigkeit weder aufgrund einer gesetzlichen Bestimmung verpflichtend erfolgen muss, noch aufgrund eines Vertrags durchgeführt wird und auch nicht im überwiegenden berechtigten Interesse der FH Vorarlberg ist.

Einwilligungserklärungen sind nur dann gültig, wenn die betroffenen Personen auf ihr Widerrufsrecht hingewiesen werden und sie darüber informiert werden, wer die

für die Verarbeitung der personenbezogenen Daten Verantwortliche ist und für welche Zwecke die Daten verarbeitet werden.

Die Einwilligung muss informiert, freiwillig und eindeutig erfolgen. Zu Beweis Zwecken ist es empfehlenswert, schriftliche Einwilligungen einzuholen (Muster).

Bisher erhaltene Einwilligungen gelten weiter, sofern sie den Anforderungen der DSGVO entsprechen. Es ist zu prüfen, ob der Zweck der Datenverarbeitung angegeben und ob eine Widerrufsrechtsbelehrung enthalten war und ob die Einwilligung nachweisbar ist. Andernfalls müssen Einwilligungen neu eingeholt werden.

4. RECHTE VON BETROFFENEN

4.1. AUSKUNFTSRECHTE

Betroffene haben das Recht zu erfahren, ob und welche Daten die FH Vorarlberg zu ihrer Person verarbeitet. Den Kontakt zur anfragenden Person hält grundsätzlich ausschließlich der/die definierte Datenschutzverantwortliche bzw. deren Vertretung.

Jede/r Mitarbeitende ist verpflichtet, bei Anfragen mit datenschutzrechtlicher Relevanz die anfragende Person darauf hinzuweisen, dass derartige Anfragen ausschließlich an datenschutz@fhv.at zu richten sind. Ungeachtet dessen muss die für derartige Anfragen zuständige Person (derzeit Stabstelle Recht) unverzüglich von diesen Anfragen unterrichtet werden.

4.2. INFORMATIONSRECHTE

Werden Daten eines Betroffenen erhoben, so ist er im Zeitpunkt der Datenerhebung von der Speicherung und über den Zweck der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Darüber hinaus sind ihr/ihm allfällige Übermittlungsempfänger samt dem Übermittlungszweck mitzuteilen, genauso wie die Kontaktdaten der FH Vorarlberg (sofern ihm diese noch nicht bekannt sind) und die Kontaktdaten der Datenschutz-Ansprechperson (datenschutz@fhv.at).

4.3. BERICHTIGUNGSRECHT

Betroffene Personen haben das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten oder die Vervollständigung unvollständiger Daten zu verlangen.

4.4. LÖSCHUNGSRECHT

Betroffene Personen haben das Recht, die Löschung von sie betreffenden personenbezogenen Daten zu verlangen. Die FH Vorarlberg prüft derartige Ansuchen mit den betroffenen Abteilungen genau. Es können nur jene Daten gelöscht werden, hinsichtlich derer die FH Vorarlberg kein berechtigtes Interesse an deren weiterer Speicherung hat.

4.5. WIDERSPRUCHSRECHT:

Betroffene Personen haben das Recht, jederzeit gegen Verarbeitungstätigkeiten sie betreffender personenbezogener Daten, welche auf der Rechtsgrundlage des überwiegenden berechtigten Interesses der FHV erfolgen, Widerspruch einzulegen.

4.5. ABWICKLUNG VON DATENSCHUTZANFRAGEN

Die standardisierte, fristgerechte Abwicklung von Auskunfts-, Berichtigungs- und Lösungsbegehren regelt die FHV-interne Verfahrensanweisung „VA-057 Datenschutzanfragen abwickeln“ (<https://inside.fhv.at/display/kompakt/VA-057+Datenschutzanfragen+abwickeln>). Diese Verfahrensanweisung stellt eine verbindliche Vorgabe für alle MitarbeiterInnen der FHV dar.

