CHSH

Cerha Hempel Spiegelfeld Hlawati

Datenschutzrichtlinie der Hochschülerinnen- und Hochschülerschaft an der FH Kufstein Tirol (ÖH FH Kufstein)

Verantwortlich für den Inhalt:	Lukas Kraxberger	Vorsitzender der ÖH FH Kufstein
Autor/in:	Matthias Erharter	Datenschutzbeauftragter der ÖH FH Kufstein
Genehmigt durch:		

Vorsitzender der ÖH FH Kufstein

Lukas Kraxberger

Inhalt

Anlagen

Anlage ./1 [LokaleR DatenschutzbeauftragteR]

1. Einleitung und Zielsetzung

In dieser Datenschutzrichtlinie werden die Grundsätze, welche bei der Verarbeitung von personenbezogenen Daten in der ÖH FH-Kufstein zu beachten sind, erläutert. Diese ÖH-Datenschutzrichtlinie gilt für die österreichische Hochschülvertretung an der Fachhochschule Kufstein. AdressatInnen sind auch die einzelnen StudierendenvertreterInnen und Beschäftigten (im Folgenden kurz: MitarbeiterInnen), denen es insbesondere untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten, zu übermitteln oder auf andere Weise zu nutzen. Auch wenn das Datenschutzrecht in weiten Teilen nur das Datengeheimnis natürlicher Personen schützt, sind Geschäfts- und Betriebsgeheimnisse im gleichen Ausmaß als schützenswert anzusehen, sodass von MitarbeiterInnen die gleiche Vertraulichkeit hinsichtlich dieser Geschäfts- und Berufsgeheimnisse erwartet wird wie für beruflich bekannt gewordene personenbezogene Daten.

Diese ÖH-Datenschutzrichtlinie gilt für die Verarbeitungen personenbezogener Daten von natürlichen Personen. Anonymisierte Daten (das sind Daten, die keiner Person zugeordnet werden können), z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser ÖH-Datenschutzrichtlinie.

2. Geltungsbereich

2.1 Anwendungsbereich

Die ÖH-Datenschutzrichtlinie gilt für alle Arten der Verwendung von personenbezogenen Daten der Hochschülerinnen- und Hochschülerschaft, unabhängig vom Ort ihrer Erhebung. Personenbezogene Daten werden in der ÖH FH-Kufstein insbesondere (aber nicht ausschließlich) zu folgenden Zwecken verwendet:

a Zur Verwaltung von Studierendendaten im Rahmen der Aufgaben der Hochschülerinnen- und Hochschülerschaft;

b Zur Verwaltung von MitarbeiterInnendaten;

c Zur Anbahnung, Durchführung und Abwicklung von Verträgen mit Bildungseinrichtungen, LieferantInnen und anderen DienstleisterInnen der ÖH FH-Kufstein im Rahmen der Erbringung von Leistungen für die Hochschülerinnen- und Hochschülerschaft;

d Zum ordnungsgemäßen Umgang mit sonstigen Dritten sowie zur Erfüllung zwingender gesetzlicher Vorschriften.

Die Verwendung der Daten ist ausschließlich im Rahmen der derzeitigen und zukünftigen Aufgaben der ÖH FH-Kufstein gestattet.

2.2 Geltung lokalen Rechts

Diese ÖH-Datenschutzrichtlinie beinhaltet die in der ÖH FH-Kufstein einzuhaltenden Grundsätze bei der Verarbeitung personenbezogener Daten, ohne dass bestehendes lokales

Recht ersetzt wird. Das jeweilige lokale Recht geht dieser ÖH-Datenschutzrichtlinie vor, sofern zwingende Abweichungen oder weitergehende Anforderungen bestehen. Für innerhalb der Europäischen Union verarbeitete Daten richten sich die Anforderungen an die datenschutzkonforme Verwendung der Daten grundsätzlich nach der Datenschutz-Grundverordnung und den gesetzlichen Regelungen des jeweiligen Staates. Insbesondere sind etwaige nach lokalem Recht bestehende Melde- und Genehmigungspflichten im Zusammenhang mit der Verarbeitung von Daten zu beachten.

Die Geltung nationaler Vorschriften, die aus Gründen der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit sowie der Verhütung, Ermittlung und Verfolgung von Straftaten erlassen wurden und zur Weitergabe von Daten an Dritte verpflichten, bleibt von den Regelungen in dieser ÖH-Datenschutzrichtlinie unberührt.

2.3 Beendigung und Kündigung

Die Bindungswirkung dieser ÖH-Datenschutzrichtlinie endet, wenn diese außer Kraft gesetzt wird. Die Beendigung oder Außerkraftsetzung dieser ÖH-Datenschutzrichtlinie befreit die ÖH FH-Kufstein jedoch nicht von den Verpflichtungen und/oder Regelungen dieser ÖH-Datenschutzrichtlinie für die Verwendung bereits übermittelter Daten.

3. Datenschutzorganisation

3.1 DatenschutzbeauftragteR

Die/der Vorsitzende der ÖH FH-Kufstein bestellt für den die ÖH FH-Kufstein eineN zentraleN DatenschutzbeauftragteN.

