

DATENSCHUTZ - INFORMATIONSBLATT FÜR STUDENT*INNEN

Informationen zur Datenverarbeitung und zu den Rechten betroffener Personen

Liebe Student*innen,

wir nehmen den Datenschutz an unserer Universität sehr ernst und Eure/Ihre diesbezüglichen Rechte liegen uns sehr am Herzen. Du/Sie erhalten hier alle mitteilungspflichtigen und wissenswerten Informationen zum Datenschutz des AStA an der Universität Lüneburg.

Wer ist bei uns für den Datenschutz verantwortlich und an wen kann man sich bei Fragen wenden:

Verantwortliche Stelle im Sinne der DS-GVO ist:

Studierendenschaft der Universität Lüneburg
Vertreten durch die AStA-Sprecher*innen
Universitätsallee 1, 21335 Lüneburg
Telefon: 04131 / 677 - 1510
E-Mail: sprecherinnen@asta-lueneburg.de
Internet: www.asta-lueneburg.de

Unser Datenschutzbeauftragter:

Tobias Lange
Externer Datenschutzbeauftragter
Berner Heerweg 246, 22159 Hamburg
E-Mail: datenschutz@asta-lueneburg.de
Telefon: 040/ 5700 3925

Organisation des AStA und verschiedener Unterorganisationen:

Der AStA bildet zur Ausübung seiner Tätigkeiten eine Vielzahl von eigenständigen oder unter dem AStA tätigen Organisationen, Organen, Referaten oder anderweitige Vertretungen. Hierfür ist der AStA, vertreten durch die AStA Sprecher*innen als verantwortliche Stelle im Sinne des Datenschutzes.

Einen Überblick über unsere Organisationen, Organe, Referate und sonstigen Vertretungen finden sich auf unserer Webseite: www.asta-lueneburg.de Die Auflistungen auf unserer Webseite haben keinen Anspruch auf Vollständigkeit. Im Weiterem ist nicht jeder Zusammenschluss von Student*innen an der Universität grundsätzlich unter dem AStA legitimiert. Student*innen steht es frei sich beliebig zu organisieren und in beliebiger Rechtsform (universitäts)öffentlich tätig zu sein, ohne dass man dabei dem AStA untersteht. Sollten in einem konkreten Fall

Zweifel darüber bestehen, ob eine Organisation zum AStA gehört, kann Klärung durch Rückfrage beim AStA erfolgen. Diese Datenschutzinformationen beziehen sich nur auf Organisationen, Organe, Referate und Vertretungen, die vom AStA legitimiert sind.

Besonderer Schutz von personenbezogenen Daten Jugendlicher in Bezug auf Dienste der Informationsgesellschaft:

Der Gesetzgeber hat vorgesehen, dass personenbezogene Daten von Personen unter 16 Jahren in der Verarbeitung mit Diensten der Informationsgesellschaft besonders schutzbedürftig sind und dieses in Art. 8 und an anderen Stellen der DS-GVO zum Ausdruck gebracht.

Unsere Angebote, online wie offline, richten sich nicht ausdrücklich oder schwerpunktmäßig an Jugendliche unter 16 Jahren. Dennoch können und werden auch Personen dieser Gruppe sich bei uns über Studienmöglichkeiten und andere Themen informieren. Grundsätzlich erheben und verarbeiten wir auf unseren Webseiten keine personenbezogenen Daten, somit auch keine von Jugendlichen unter 16 Jahren. Wir verwenden auch keine Anwendungen Dritter in unseren Webseiten, die so etwas tun könnten, noch laden wir auf Webseiten Inhalte von dritten Servern. Insbesondere nutzen wir keine Tracking-Cookies oder andere Technologien, die ein Nutzerverhalten aufzeichnen und auch über Anwendungen und Geräte hinaus verfolgen könnten.