5. ERFORDERLICHE MASSNAHMEN

5.1. ZUTRITTS- UND ZUGRIFFSCHUTZ

Sobald ein Arbeitsplatz für längere Zeit nicht besetzt ist, müssen alle sensiblen und vertraulichen Dokumente vom Schreibtisch verstaut (auch Speichermedien wie z. B. USB-Sticks) und Computerarbeitsplätze gesperrt (PC mit Tastenkombination "Windows-Taste + L") werden.

Die Türen nicht besetzter Büroräume sind abzuschließen. Dadurch wird verhindert, dass Unbefugte auf darin befindliche Unterlagen und IT-Einrichtungen zugreifen können. Sofern Arbeiten im Home-Office durchgeführt werden ist, ebenfalls darauf zu achten, dass FH Vorarlberg betreffende Dokumente vor dem Zugriff Unbefugter geschützt sind.

5.2. PROTOKOLLIERUNG VON VERWENDUNGSVORGÄNGEN

Nach Möglichkeit ist Protokoll zu führen, damit durchgeführte Verwendungsvorgänge, wie Änderungen, Abfragen und Übermittlungen im Hinblick auf ihre Zulässigkeit nachvollzogen werden können.

5.3. MESSENGER-DIENSTE

Bei der Nutzung von Messenger-Diensten wie z. B. WhatsApp findet die Verarbeitung von personenbezogenen Daten statt. Aus datenschutzrechtlicher Sicht ist der Einsatz von WhatsApp zur dienstlichen Kommunikation oder der Kommunikation mit Studierenden daher nicht zulässig.

Dies gilt auch für andere Messenger-Dienste, bei denen die Übertragung von Kontaktdaten aus dem Adressbuch der Nutzer an den Dienstanbieter stattfindet oder andere datenschutzrechtliche Vorgaben missachtet werden.

Für die dienstliche Kommunikation sind die vorhandenen internen Kommunikationswege zu nutzen.

5.4. E-MAIL-KOMMUNIKATION UND DATENÜBERTRAGUNG

a) Bei E-Mails zwischen internen E-Mail EmpfängerInnen (fhv.at, students.fhv.at und schlosshofen.at) sind keine besonderen Vorkehrungen erforderlich, da wir

innerhalb der FH besondere Vorkehrungen für den Schutz solcher Daten vorgesehen haben.

b) Eine Übermittlung von E-Mails an externe EmpfängerInnen, in denen bereits im Text personenbezogene Daten enthalten sind, ist nur zulässig, wenn die Nachrichten selber verschlüsselt sind.

Bitte beachten Sie, dass auch die EmpfängerInnen die technischen Voraussetzungen für eine E-Mail Verschlüsselung verwenden und korrekt anwenden müssen. Voraussetzung ist auch eine korrekte digitale Signatur im Vorfeld auszutauschen (durch den Versand signierter E-Mails zwischen den Partnern).

Die FH Vorarlberg stellt jedem/jeder Benutzer/in grundsätzlich ein persönliches Zertifikat zur Verfügung. Nähere Informationen dazu sind zu finden unter <https://inside.fhv.at/display/is/TCS+-+Persoenliche+Zertifikate> (Anmerkung: Alternativ kann auch PGP verwendet werden).

c) Eine Übermittlung von E-Mails an externe EmpfängerInnen, in denen lediglich in den Anhängen personenbezogene Daten enthalten sind, ist auch zulässig, jedoch nur wenn die Anhänge verschlüsselt sind. Nähere Informationen dazu sind zu finden unter <https://inside.fhv.at/display/is/TCS+-+Persoenliche+Zertifikate>.