3.1.1 DatenschutzbeauftragteR

Die/der Datenschutzbeauftragte untersteht in dieser Funktion direkt der/dem Vorsitzenden der Hochschülerinnen- und Hochschülerschaft. Der/die Datenschutzbeauftragte wird durch den/die VorsitzendeN bestellt und die Bestellung in geeigneter Weise kommuniziert. In allen Angelegenheiten des Datenschutzes ist der/die Datenschutzbeauftragte gegenüber allen MitarbeiterInnen der ÖH FH-Kufstein weisungsbefugt. Der/dem Datenschutzbeauftragten sind bereits im Planungsstadium Projekte zur Kenntnis zu bringen, die eine Verarbeitung personenbezogener Daten erfordern können. Sofern die/der Datenschutzbeauftragte als ReferentIn, SachbearbeiterIn oder AngestellteR der ÖH FH-Kufstein bestellt wird, sind zusätzlich die jeweiligen Bestellungs- bzw Wahlvoraussetzungen nach HSG und Satzung einzuhalten.

Der Datenschutzbeauftragte hat die Einhaltung des Datenschutzes stichprobenartig laufend zu überprüfen. Die Überprüfungen sind zu dokumentieren.

Weitere Aufgaben des/r Datenschutzbeauftragten:

a AnsprechpartnerIn für alle Referate und Geschäftsbereiche, einschließlich der ArbeitnehmerInnenvertretung, in der Anwendung und Umsetzung datenschutzrechtlicher Maßnahmen;

b AnsprechpartnerIn für die Datenschutzbehörden und Sicherstellung einer einheitlichen Kommunikation mit den Behörden;

c Zentrale Verwaltung der Verarbeitungsverzeichnisse der Hochschülerinnen- und Hochschülerschaft;

d Kontrolle der AuftragsverarbeiterInnen, die im Auftrag der ÖH FH-Kufstein personenbezogene Daten verarbeiten;

e Auf Anfrage der/des Vorsitzenden, Durchführung einer Risikobewertung sowie, falls erforderlich, Durchführung einer Datenschutz-Folgenabschätzung;

f Kontrolle und Überwachung der Übermittlung personenbezogener Daten in Nicht-EU/EWR-Staaten (inkl. Datenübermittlungen innerhalb der Hochschülerinnen- und Hochschülerschaft);

g Kommunikation mit Betroffenen im Falle von Anfragen oder der Inanspruchnahme von Betroffenenrechte;

h Erarbeitung und Implementierung eines zentralen Betroffenenanfrage und –rechte Managements;

i Meldung von Datenschutzverletzungen;

j Kontrolle datenschutzrechtlicher Vorgaben zur Datensicherheit;

k Erstellung und Aktualisierung von Richtlinien und Leitfäden auf dem Gebiet des Datenschutzes;

l Mitwirkung und Unterstützung bei der Gestaltung von datenschutzrelevanten Vorhaben, Verträgen und Projekten;

m Aufrechterhaltung des ständigen Austausches zwischen den lokalen Datenschutzverantwortlichen zur einheitlichen Umsetzung der datenschutzrechtlichen Vorgaben;

n Sonstige in dieser ÖH-Datenschutzrichtlinie genannte Aufgaben.

Der/die Datenschutzbeauftragte ist berechtigt, zur operativen Durchführung bzw. zu seiner Vertretung geeignete MitarbeiterInnen zu beauftragen. Im Verhinderungsfall wird der/die Datenschutzbeauftragte durch den/die Datenschutzbeauftragte(n)-StellvertreterIn bei der Erfüllung seiner/ihrer Aufgaben vertreten.

Der/die Datenschutzbeauftragte ist berechtigt, geringfügige Änderungen oder Anpassungen in der vorliegenden ÖH-Datenschutz-Richtlinie eigenverantwortlich vorzunehmen, sofern diese den Inhalt nicht materiell verändern.

Der/die Datenschutzbeauftrage erstellt einmal jährlich einen zusammenfassenden Bericht für den/die Vorsitzende/n der ÖH FH-Kufstein betreffend datenschutzrechtliche Themen des vorangehenden Geschäftsjahrs.

Der/die Datenschutzbeauftragte koordiniert die Zusammenarbeit und Abstimmung zu allen wichtigen Fragen des Datenschutzes innerhalb der Hochschülerinnen- und Hochschülerschaft. Er/Sie informiert bei Bedarf den/die Vorsitzende/n zu den aktuellen Entwicklungen oder formuliert Empfehlungen.

Es obliegt dem/der Datenschutzbeauftragten die Datenschutzpolitik innerhalb der ÖH FH-Kufstein zu entwickeln und fortzuschreiben. Die lokalen Datenschutzverantwortlichen der ÖH FH-Kufstein werden dabei angemessen eingebunden. Sie entwickeln die Datenschutzpolitik für die Referate der Hochschülerinnen- und Hochschülerschaft.

3.2 Überprüfungen des Datenschutzniveaus

Überprüfungen der Einhaltung der Vorgaben dieser ÖH-Datenschutzrichtlinie und des sich daraus abzuleitenden Datenschutzniveaus erfolgen durch Kontrollen, die von der/vom Datenschutzbeauftragten anhand eines jährlichen Kontrollplans durchgeführt werden, sowie durch andere Maßnahmen wie etwa Kontrollen der lokalen Datenschutzverantwortlichen oder Reports.