Im Rahmen von Härtefallanträgen kann es dazu kommen, dass Daten von Personen unter 16 Jahren, nämlich Daten zu eigenen oder im Haushalt einer Verantwortungsgemeinschaft lebenden Kindern oder Jugendlichen von Student*innen, gespeichert und verarbeitet werden. Dieses geschieht lediglich zum Nachweis einer Bedürftigkeit im Rahmen der Prüfung der Härtefallanträge. Die Verarbeitung und spätere Aufbewahrung dieser personenbezogenen Daten erfolgt auch auf digitalen Wegen. Wir haben für solche Daten besondere technische und organisatorische Maßnahmen getroffen, um eine besonders sichere Verarbeitung zu gewährleisten.

Zweck, Rechtsgrundlagen und Dauer der Speicherung personenbezogener Daten:

(Stand November 2021)

Wir erheben und verarbeiten Daten auf Grundlage der Satzungen und Aufgaben, die wir an der Universität Lüneburg zu erfüllen haben. Uns werden hierzu, im Rahmen Ihrer/Eurer Verträge mit der Universität personenbezogene Daten von der Universität übermittelt. Wir verarbeiten Ihre/Eure Daten zu keinem anderen Zweck als für die Durchführung der von der Universität vorgeschriebenen Aufgaben. Insbesondere übertragen wir Ihre/Eure Daten keinen unbefugten Dritten noch erstellen wir aus den personenbezogenen Daten Profile im Sinne von Art. 4 Abs. 4 DS-GVO.

Rechtsgrundlage für die Verarbeitung der Daten ist dabei der mit Euch/Ihnen geschlossene Vertrag mit der Universität gem. Art. 6 Abs. 1 lit. b.) DS-GVO. Hiernach ist es uns erlaubt alle unmittelbar für die Durchführung der Aufgaben des AStA notwendigen personenbezogenen Daten von Euch/Ihnen zu speichern und zu verarbeiten, als auch diese von der Universität hierfür übertragen zu bekommen.

Wir sind nach gesetzlichen Vorschriften verpflichtet, bestimmte Daten von Euch/Ihnen im Rahmen unserer Aufgaben zu dokumentieren oder an die Universität zu übermitteln, was auf Grundlage von Art. 6 Abs. 1 lit. c.) DS-GVO erfolgt. Wir erheben im Einzelfall personenbezogene Daten über die vorab genannten Daten hinaus, wenn dieses für die Durchführung der Aufgaben erforderlich ist oder gesonderte Umstände es erforderlich machen. Eine derartige Sammlung und Verarbeitung personenbezogener Daten erfolgt entweder auf Grundlage einer freiwilligen ausdrücklichen Einwilligung durch Euch/Sie, im Sinne des Art. 6 Abs. 1 lit. a.) DS-GVO, aufgrund eines berechtigten Interesses gem. Art. 6 Abs. 1 lit. f.) DS-GVO, aufgrund des Schutzes Eurer/Ihrer lebenswichtigen Interessen nach Art. 6 Abs. 1 lit. d.) DS-GVO, aufgrund eines öffentlichen Interesses nach Art. 6 Abs. 1 lit. c.) oder auf der Grundlage von Art. 6 Abs. 1 lit. f.) i.V.m. Art. 9 Abs. 2 lit. f.) DS-GVO, wenn ein berechtigtes Interesse auch die Verarbeitung besonders schutzbedürftiger Daten notwendig macht.