Bitte beachten Sie, dass der Austausch personenbezogener Daten mit Dritten nur im Rahmen von entsprechenden vertraglichen Vereinbarungen zulässig ist (z.B. Auftragsverarbeitungsvereinbarung, Vereinbarung gem. Art. 26 DSGVO, Geheimhaltungsvereinbarung). Übermittlungen von Inhalten mit besonderen Kategorien von personenbezogenen Daten, sowie von vertraulichen und geheimen Informationen (Betriebs- und Geschäftsgeheimnisse, Datenklassifikation C und D) sollten nicht per E-Mail, sondern mittels eines anderen technischen Systems erfolgen. Im Zuge der Organisation eines solchen Datenaustauschs empfiehlt die FH Vorarlberg dringend entsprechende Teams auf Dropbox FHV einzurichten und gänzlich auf die Übermittlung via Email zu verzichten. Weitere Informationen erhalten Sie unter <https://inside.fhv.at/display/is/Dropbox+FHV>.

5.5. DATENKLASSIFIZIERUNG

5.5.1. ZUR NOTWENDIGKEIT DES SCHUTZES VON PERSONENBEZOGENEN ODER VERTRAULICHEN DATEN

Die Notwendigkeit einer Klassifizierung von personenbezogenen Daten ergibt sich schon aufgrund der EU-DSGVO. Aus dieser ist die Unterteilung in „nicht-personenbezogene Daten“, „personenbezogene Daten“ und „besondere Kategorien personenbezogener Daten (bisher im DSG 2000 sensible Daten) abzuleiten.

Deshalb gilt, personenbezogene Daten, unabhängig davon, ob es solche von Studierenden, MitarbeiterInnen, an Veranstaltung teilnehmenden Personen, Kontaktpersonen, juristischen Personen oder sonstigen Personen sind, zu denen die MitarbeiterInnen der FH Vorarlberg Kontakt haben, im Hinblick auf die allgemeinen Datenschutzbestimmungen mit der jeweils erforderlichen Vertraulichkeit und

Integrität zu behandeln. Dabei sind die Gebote der Datensparsamkeit, Transparenz, Richtigkeit und Speicherbegrenzung einzuhalten.

Hilfreich dafür ist ein Schutzstufenkonzept für die personenbezogenen Daten.

Neben den Unterlagen mit personenbezogenen Daten unterliegen auch andere interne Unterlagen mit internen vertraulichen Informationen (Betriebs- und Geschäftsgeheimnisse) entsprechenden Geheimhaltungspflichten und ist auch hierfür das Schutzstufenkonzept heranzuziehen.

5.5.2. ZUR ANWENDUNG DES DATENKLASSIFIKATIONSSCHEMAS DER FH VORARLBERG

Umgang mit Altdaten

Die Datenklassifikation der FH Vorarlberg tritt mit Herbst 2019 in Kraft. Daten, die vor diesem Datum erstellt oder verändert wurden gelten als "B: intern/internal" klassifiziert, es sei denn diese fallen sinngemäß unter die Datenklassifikationen "C: vertraulich/ confidential" oder "D: geheim/secret" oder sind bereits öffentlich zugänglich.

Umgang mit öffentlichen Daten (Datenklassifikation A: öffentlich/public)

Öffentliche Daten müssen nicht gesondert klassifiziert werden.

Zu den öffentlichen Daten zählen neben klassischen ohne besondere Berechtigungen zugänglichen Informationen (z.B. in Printmedien oder auf web homepages) auch Veröffentlichungen in sozialen Medien.

Zu beachten ist, dass auch alle Informationen, die an alle oder an eine große Gruppe von Studierenden übermittelt werden, im Sinne der vorliegenden Datenklassifikation als öffentlich gelten.

Umgang mit eingeschränkten Daten (Datenklassifikation B: intern/internal)

Eingeschränkte Daten müssen nicht gesondert klassifiziert werden.

Unklassifizierte Dokumente gelten per Definition als "B: intern/internal" klassifiziert wenn sie nur MitarbeiterInnen oder aber einer bestimmten Gruppen von MitarbeiterInnen zugänglich sind. Diese Regelung hat den Zweck die Handhabung der Datenklassifikation zu vereinfachen.