Die Kontrollen des/der Datenschutzbeauftragten werden durch interne oder externe Auditoren durchgeführt. Darüber hinaus werden regelmäßige Self-Assessment Verfahren innerhalb der ÖH FH-Kufstein durchgeführt und von der/vom Datenschutzbeauftragten koordiniert. Die Ergebnisse wesentlicher Kontrollen sowie die dazu vereinbarten Maßnahmen werden dem/der Vorsitzenden der ÖH FH-Kufstein mitgeteilt. Die zuständige Aufsichtsbehörde kann auf Nachfrage eine Kopie des Kontrollergebnisses erhalten. Zudem kann die für eine ÖH FH-Kufstein zuständige Aufsichtsbehörde auch eine Kontrollmaßnahme anstoßen. Diese Kontrollmaßnahmen werden von der jeweiligen ÖH FH-Kufstein bestmöglich unterstützt und die daraus abgeleiteten Maßnahmen werden umgesetzt.

Werden im Rahmen einer Kontrolle Schwachstellen festgestellt, sind diese durch entsprechende Maßnahmen durch die jeweilige ÖH FH-Kufstein zu beheben. Der/die Datenschutzbeauftragte verfolgt die Umsetzung der Maßnahmen. Sollten diese ohne ausreichende Begründung nicht umgesetzt werden, bewertet der/die Datenschutzbeauftragte die Auswirkungen auf den Datenschutz und leitet die notwendigen Konsequenzen und gegebenenfalls Sofortmaßnahmen ein und informiert den/die Vorsitzende/n der Hochschülerinnen- und Hochschülerschaft.

Sofern keine gesetzlichen Beschränkungen bestehen, sind der/die Datenschutzbeauftragte und die lokalen Datenschutzverantwortlichen jeweils für ihr Referat befugt, die ordnungsgemäße Verarbeitung von personenbezogenen Daten zu überprüfen. Dazu gewähren die Referate umfassend Zutritt und Einsicht zu den Informationen, die der/die Datenschutzbeauftragte und die jeweiligen lokalen Datenschutzverantwortlichen zur Aufklärung und Bewertung des Sachverhalts für notwendig erachten. Der/die Datenschutzbeauftragte und die lokalen Datenschutzverantwortlichen können in diesem Zusammenhang Weisungen erteilen.

Die lokalen Datenschutzverantwortlichen bedienen sich im Rahmen ihrer Prüfaufgabe

nach Möglichkeit referatsweit gleichartige Verfahren, z.B. in Form von gemeinsamen Datenschutzaudits. Diese Verfahren können vom/von der Datenschutzbeauftragten zur Verfügung gestellt und koordiniert werden.

3.3 MitarbeiterInnenverpflichtung und Schulung

Die ÖH FH-Kufstein verpflichtet ihre MitarbeiterInnen spätestens bei Aufnahme ihrer Tätigkeit auf das Daten- und Fernmeldegeheimnis. Im Rahmen der Verpflichtung werden die MitarbeiterInnen ausreichend auf die Belange des Datenschutzes geschult. Dafür richtet jedes Referat in Abstimmung mit dem/der Datenschutzbeauftragten geeignete Prozesse ein und stellt Materialien zur Verfügung.

3.4 Zuständige Stellen für Kontakte und Anfragen

Zuständige Stelle für Kontakte und Anfragen zu dieser ÖH-Datenschutzrichtlinie sind die lokalen Datenschutzverantwortlichen (Details entnehmen Sie bitte der Anlage 1) oder der/die Datenschutzbeauftragte.

4. Prinzipien für die Verarbeitung personenbezogener Daten

Jede Verarbeitung personenbezogener Daten hat zum Schutz der Rechte, insbesondere dem Recht auf die Privatsphäre, und Freiheiten der betroffenen Personen nach untenstehenden Grundsätzen zu erfolgen. Bei der Konzipierung neuer Datenverarbeitungen und Erweiterung bestehender Datenverarbeitungen werden die unten angeführten Prinzipien beachtet.

4.1 Transparenzprinzip

Die personenbezogenen Daten sind grundsätzlich bei dem/der Betroffenen selbst zu erheben. Um dem Transparenzprinzip Rechnung zu tragen, treffen eine ÖH FH-Kufstein als Verantwortliche Informations- und Auskunftspflichten. Bei Verarbeitungen von personenbezogenen Daten muss der/die Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden:

– Identität des/der Verantwortlichen (d. h. wer bestimmt die Mittel und Zwecke der Verarbeitung);

– Zweck(e) und Rechtsgrundlage(n) der Verarbeitung; ggf. die berechtigten Interessen, die mit der Datenverarbeitung verfolgt werden;

– EmpfängerIn, an welche die Daten gegebenenfalls weitergegeben werden (auch andere Hochschülerinnen- und Hochschülerschaften fallen hierunter);

– erhobene Datenarten und -kategorien; ggf. die Rechtsgrundlage für internationale Datentransfers;

– Dauer der Datenverarbeitung; Dauer der Datenaufbewahrung; Betroffenenrechte; Beschwerderechte; ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist,

ob der Betroffene verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte; automatisierte Entscheidungen.

Die Informationen müssen den Betroffenen bei der Erhebung der Daten sowie danach stets bei Bedarf zur Verfügung stehen.