Dieses heißt im Detail, wobei die nachstehende Aufstellung nur als Aufstellung aller möglichen, aber keinesfalls tatsächlich erhobenen Daten jedes Einzelfalls zu sehen ist:

- Wir erheben im Zusammenhang mit Euch/Ihnen:
 - Namens, Adress- und Kontaktdaten
 - Geburtsdaten
 - Matrikelnummern
 - Studienfächer oder Daten zum Studiengang
 - Daten zu Aktivitäten und ehrenamtlichen Aufgaben an der Universität

- Im Rahmen von Härtefallanträgen speichern und verarbeiten wir Daten zur finanziellen Situation, zur Lebenssituation als auch Gesundheitsdaten.
- Wir erheben und verarbeiten von Euch/Ihnen in besonderen Fällen auch biografische Daten (Geburtsort, Lebenslauf, Ausbildung, besuchte Schulen und Arbeitstätigkeiten sowie frühere Wohnorte etc.) wenn solche Informationen zur Durchführung bestimmter Aufgaben notwendig sind.
- Wir ergreifen im Falle eines medizinischen Notfalls Eurer/Ihrerseits, sofern keine anderen Absprachen bestehen, die der Situation angemessenen und notwendigen Mittel. Zu diesem Zweck verarbeiten wir auch Eure/Ihre personenbezogenen Daten, zum Beispiel beim Rufen eines Rettungswagens.
- Sollte in Einzelfällen eine Sammlung und Verarbeitung Eurer/Ihrer personenbezogenen Daten auf Grundlage eines berechtigten Interesses durch uns erfolgen, tätigen wir dieses nur nach einer Abwägung Eurer/Ihrer berechtigten Schutzinteressen, die unsere Interessen nicht übersteigen dürfen, und unter Konsultation unseres Datenschutzbeauftragten. In diesem Fall wird Ihnen die Interessenabwägung in angemessenem Umfang dargelegt.

Sofern wir von Euch/Ihnen Daten verarbeiten, die unter den Art. 9 DS-GVO fallen oder aus einem sonstigen Grund einen besonderen Schutzbedarf haben, geschieht dieses nur auf der Grundlage von besonderen technischen und organisatorischen Maßnahmen, die die rechtmäßige Speicherung und Verarbeitung und ggf. auch Weiterübertragung dieser Daten sicherstellen.

Wir regeln im weiterem die konkreten Verarbeitungen von personenbezogenen Daten und deren Zweck sowie Aufbewahrung in unseren Satzungen und Ordnungen.

Wir bewahren personenbezogene Daten nur so lange auf, wie der Zweck der Verarbeitung vorliegt. Hiernach werden Eure/Ihre Daten unwiederbringlich gelöscht. Sofern gesetzliche Bestimmungen uns zu einer Aufbewahrung Eurer/Ihrer Daten darüber hinaus verpflichten, werden Eure/Ihre Daten archiviert. Derartige Daten sind in der Verarbeitung eingeschränkt und bestehen nur zum Zwecke des Einhaltens der Aufbewahrungsfristen fort. Sie werden nur verarbeitet, soweit es aufgrund gesetzlicher oder sonstiger Bestimmungen zu einer diesbezüglichen Anfrage kommt oder eine Rechtsverteidigung notwendig ist.

Bei der Sammlung und Verarbeitung Eurer/Ihrer persönlichen Daten verfahren wir streng nach dem

(Stand November 2021)

Prinzip der Datensparsamkeit und der minimalen Verwendung. Dieses Prinzip ist auch Grundlage der Verarbeitung Eurer/Ihrer personenbezogenen Daten durch unsere Mitarbeiter*innen und Vertreter*innen. Mitarbeiter*innen und Vertreter*innen erhalten nur auf Grundlage des Minimalprinzips die für die Erbringung der jeweiligen Leistung notwendigen personenbezogenen Daten übermittelt.

Auf dem Prinzip der Datensparsamkeit übermitteln wir auch nur personenbezogene Daten an Dritte, wenn wir hierfür berechtigt oder verpflichtet sind. Es folgt eine Aufstellung möglicher berechtigter Empfänger, aber nicht unbedingt tatsächlicher Empfänger Eurer/Ihrer personenbezogenen Daten:

- Von Euch/Ihnen uns schriftlich benannte Bevollmächtigte oder Kontaktpersonen
- Andere Student*innen
- Stellen der Universität
- Externe dritte verantwortliche Stellen

Ob eine Übertragung an einen dieser Empfänger im Einzelfall erfolgt und mit welchem Umfang an personenbezogenen Daten, basiert auf der mit Euch/Ihnen getroffenen Vereinbarungen und die im individuellen Fall vorliegenden Genehmigungen, Einwilligungen und gesetzlichen Bestimmungen.