Grundsätzlich hat der/die Autorin durch die Wahl des Veröffentlichungsortes oder durch explizite Berechtigungseinstellungen festzulegen, dass Daten nur den berechtigten und notwendigen Personen zugänglich sind.

Umgang mit vertraulichen oder geheimen Daten (Datenklassifikation C: vertraulich/confidential bzw. Datenklassifikation D: geheim/secret)

Dokumente vertraulicher oder geheimer Art müssen vom/von der Autor/in als "C: vertraulich/confidential" oder "D: geheim/secret" explizit klassifiziert werden und dürfen nur den unmittelbar notwendigen und berechtigten Personen zugänglich gemacht werden.

Dabei hat die Klassifizierung durch den/die Autor/in so zu erfolgen, dass die/der Empfänger/in diese umgehend erkennt, z.B. am Anfang des Dokuments oder im Subject einer E-Mail.

Für die konkrete technische Realisierung ist aufgrund des zügig voranschreitenden technologischen Fortschritts die Dokumentation unter <https://inside.fhv.at/pages/viewpage.action?pageId=190291547> verbindlich einzuhalten.

Die Pflichten im Zusammenhang mit der Rolle der/des Verantwortlichen sind nicht delegierbar. Es kann aber eine Stellvertretung nominiert werden.

5.5.3. DATENKLASSIFIKATIONSSCHEMA

Datenklassifikation	Definition	Anwendung und Beispiele
Datenklassifikation A: öffentlich/public	Daten, die keinen besonderen Beschränkungen unterliegen oder bereits veröffentlicht wurden. Daten gelten dann als öffentlich im Sinne dieser Datenklassifikation, wenn sie allen internen BenutzerInnen (Mitarbeitende und Studierende) oder dem Großteil davon zugänglich gemacht werden. Daten im Intranet gelten aufgrund des grossen Empfängerkreises ebenfalls als öffentlich, wenn der Nutzerkreis nicht explizit durch den Autor auf eine spezifische Gruppe eingeschränkt wurde.	Daten im Internet, Daten im Firmenbuch, FH weit verfügbare Daten
Datenklassifikation B: intern/internal	Daten, hinsichtlich derer innerhalb einer Organisationseinheit keine Beschränkungen erforderlich sind, außerhalb der Organisationseinheit jedoch Beschränkungen hinsichtlich Zugriffsrechten, Verarbeitung und Weitergabe benötigt werden.	z.B. unternehmensinterne Kommunikation und sonstige Unterlagen ohne hohe Vertraulichkeit.
Datenklassifikation C: vertraulich/confidential	Daten, die nur einem bestimmten Personenkreis zur Verfügung stehen und deren unsachgemäße Handhabung oder Verbreitung die betroffenen Personen oder die FH Vorarlberg in ihrer gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen“)	Die Daten stehen nur einem bestimmten Personenkreis zur Verfügung, hinsichtlich der Zugriffs-, Verarbeitungs- und Weitergaberechte unterliegen die Daten entsprechenden Beschränkungen. z.B. Einkommensdaten, Daten zu Sozialleistungen
Datenklassifikation D: geheim/secret	Daten, die nur einem sehr eingeschränkten bestimmten	Nur ein sehr eingeschränkter Personenkreis hat Zugriffs-,

	<p>Personenkreis zur Verfügung stehen und deren unsachgemäße Handhabung oder Verbreitung die betroffenen Personen oder die FH Vorarlberg in ihrer gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen sehr beeinträchtigen könnten. („Existenz“). Die Daten unterliegen einem rechtlichen Geheimhaltungsschutz.</p>	<p>Verarbeitungs- und Weitergaberechte.z.B. Dienstliche Beurteilungen, Gesundheitsdaten, Schulden/Exekutionen, Forschungsergebnisse, für die Geheimhaltungsvereinbarungen gelten</p>
--	--	--

5.6. SICHERES ENTSORGEN VON DATEN – LÖSCHKONZEPTE

Für alle Verarbeitungstätigkeiten sind Löschkonzepte für die Löschung der personenbezogenen Daten und Entsorgung der Papierunterlagen erforderlich.