4.2 Zulässigkeitsvoraussetzung für die Verarbeitung von personenbezogenen Daten

Grundsätzlich ist jede Verarbeitung von personenbezogenen Daten verboten, außer es gibt einen Erlaubnistatbestand. Eine Ausnahme besteht etwa dann, wenn es eine ausdrückliche gesetzliche Regelung dafür gibt oder die Betroffenen in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben (Rechtfertigung/Erlaubnistatbestand). Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck einer Datenverarbeitung gegenüber der ursprünglichen Zweckbestimmung geändert werden soll. Die Verwendung von bereits erhobenen Daten für andere Zwecke ist nur zulässig, wenn dafür die Zulässigkeitsvoraussetzungen nach Maßgabe der unten angeführten Bestimmungen vorliegen. Erlaubnistatbestände bzw. Rechtfertigungen für eine Verarbeitung personenbezogener Daten sind:

4.2.1 Überwiegende berechtigte Interessen

Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn dies zur Verwirklichung eines berechtigten Interesses des/der Verantwortlichen oder eines Dritten erforderlich ist und schutzwürdige Interessen des Betroffenen nicht überwiegen.

Berechtigte Interessen können beispielsweise das Geltendmachen, die Ausübung und Verteidigung rechtlicher Ansprüche, Betrugsbekämpfung, etc. sein.

4.2.2 Erfüllung vertraglicher Verpflichtungen

Die Verarbeitung ist zulässig, sofern sie für die Erfüllung eines Vertrags, dessen Vertragspartei der Betroffene ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des/der Betroffenen erfolgen, erforderlich ist.

4.2.3 Zustimmungserklärung (Einwilligung des/r Betroffenen)

Die Verarbeitung personenbezogener Daten unterliegt keinen Beschränkungen, sofern der/die Betroffene seine/ihre Einwilligung zur konkreten Verarbeitung für einen oder mehrere bestimmte Zwecke unmissverständlich erteilt hat. Eine Einwilligungserklärung muss jederzeit widerrufbar sein und hat freiwillig, in Kenntnis der konkreten Sachlage zu erfolgen. Zudem sind Einwilligungserklärungen aus Beweisgründen schriftlich einzuholen und aufzubewahren.

Bei Verträgen bei denen der Widerruf dazu führt, dass vertragliche Pflichten nicht mehr erfüllt werden können, ist der/die Betroffene darüber zu informieren.

4.2.4 Gesetze, Verordnungen oder sonstige verbindliche Normen

Die Verarbeitung von personenbezogenen Daten ist auch dann zulässig, wenn dies zur Erfüllung einer rechtlichen Verpflichtung, welcher der/die Verantwortliche unterliegt, erforderlich ist.

Darunter fallen auch Verpflichtungen des/der Verantwortlichen aus Kollektivregelungen. Kollektivregelungen sind Betriebsvereinbarungen, Kollektivverträge, Tarifverträge oder sonstige Vereinbarungen zwischen ArbeitgeberInnen und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweils lokalen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des lokalen Rechts gestaltbar.

4.2.5 Lebenswichtige Interessen des/der Betroffenen

Eine Verarbeitung ist weiters gestattet, um lebenswichtige Interessen des/r Betroffenen oder einer anderen natürlichen Person zu schützen.

4.2.6 Verarbeitung sensibler Daten (besondere Kategorien von Daten und Daten mit strafrechtlichem Bezug)

Die Verarbeitung besonderer Kategorien von Daten (z.B. Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, Gesundheitsdaten, etc.) darf im Rahmen der datenschutzrechtlichen Bestimmungen nur sehr eingeschränkt erfolgen, z.B. wenn dies gesetzlich erforderlich ist, der/die Betroffene ausdrücklich eingewilligt hat oder zum Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin für die Beurteilung der Arbeitsfähigkeit erforderlich ist.

Die Verarbeitung von Daten mit strafrechtlichem Bezug erfolgt nach Maßgabe von lokalen Rechtsvorschriften.

Vor Beginn einer solchen Erhebung, Verarbeitung oder Nutzung sensibler Daten ist der/die jeweils zuständige lokale Datenschutzverantwortliche zu informieren und dies zu dokumentieren.

4.3 Zweckbindungs- und Wesentlichkeitsprinzip

Jeder Verarbeitung von personenbezogenen Daten muss ein bestimmter legitimer Zweck zugrunde liegen. Die Verarbeitung darf nicht in einer mit den festgelegten Zwecken unvereinbaren Weise erfolgen. Personenbezogene Daten dürfen nur für die Zwecke verwendet werden, für die sie ursprünglich erhoben wurden. Die Verwendung von bereits erhobenen Daten für andere Zwecke ist nur dann zulässig, wenn dafür die Zulässigkeitsvoraussetzungen vorliegen.

4.4 Datenvermeidung und -sparsamkeit („Data protection by design and default“)

Unter Datenvermeidung und Datensparsamkeit versteht man, dass nur so viele personen-

bezogene Daten erhoben, verarbeitet und genutzt werden sollen, wie zur Erreichung des angestrebten, legitimen Zwecks erforderlich sind.

Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder pseudonymisierte Daten zu verwenden.