Wir bewahren personenbezogene Daten, die Aufbewahrungspflichtig sind, nach den bestehenden gesetzlichen Vorschriften auf. Hiernach sind bestimmte Daten bis zu 10 Jahren aufzubewahren. Im Einzelnen:

- Geschäfts- und Handelsbriefe 6 Jahre
- Buchungsunterlagen 6 Jahre
- Jahresabschlussrelevante Unterlagen 10 Jahre
- Abrechnungsunterlagen 10 Jahre
- Wahlunterlagen nach den Satzungen regelmäßig für die bestehende Wahlperiode
- Verpflichtungserklärungen auf den Datenschutz oder ähnliche Dokumente gem. den Verjährungsfristen 3 Jahre

Ferner kann, auf Grundlage der §§ 195ff BGB, zu Zwecken der Erhaltung gesetzlicher Beweismittel, im Rahmen gesetzlicher Verjährungsfristen in Rechtsstreitigkeiten, eine Aufbewahrungsfrist von bis zu 30 Jahren möglich sein. Wenn wir auf dieser Grundlage personenbezogene Daten über den eigentlichen Zeitraum der verpflichtenden Aufbewahrung aufbewahren, erfolgt dieses auf Grundlage des Art. 6 Abs. 1 lit f.) DS-GVO.

Personenbezogene Daten, für die keine Aufbewahrungspflichten, kein Zweck der Verarbeitung und kein berechtigtes oder öffentliches Interesse mehr bestehen, werden unwiderruflich gelöscht. Sofern

Ihr/Sie zu einzelnen personenbezogenen Daten rechtswirksam ein Euch/Ihnen zustehendes Recht gegenüber uns ausübt, zum Beispiel eine Einwilligung widerruft oder die Löschung bestimmter Daten verlangt, erfolgt diese Löschung unmittelbar und unwiderruflich mit Ausübung des Rechts.

Zu Zwecken der Werbung und Außendarstellung betreiben wir eine Webseite im Internet:

www.asta-lueneburg.de
www.kritische-festschrift.de
www.queereringvorlesung.de

Für die vorgenannten Webseite gelten zusätzlich und vorrangig die Datenschutzbestimmungen, die auf der Webseite ausgeführt sind. Wir sammeln auf dieser Webseite keine personenbezogenen Daten noch setzen wir solche Techniken über Drittanbieter ein. Eine Datenübertragung an Dritte, insbesondere nach außerhalb der EU, erfolgt ebenso nicht.

Zu Kontaktzwecken speichern und verarbeiten wir Eure/Ihre privaten E-Mailadressen. Dieses erfolgt nur nach einer ausdrücklichen freiwilligen Einwilligung durch Euch. Dabei sehen wir diese Einwilligung auch dann, im Sinne eines schlüssigen Verhaltens, als erteilt an, wenn von Euch/Ihnen uns E-Mailadressen zur Kontaktaufnahme oder zu bestimmten Zwecken übermittelt werden und der Wunsch der Kommunikation per E-Mail deutlich erkennbar ist. Wir speichern und nutzen Eure/Ihre privaten E-Mailadressen nur zu dem Zweck, für den uns diese übermittelt wurden. E-Mailadressen veröffentlichen wir grundsätzlich nicht. Sofern in bestimmten Fällen eine Veröffentlichung erfolgt, geschieht diesen nur nach einer freiwilligen informierten Einwilligung durch Euch/Sie. In Hinblick auf mögliche Risiken im E-Mailverkehr oder der Veröffentlichung von E-Mailadressen bitten wir um Kenntnisnahme der Anlage A2 „Risiken im E-Mailverkehr“ zu diesem Informationsblatt.