Die Löschungen und Entsorgung der Papierunterlagen müssen entsprechend der Löschkonzepte erfolgen.

Für die Entsorgung von Papierunterlagen stehen verschiedene Möglichkeiten zur Verfügung, diese erfolgt entsprechend den darin enthaltenen Informationen:

Art der Unterlagen	Datenklassifikation	Sicherheitsstufe	Entsorgungsart / Sicherheitsstufe nach ÖNORM
Daten, die keinen besonderen Beschränkungen unterliegen <u>und</u> bereits veröffentlicht wurden <u>und keine personenbezogene</u> Daten enthalten.	Teils Datenklassifikation A: öffentlich/ public z.B. Prospekte, Werbematerial, Zeitungen, Veranstaltungseinladungen ohne Personalisierung	P-1	Kartonschachtel
Daten, die keinen besonderen Beschränkungen unterliegen <u>und</u> bereits veröffentlicht wurden <u>und personenbezogene Daten</u> enthalten.	Datenklassifikation A: öffentlich/ public z.B. personalisierte Werbung	P-1 bis P-3	Aktenvernichtungsbox
Daten, hinsichtlich derer innerhalb einer Organisationseinheit keine Beschränkungen erforderlich sind, außerhalb der Organisationseinheit jedoch Beschränkungen hinsichtlich Zugriffsrechten, Verarbeitung und Weitergabe benötigt werden.	Datenklassifikation B: Intern/internal z.B. unternehmensinterne Kommunikation und sonstige Unterlagen ohne hohe Vertraulichkeit	P-2 bis P-5	Aktenvernichtungsbox oder Aktenvernichter mit Sicherheitsstufe P-2 (Streifenbreite max. 6 mm)
Daten, die nur einem bestimmten Personenkreis zur Verfügung stehen und deren unsachgemäße Handhabung oder Verbreitung die betroffenen Personen oder die FH Vorarlberg in ihrer gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen beeinträchtigen könnte (Ansehen).	Datenklassifikation C: Vertraulich/confidential z.B. Einkommensdaten, Daten zu Sozialleistungen, Anfragen Angebote, Personaldaten und -akten, Studierendendaten, außer sie fallen unter die Datenklassifikation D	P-4 bis P-5	Aktenvernichtungsbox oder Aktenvernichter mit Sicherheitsstufe P-4 (max. 160 mm ² Partikelfläche)
Daten, die nur einem sehr eingeschränkten Personenkreis zur Verfügung stehen und deren unsachgemäße Handhabung oder Verbreitung die betroffenen Personen oder die FH Vorarlberg in ihrer gesellschaftlichen Stellung oder wirtschaftl. Verhältnissen sehr beeinträchtigen könnte (Existenz).	Datenklassifikation D: Geheim/secret z.B. Dienstliche Beurteilungen, Gesundheitsdaten, Schulden/Exekutionen, Forschungsergebnisse und Daten, hinsichtlich derer Geheimhaltungsvereinbarungen abgeschlossen wurden, geheime F & E Daten, Finanzdaten, Unterlagen der Geschäftsleitung	P-5	Aktenvernichter mit Sicherheitsstufe P-5 (max. 30 mm ² Partikelfläche)

Jeglicher Papiermüll, der personenbezogene Informationen enthält, muss sicher entsorgt werden.

Sollen elektronische Datenträger weitergegeben oder entsorgt werden, müssen die darauf enthaltenen Daten, vor der Weitergabe oder Entsorgung des Speichermediums gelöscht werden.