Pseudonymisierung bedeutet, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

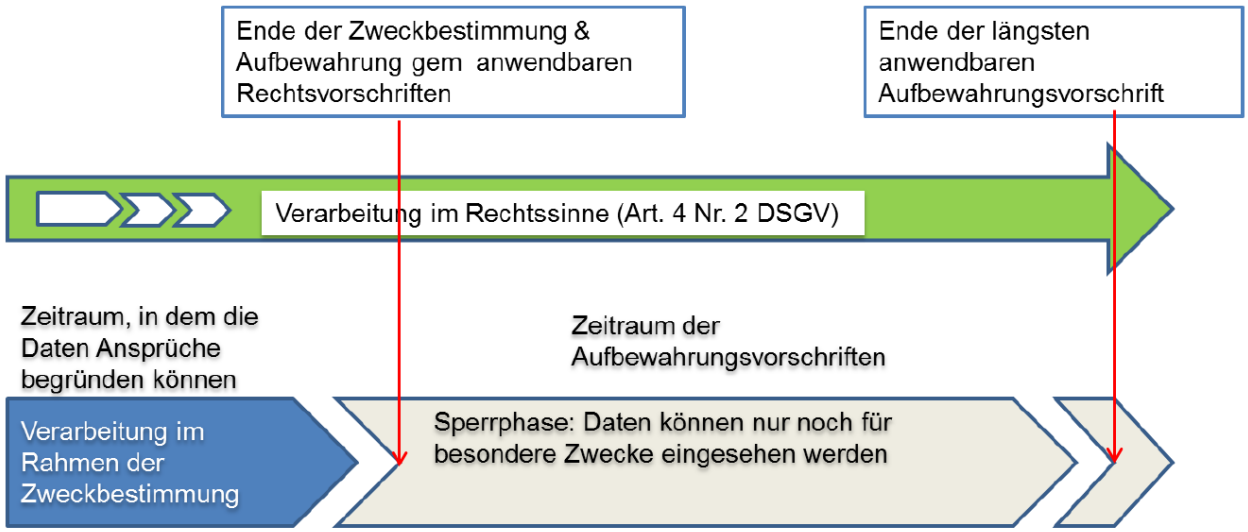
Anonymisierung bedeutet, dass sich (ursprünglich) personenbezogene Daten, nicht oder nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch lokales Recht vorgeschrieben oder erlaubt.

4.5 Löschen und Sperren

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder prozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Dazu sind die Hochschülerinnen- und Hochschülerschaften verpflichtet, in Abstimmung mit dem/der lokalen Datenschutzverantwortlichen für jede Verarbeitungstätigkeit entsprechende Löschkonzepte zu erarbeiten.

Personenbezogene Daten sind zu sperren, wenn der ursprüngliche Verwendungszweck erfüllt ist und (gesetzliche, vertragliche oder satzungsmäßige) Aufbewahrungsfristen anzuwenden sind. Sperren ist das kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.



Bestehen im Einzelfall Anhaltspunkte, dass personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke von Bedeutung sind, muss in Abstimmung mit dem/der lokalen Datenschutzverantwortlichen und dem/der Datenschutzbeauftragten geklärt werden, ob eine weitere Datenverarbeitung zu diesen Zwecken zulässig ist.

4.6 Profiling und automatisierte Entscheidungen

Automatisierte Verarbeitungen von personenbezogenen Daten, durch die einzelne Persönlichkeitsmerkmale (z. B. Auswertung von Fähigkeitsprofilen oder sonstigen Auswertungen im Rahmen der Arbeitsleistung, Analyse der wirtschaftlichen Lage, etc.) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit rechtlichen Folgen oder erheblichen Beeinträchtigungen für den/die Betroffene/n sein. Dem/der Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen müssen die Kontrolle und eine Plausibilitätsprüfung durch eine/n Mitarbeiter/in gewährleistet werden.

4.7 Richtigkeit

Die verarbeiteten personenbezogenen Daten müssen richtig, vollständig und soweit erforderlich auf dem aktuellen Stand sein. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

4.8 Vertraulichkeit und Datensicherheit

Personenbezogene Daten unterliegen dem Datengeheimnis und sind streng vertraulich zu behandeln. Der Zugang zu personenbezogenen Daten durch MitarbeiterInnen ist nur soweit zulässig, soweit dies zur Erfüllung der jeweiligen Aufgaben erforderlich ist („Need-to-Know-Prinzip“).

MitarbeiterInnen dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

MitarbeiterInnen müssen bei Beginn ihrer Tätigkeit über die Pflicht zur Wahrung des Datengeheimnisses unterrichtet werden. Diese Verpflichtung muss auch nach Beendigung des Beschäftigungsverhältnisses fortbestehen.

Bei der Verarbeitung von personenbezogenen Daten sind angemessene organisatorische und technische Maßnahmen umzusetzen, um unberechtigte Zugriffe, unrechtmäßige Verarbeitungen oder Weitergaben sowie versehentlichen Verlust, Veränderung oder Zerstörung zu verhindern. Insgesamt muss durch das Ergreifen von technischen und organisatorischen Maßnahmen ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau erreicht werden. Diese Maßnahmen haben sich am Stand der Technik, den Implementierungskosten, den von der Verarbeitung ausgehenden Risiken

und dem Schutzbedarf der Daten zu orientieren.

4.9 Internet und Telekommunikation

Werden auf Webseiten oder in Apps der ÖH FH-Kufstein personenbezogene Daten erhoben, verarbeitet und genutzt, sind die Betroffenen hierüber in Datenschutzhinweisen und gegebenenfalls Cookie-Hinweisen entsprechend zu informieren. Die Datenschutzhinweise und Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

4.10 Betroffenenrechte

Betroffene haben nicht nur das Recht auf Information über die zu ihrer Person verarbeiteten Daten, sondern auch ein Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragung und Widerspruch zur Datenverarbeitung.

Im Falle von Anfragen von Betroffenen an eine ÖH FH-Kufstein ist diese unverzüglich an den/die lokale/n Datenschutzverantwortliche/n weiterzuleiten und das weitere Vorgehen in Abstimmung mit dem/der Datenschutzbeauftragten und dessen implementierten Betroffenenanfrage- und -rechtemanagements festzulegen. Wenn Daten nur im Auftrag verarbeitet werden, ist die Anfrage an den/die lokale/n Datenschutzverantwortliche/n des/der Verantwortlichen weiterzuleiten. Der/die lokale Datenschutzverantwortliche wird die Identität des Betroffenen feststellen und den Betroffenen über eine allfällige Überschreitung der Frist informieren und die Auskunftserteilung dokumentieren und den Prozess mit dem/der Datenschutzbeauftragten eng abzustimmen.