Werden als Arbeitsbehelf Excellisten mit personenbezogenen Daten verwendet, so sind diese Daten zu löschen, wenn die Arbeit beendet und der Zweck erfüllt ist, sofern diese Daten nicht mehr gebraucht werden. Dabei ist das Löschkonzept zu beachten.

Für statistische oder vergleichbare Zwecke müssen Berechtigte personenbezogene Daten unmittelbar **vor der weiteren Speicherung oder Verarbeitung** anonymisieren.

5.6. ABWESENHEITSNOTIZ MIT VERTRETUNG

Um die fristgerechte Abwicklung von Datenschutzanfragen gewährleisten zu können, sind bei einer Abwesenheit von mehr als drei Tagen von den Mitarbeitenden Mail-Abwesenheitsassistenten einzurichten und mit der Information auszustatten, dass diese E-Mail nicht weitergeleitet wird sowie wer in Vertretung angeschrieben werden kann.

Ist keine Vertretung durch (Fach)KollegInnen oder Vorgesetzte möglich, kann in begründeten Fällen info@fhv.at angegeben werden.

5.7. HAFTUNG NUTZER/URHEBERRECHT

Bei der Nutzung verschiedener Daten, Medien oder Software ist darauf zu achten, dass Urheberrechte Dritter (z. B. Fotos, Videos, Musik, Texte) nicht verletzt werden. Ohne Zustimmung des Urhebers bzw. des Rechteinhabers dürfen solche Inhalte nicht genutzt werden.

Generell ist die Verarbeitung von Daten unzulässig

- wenn diese gegen bestehende Rechtsvorschriften verstößt oder die Sittlichkeit gefährdet,
- wenn dadurch die Rechte anderer verletzt werden (z.B. Datenschutz, Persönlichkeitsrechte),
- wenn dadurch andere behindert, belästigt (Spam), verängstigt oder die Daten schädliche Komponenten enthalten (z.B. Viren),
- wenn die Verarbeitung zur Erlangung eines unautorisierten Zugriffs dienen (z.B. Passwort-Scan) und
- wenn dadurch eine Beeinträchtigung des Betriebs (z.B. des Netzbetriebs) beabsichtigt ist.

Darüber hinaus sind bei allen Tätigkeiten die jeweils geltenden Lizenzbestimmungen einzuhalten. Dabei ist zu berücksichtigen, dass auch freie Software oder Daten an bestimmte Lizenzbestimmungen gebunden sind (z.B. GPL, BSD, MIT, CC), welchen Folge zu leisten ist.

5.8. VERWENDUNG VON PRIVATEN GERÄTEN IM ZUSAMMENHANG MIT DATEN UND IT-BETRIEBSMITTELN DER FH VORARLBERG

Für den Zugriff von privaten IT Geräten auf IT Betriebsmittel (u.a. Server, Informationssysteme, Netzwerklaufwerke, Cloud Dienste) der FH Vorarlberg gelten

die folgenden Regelungen. Diese gelten insbesondere für externe Lehrende, aber auch für interne MitarbeiterInnen, die ihre privaten IT-Geräte (z.B. Smartphones) für dienstliche Zwecke nutzen. Die Vorgaben gelten auch, wenn die dienstliche Nutzung von Privatgeräten von der Geschäftsführung genehmigt wurde.

Generell sollen auf privaten (Mobil-)Geräten und Speichermedien nur die unbedingt erforderlichen dienstlichen Daten gespeichert werden.

Eine Speicherung von personenbezogenen, vertraulichen oder geheimen Daten in privaten Cloud Diensten ist aber in jedem Fall untersagt.

Ein Zugang zu FH Systemen erfordert die verbindliche Einhaltung der folgenden Regelungen.

- Sperrung des Gerätes durch ein ausreichend sicheres Kennwort oder PIN, der zusätzliche Einsatz weiterer Methoden (z.B. biometrische Merkmale, 2FA) wird empfohlen
- Verschlüsselung der Festplatte (Dies gilt insbesondere, wenn sensible Daten gespeichert sein sollten.)
- keine Weitergabe des entsperrten Geräts an Dritte
- Datenträger oder Geräte, die unbekannter Herkunft sind, dürfen nicht an das Gerät angeschlossen werden (Viren, Trojaner, Malware etc.).
- regelmäßige Aktualisierung des Betriebssystems und einer Schutz-Software gegen Viren u.ä.

Die FH Vorarlberg empfiehlt diese Regeln generell zu beachten, da diese dem Schutz der persönlichen privaten Daten dienen, und zwar unabhängig von einer dienstlichen Nutzung.

Sollte hinsichtlich von FH Daten ein Verdacht auf eine Datenpanne oder ähnliche sicherheitsgefährdende Umstände bestehen, ist die FH Vorarlberg unverzüglich über datenschutz@fhv.at zu informieren.

Wenn ein mobiles Gerät (Notebook, Smartphone, Datenstick etc.), das dienstlich genutzt wird, verloren gehen oder gestohlen werden sollte, so ist unverzüglich eine Meldung an den Datenschutzbeauftragten datenschutz@fhv.at zu erteilen. In diesem Fall könnte nämlich eine Datenpanne (Data Breach) vorliegen. Eine solche ist von der FH Vorarlberg innerhalb von 72 Stunden an die Datenschutzbehörde zu melden. Siehe auch Punkt 6.

Bitte beachten Sie: Die private Nutzung von FH IT Betriebsmitteln ist in den IT Sicherheitsrichtlinien für MitarbeiterInnen im Kapitel „Compliance Anforderungen für die private Nutzung von IT Betriebsmitteln / Compliance requirements for the private use of IT resources“ geregelt (<https://inside.fhv.at/pages/viewpage.action?pageId=163717136>)

5.9. WEITERE REGELUNGEN

5.9.1. PLAGIATSPRÜFUNG MIT TURNITIN

Titelblatt, Widmungen und Danksagungen sind bei der Verwendung von Turnitin zur Plagiatsprüfung nicht einzuspielen bzw. vor dem Upload zu schwärzen.

5.9.2. SOFTWARE ZUR TERMINFINDUNG

Für Terminsuchen, Schulungsanmeldungen, etc. die FHV-interne Personen betreffen, ist das interne System Easyevent im inside zu verwenden.

Für Terminsuchen mit externen Personen wird empfohlen statt Doodle zukünftig Termino oder den DFN Terminplaner zu verwenden:

<https://www.termino.gv.at/meet/>,

<https://www.dfn.de/dienstleistungen/dfnterminplaner/>

5.9.3. BETREUUNG VON BACHELOR- UND MASTERARBEITEN

Bei der Erstellung wissenschaftlicher Abschlussarbeiten haben Studierende aus datenschutzrechtlicher Sicht meist die Rolle des Verantwortlichen. Aufgrund der Erstellung der wissenschaftlichen Arbeit im Rahmen von Lehrforschungsprojekten oder Forschungsprojekten besteht jedoch auch die Möglichkeit, dass eine gemeinsame Verantwortung der FH und der Studierenden vorliegt oder dass die FH die datenschutzrechtliche Verantwortung trifft. Im Zweifel kann datenschutz@fhv hinzugezogen werden.

Sofern Bachelor- oder Masterarbeiten personenbezogene Daten von betroffenen Personen beinhalten, sind die Studierenden darauf hinzuweisen, dass die Betroffenenrechte (Informationspflicht gem. Art. 13f DSGVO, allenfalls erforderliche Einholung von Einwilligungen) gewahrt werden müssen und gegebenenfalls eine Risikoprüfung und Datenschutzfolgenabschätzung durchzuführen ist sowie allenfalls eine Bewilligung der Datenschutzbehörde erforderlich ist. Weitere wichtige Informationen zum Umgang mit wissenschaftlichen Abschlussarbeiten, die personenbezogene Daten enthalten sind zu finden unter <https://inside.fhv.at/pages/viewpage.action?pagelId=192230106>.