Der/die lokale Datenschutzverantwortliche wird den/die Datenschutzbeauftragte/n und IT-Verantwortliche/n informieren. Der/die IT-Verantwortliche schafft die technischen Voraussetzungen, um eruieren zu können, in welchen Systemen personenbezogene Daten von Betroffenen verarbeitet werden. Der/die IT-Verantwortliche wird dem/r Datenschutzbeauftragten innerhalb von zwei Werktagen Informationen zur Verfügung stellen, in welchen Systemen die personenbezogenen Daten eines/r Betroffenen verarbeitet werden und welche Daten in diesen Systemen enthalten sind. Der/die lokale Datenschutzverantwortliche, der/die Datenschutzbeauftragte und IT-Verantwortliche werden die Möglichkeiten der Übermittlungsmodalitäten erörtern und feststellen, inwieweit es möglich ist, dem/r Betroffenen durch Bereitstellung eines Fernzugangs zu einem sicheren System direkt Zugang zu den Daten einzuräumen.

5. Besonderheiten bei Studierenden- und VertragspartnerInnendaten

5.1 Datenverarbeitung von Studierendendaten

Studierendendaten, die der ÖH FH-Kufstein von Gesetzes wegen übermittelt werden unterliegen Art 6 Abs 1 lit e DSGVO.

5.2 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten eine/s/r Vertragspartner/in/s dürfen zur Begründung, zur Durch-

führung und zur Beendigung eines Vertrags verarbeitet werden. Dies umfasst auch die Betreuung des/r Vertragspartner/in/s, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrags – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des/der Interessent/in/en erlaubt. InteressentInnen dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell von InteressentInnen geäußerte Einschränkungen sind zu beachten. Für darüber hinausgehende Werbemaßnahmen müssen besondere Voraussetzungen erfüllt sein.

5.3 Datenverarbeitung zu Werbezwecken

Wendet sich der/die Betroffene mit einem Informationsanliegen an eine ÖH FH-Kufstein (z. B. Wunsch nach Zusendung von Informationsmaterial), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

6. Besonderheiten bei MitarbeiterInnendaten

6.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrags erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von BewerberInnen verarbeitet werden. Nach Ablehnung sind die Daten des/r Bewerber/in/s unter Berücksichtigung beweisrechtlichen Fristen zu löschen. In der Regel sind BewerberInnendaten acht Monate ab dem Zeitpunkt, ab dem endgültig klar ist, dass einem/r Bewerber/in kein Angebot gemacht wird oder dieser ein Angebot ablehnt, zu löschen. Darüber hinaus können die Daten aufbewahrt werden, sofern der/die BewerberIn in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt hat. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren erforderlich.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung auf den Zweck des Arbeitsvertrags bezogen sein, sofern nicht ein anderer Erlaubnistatbestand gem. 4.2 die Datenverarbeitung rechtfertigt.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den/die BewerberIn bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des/der Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrags dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können insbesondere gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des/r Mitarbeiter/in/s oder die berechtigten Interessen des Unternehmens sein.

6.2 Datenverarbeitung aufgrund rechtlicher Verpflichtung

Die Verarbeitung personenbezogener MitarbeiterInnendaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen schutzwürdige Interessen des/r Mitarbeiter/in/s berücksichtigt werden. Geht eine Datenverarbeitung über das gesetzliche zulässige Maß hinaus, muss geprüft werden, ob diese Datenverarbeitung auf eine andere Rechtsgrundlage gestützt werden kann.

6.3 Kontrollmaßnahmen

Kontrollmaßnahmen, die eine Verarbeitung von MitarbeiterInnendaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine rechtliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und interner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des/r von der Maßnahme betroffenen Mitarbeiter/in/s am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der MitarbeiterInnen müssen vor jeder Maßnahme festgelegt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte der ArbeitnehmerInnenvertretung, wie in Österreich beispielsweise nach § 96f ArbVG, Informationsrechte des/r Betroffenen) berücksichtigt werden.

7. Weitergabe von personenbezogenen Daten

7.1 Arten und Zwecke der Weitergabe von personenbezogenen Daten

Personenbezogene Daten können derart weitergegeben werden, dass die empfangende Stelle für die erhaltenen Daten eigenverantwortlich ist (Übermittlung), oder dass sie die Daten nur nach Weisung und Maßgabe der weitergebenden Stelle verwenden darf (Auftragsverarbeitung).

Die Weitergabe von personenbezogenen Daten erfolgt ausschließlich zu den oben genannten zulässigen Zwecken im Rahmen der Aufgaben der Hochschülerinnen- und Hochschülerschaft, ihrer rechtlichen Verpflichtungen oder der Einwilligung der betroffenen Person.

7.2 Datenverarbeitung im Auftrag

Der Verantwortliche hat im Zusammenhang mit der Verarbeitung von personenbezogenen Daten die in Punkt 4 normierten Prinzipien einzuhalten. Jede Heranziehung eines Auftragsverarbeiters setzt eine schriftliche Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter voraus („Auftragsverarbeitungsvereinbarung“ oder „Data Processing Agreement“), die einen vorgegebenen Mindestinhalt regeln muss (Gegenstand und Dauer

der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien der Betroffenen und die Pflichten und Rechte des/r Verantwortlichen und des/r Auftragsverarbeiter/in/s).

Ein Auftragsverarbeiter darf die ihm überlassenen personenbezogenen Daten nicht für eigene oder fremde Zwecke verwenden. Die Einbindung von sogenannten Unter- oder SubauftragsverarbeiterInnen durch den/die AuftragsverarbeiterIn zur Erfüllung der vertraglichen Verpflichtungen (Datenverarbeitungstätigkeiten), bedarf der vorherigen Zustimmung des/r Verantwortlichen. Die Zustimmung kann entweder für jedes Subauftragsverarbeitungsverhältnis gesondert oder allgemein mit Information und Widerspruchsrecht des/r Verantwortlichen erteilt werden und ist in der Auftragsverarbeitungsvereinbarung entsprechend zu regeln. Bei der zulässigen Einbindung von SubauftragsverarbeiterInnen hat der/die AuftragsverarbeiterIn den/die SubauftragsverarbeiterIn auf die Vereinbarungen (in Form der „Auftragsverarbeitungsvereinbarung"), die zwischen dem/der AuftragsverarbeiterIn und dem/der Verantwortlichen getroffen wurden, entsprechend zu verpflichten.

Die/der AuftragsverarbeiterIn sind von der ÖH FH-Kufstein sorgfältig nach ihrer Fähigkeit, die Datenverarbeitung im Einklang mit datenschutzrechtlichen Anforderungen zu erbringen und den Schutz der Rechte der betroffenen Personen zu gewährleisten, auszuwählen.

Trotz Abschlusses einer Auftragsverarbeitungsvereinbarung bleiben die Pflichten des/der Verantwortlichen unverändert aufrecht.

8. Verletzung des Schutzes personenbezogener Daten („Datenschutzverletzung")

Eine Verletzung des Schutzes personenbezogener Daten (auch „Data Breach" genannt) sind unbeabsichtigte oder unrechtmäßige Datenvernichtungen, -verluste, -veränderungen, und -offenlegungen. Im Falle der Verletzung des Schutzes personenbezogener Daten (z.B. aufgrund eines Hackerangriffs, Verlust externer Datenträger, etc.) sind die ÖH-internen Melde- und Informationspflichten entsprechend der ÖH-Datenschutzrichtlinie sowie die nach jeweils anwendbaren lokalem Recht bestehenden Melde- und Informationspflichten zu beachten. Jedenfalls sind die lokalen Datenschutzverantwortlichen einer ÖH FH-Kufstein oder der/die Datenschutzbeauftragte über Verstöße oder konkrete Anhaltspunkte für einen Verstoß gegen Datenschutzbestimmungen zu informieren.

Eine Datenschutzverletzung im Sinne dieser ÖH-Datenschutzrichtlinie liegt unabhängig davon vor, ob die Datenschutzverletzung durch bewusste oder unbewusste Aktivitäten erfolgt ist, und unabhängig davon, ob Originaldateien oder Kopien betroffen sind. Ein/e lokale/r Datenschutzverantwortliche/r informiert unverzüglich den/die Datenschutzbeauftragte/n.

Eine Informationspflicht besteht jedenfalls, wenn aufgrund der Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Dies ist beispielsweise der Fall, wenn dem/r Betroffenen ein physischer, materieller oder immaterieller Schaden entsteht, wie etwa der Verlust der Kontrolle über seine/ihre perso-

nenbezogene Daten, Identitätsdiebstahl oder –betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andre erhebliche wirtschaftliche oder gesellschaftsrechtliche Nachteile.

Im Falle einer Datenschutzverletzung oder bei Verdacht auf Vorliegen einer Verletzung ist jede/r MitarbeiterIn verpflichtet, unverzüglich eine Meldung entweder an den lokalen Datenschutzverantwortlichen. Der/die jeweilige lokale Datenschutzverantwortliche und der/die Datenschutzbeauftragte werden einander gegenseitig sowie den/die Vorsitzenden der ÖH FH-Kufstein informieren. Danach werden sie Art und Schwere der nachteiligen Folgen für Betroffene einschätzen.

Inwieweit zusätzlich eine Meldung an die lokale Aufsichtsbehörde (Frist im Regelfall 72 Stunden ab Kenntnis der Datenschutzverletzung), an den/die Betroffene/n sowie an die Öffentlichkeit zu erfolgen hat und gegebenenfalls der Inhalt dieser Meldung sind vom/von der lokalen Datenschutzverantwortlichen. Der/die lokale Datenschutzverantwortliche wird unter Berücksichtigung der Meldefristen unverzüglich, jedenfalls jedoch vor Veröffentlichung bzw. Meldung, den/die Datenschutzbeauftragten sowie den/die Vorsitzende/n der ÖH FH-Kufstein informieren. Der/die lokale Datenschutzverantwortliche und der/die Datenschutzbeauftragte werden, sofern notwendig, eine Meldung an die Behörde und Betroffenen vorbereiten und veröffentlichen. Weitere Maßnahmen zur Schadensbeseitigung zugunsten der Betroffenen werden eventuell nach Maßgabe der Auflagen der Datenschutzbehörde getroffen.