Wenn eine gemeinsame Verantwortung vorliegt oder die Studierenden als Auftragsverarbeiter zu klassifizieren sind, ist es erforderlich, die entsprechenden Verträge (Vereinbarung gemäß Art. 26 oder Auftragsverarbeitungsvereinbarung) abzuschließen.

6. MELDEPFLICHTIGE DATENSCHUTZVORFÄLLE

6.1. MELDUNG VON DATENSCHUTZVERLETZUNGEN („DATA BREACH“)

Als Datenschutzverletzung wird ein Vorfall bezeichnet, durch den Unbefugten der Zugriff auf Daten möglich wird (z.B. Verlust eines Datenträgers, Hackerangriff ...). Dadurch kann den betroffenen Personen ein physischer, materieller oder immaterieller Schaden entstehen, wie etwa der Verlust der Kontrolle über ihre personenbezogenen Daten, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche Nachteile.

Die DSGVO gibt für den Fall einer solchen Verletzung des Schutzes personenbezogener Daten Melde- und Benachrichtigungspflichten vor.

Es ist **unverzüglich** zu melden, wenn Dokumente, IT-Systeme oder Datenträger verloren oder gestohlen wurden. Dies gilt auch für private Geräte, die dienstlich genutzt werden.

6.2. MELDEWEGE

Bei einem Datenschutzvorfall sind folgende Meldewege zu beachten:
Unverzügliche interne Meldung (auch bereits bei Verdacht) telefonisch an Ansprechperson für Datenschutz (derzeit Stabstelle Recht: +43 5572 792 2002) oder Leitung Information Service (= Leitung IS, Vertretung der Ansprechperson Datenschutz bzw. der/des Datenschutzbeauftragten: +43 5572 792 2201 oder per E-Mail an datenschutz@fhv.at

7. WEITERFÜHRENDE VERBINDLICHE REGELUNGEN UND INFORMATIONEN

7.1. IT-SICHERHEITSRICHTLINIEN FÜR MITARBEITERINNEN DER FH VORARLBERG

Diese sind verbindlich einzuhalten und sind im Inside unter folgendem Link zu finden: <https://inside.fhv.at/pages/viewpage.action?pageld=163717136>

7.2. BEFRAGUNGEN, BERICHTE UND STATISTIKEN

Weiters werden die Mitarbeiterinnen und Mitarbeiter der FH Vorarlberg darüber informiert, dass regelmäßig diverse Befragungen durchgeführt werden, von denen sie auch betroffen sein könnten. Die Durchführung derartiger Befragungen ist in der Rahmen-BV zur automationsunterstützten Verarbeitung personenbezogener Daten der Mitarbeiterinnen und Mitarbeiter geregelt, die Befragungen sind unter folgendem Link zu finden:

<https://inside.fhv.at/display/kompakt/Befragungen%2C+Berichte+und+Statistiken>

7.3. ARBEITSBEHELFE ZU COMPLIANCE ANFORDERUNGEN AN HOMEPAGES, FACEBOOK & CO

<https://inside.fhv.at/pages/viewpage.action?pageld=163730730>

7.4. RICHTLINIE SOCIAL MEDIA

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

7.6. ANLEITUNG ZUR VERSCHLÜSSELTEN DATENÜBERMITTLUNG IN E-MAILS

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

7.7. BETRIEBSVEREINBARUNG „AUTOMATIONSUNTERSTÜTZTE EVALUATION LEHRE DURCH DIE STUDIERENDEN“

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

**7.8. BETRIEBSVEREINBARUNG AUTOMATIONSUNTERSTÜTZTE VERARBEITUNG
PERSONENBEZOGENER DATEN DER MITARBEITERINNEN UND MITARBEITER**

<https://inside.fhv.at/pages/viewpage.action?pagelId=162827196>