9. Konsequenzen für MitarbeiterInnen

Der/die Datenschutzbeauftragte hat den/die Vorsitzende/n zu informieren, wenn er gravierende Verstöße gegen diese ÖH-Datenschutzrichtlinie durch eine/n MitarbeiterIn der ÖH FH-Kufstein erkennt.

Im Fall eines Verstoßes gegen datenschutzrechtliche Vorschriften oder gegen Bestimmungen dieser ÖH-Datenschutzrichtlinie muss jedeR (angestellte) MitarbeiterIn mit disziplinären oder arbeitsrechtlichen Konsequenzen bzw einer möglichen Abwahl rechnen. Darüber hinaus können missbräuchliche Verarbeitungen personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht in manchen Ländern auch straf- und zivilrechtliche Konsequenzen nach sich ziehen.

10. Verwendete Begriffe

anonymisierte Daten	Bei anonymisierten Daten gibt es keinerlei Personenbezug. Es handelt sich dabei um Daten, bei welchen die Identität des/r Betroffenen für niemanden mehr feststellbar ist. Derartige Daten sind daher auch nicht datenschutzrelevant und unterliegen nicht dieser ÖH-Datenschutzrichtlinie.

AuftragsverarbeiterIn	AuftragsverarbeiterInnen (oder datenschutzrechtliche/r DienstleisterIn) ist eine natürliche oder juristische Person bzw. Personengemeinschaft, die personenbezogene Daten ausschließlich im Auftrag des/der Verantwortlichen verarbeitet. Als AuftragsverarbeiterIn sind häufig beispielsweise die IT-DienstleisterInnen zu qualifizieren. Aber auch im Falle eines Outsourcings spricht man von AuftragsverarbeiterInnen. Zu beachten ist jedoch, dass AuftragsverarbeiterInnen in Bezug auf die personenbezogenen Daten ihrer eigenen MitarbeiterInnen, LieferantenInnen, etc. selbst als Verantwortliche gelten.
Betroffene/r	Jede natürliche Person mit deren personenbezogenen oder personenbeziehbaren Daten in der ÖH FH-Kufstein umgegangen wird.
Datenverarbeitung	Unter „Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung (d.h. Erfassen, Aufnehmen oder Aufbewahren auf einem Datenträger zum Zweck der weiteren Verarbeitung und Nutzung), die Anpassung oder Veränderung (d.h. inhaltliches Umgestalten), das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung (d.h. Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, da die Daten an den Dritten weitergegeben werden oder der/die Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft), Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen (d.h. dauerhaftes Unkenntlichmachen bzw. Vernichten gespeicherter personenbezogener Daten) oder die Vernichtung zu verstehen.
personenbezogene Daten	Von den datenschutzrechtlichen Regelungen sind ausschließlich personenbezogene Daten inklusive sensible Daten (besonderer Kategorien personenbezogener Daten), welche nicht anonymisiert sind, betroffen. Erfasst sind somit alle Informationen, die sich auf eine identifizierte oder identifizierbare (natürliche) Person beziehen. Dazu gehören unter anderem: Name; Firmenname, sofern juristische Personen unter den Anwendungsbereich von Datenschutzgesetzen fallen; Geburtsdatum; Personalnummer; Private und beruf-

	liche Kontaktdaten (Adresse, Telefonnummer, Email); Familienstand; Geschlecht; Bild- und Tonaufzeichnungen (Videos, Fotos, etc.); Sensible Daten (besondere Kategorien personenbezogener Daten wie unten definiert)
Pseudonymisierte Daten	„Pseudonymisierung" ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Pseudonymisierte Daten sind vom Anwendungsbereich der datenschutzrechtlichen Vorschriften und der gegenständlichen Datenschutzrichtlinie ebenfalls erfasst.
Sensible Daten (besondere Kategorien personenbezogener Daten)	Unter „sensible Daten" (besondere Kategorien personenbezogener Daten) sind Daten zu verstehen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Sensible Daten sind beispielsweise Religionsbekenntnis; Medizinische Diagnose; Fingerabdruck; Parteizugehörigkeit. Diese Daten gelten als besonders schutzwürdig, weswegen bei der Verarbeitung dieser Daten erhöhte Vorsicht geboten ist. Aufgrund lokalen Rechts können weitere Daten als besonders schutzwürdig eingestuft sein. So genießen Daten über strafrechtliche Verurteilungen und Straftaten vielfach einen besonderen Schutz.
Verantwortliche/r	Verantwortliche/r ist jene natürliche oder juristische Person bzw. Personengemeinschaft, die die Entscheidung trifft, personenbezogene Daten für einen bestimmten Zweck zu verwenden, bzw. über die Zwecke und Mittel der Verarbeitung entscheidet.

11. Inkrafttreten

Diese ÖH-Datenschutzrichtlinie tritt in der vorliegenden Fassung mit in Kraft und gilt als (Dienst-)Anweisung für alle MitarbeiterInnen der Hochschülerinnen- und Hochschüler-

schaft.

Diese ÖH-Datenschutzrichtlinie wird bei Bedarf über den Vorsitzenden und den Datenschutzbeauftragten aktualisiert und gegebenenfalls um spezielle Regelungen und Richtlinien ergänzt.

Kufstein, 01.November 2018

Anlage ./1

Lokale Datenschutzverantwortliche in Hochschulvertretungen ohne Rechtspersönlichkeit der Hochschülerinnen- und Hochschülerschaft

HV	DatenschutzverantwortlicheR	Kontaktdaten
ÖH FH Kufstein	Matthias Erharter	1810350745@stud.fh-kufstein.ac.at