Wir verarbeiten E-Mailadressen in Massene-mails oder dem Versand an mehrere Personen grundsätzlich nicht in der Form, dass E-Mailadressen eines Empfängers anderen Empfängern offengelegt werden. Hiervon machen wir Ausnahmen, wenn einer Gruppe von Empfängern die E-Mailadressen aller anderen Empfänger bereits bekannt sind oder davon auszugehen ist, dass für den Zweck dieser Kommunikation eine Offenlegung der E-Mailadressen innerhalb einer Gruppe eindeutig von allen beteiligten Empfängern gewollt ist. Im letzteren Sinne also dann, wenn durch den schlüssigen Ausdruck der Empfänger eine Einwilligung deutlich herzuleiten ist. Der Empfang wie Versand von E-Mails erfolgt durch eine per SSL verschlüsselte Verbindung. Wir nutzen keine Techniken, welche eine Weiterver-

(Stand November 2021)

folgung der E-Mails durch Trackingmethoden ermöglicht. Wir versenden auch keine E-Mails, die Daten aus dritten unsicheren Quellen laden.

Im Rahmen von Härtefallanträgen speichern und verarbeiten wir Daten der Antragsteller*innen zu Zwecken der Bearbeitung von Anträgen auf Zuschüsse oder Rückerstattungen gem. der Härtefallordnung der Universität. Hierbei werden ggf. auch besondere Daten im Sinne des Art. 9 DS-GVO verarbeitet. Rechtsgrundlage hierfür ist Art. 6 Abs. 1 lit. e.) DS-GVO ggf. i.V.m Art. 9 Abs 2. lit. a.) DS-GVO. Die im Rahmen der Bearbeitung von Härtefallanträgen verarbeiteten und gespeicherten Daten dienen nur dem Zweck der Durchführung der Bearbeitung und der Möglichkeit einer späteren Überprüfung der Richtigkeit. Die Bearbeitung erfolgt nur durch auf dem Datenschutz verpflichtete Mitarbeiter*innen des AStA und für die Speicherung und Aufbewahrung der Daten gelten besonders hohe Sicherheitsstandards. Die Aufbewahrung der Daten zur Klärung von eventuellen Rechtsansprüchen beträgt 3 Jahre.

In besonderen Fällen veröffentlichen wir von Euch/Ihnen Namen, Bildaufnahmen (Fotos und Videos) oder weitere Informationen in der Presse (online wie offline), auf unseren Webseiten, auf Socialmedia Portalen oder an sonstigen Orten im Internet. Wir tun dieses nur nach Eurer/Ihrer ausdrücklichen, informierten und freiwilligen Einwilligung. Bei jeder erteilten Veröffentlichung werdet Ihr/Sie separat über Art und Umfang der Veröffentlichung in Kenntnis gesetzt. Zu einer informierten und freiwilligen Einwilligung gehört hierbei eine angemessene Belehrung über mögliche Risiken einer solchen Veröffentlichung. Diese befindet sich in der Anlage 1 zu diesem Informationsblatt.

Die Ihnen zustehenden Rechte:

Ihr/Sie habt nach Art. 15 DS-GVO in Verbindung mit § 35 BDSG das Recht von uns eine Auskunft über Eure/Ihre bei uns gespeicherten personenbezogenen Daten und der in Art. 15 DS-GVO näher bestimmten Informationen zu erhalten. Ihr/Sie können dieses Recht durch formlose schriftliche oder (fern)mündliche Aufforderung an uns ausüben. Die Auskunft kann dahingehend beschränkt werden, dass Daten, welche die freiheitlichen Grundrechte dritter Personen betreffen, nicht übermittelt werden. Die Beantwortung der Auskunft erfolgt ggf. in elektronischer Form.

Euer/Ihr Auskunftsrecht erstreckt sich, im Falle der Sammlung und Verarbeitung von personenbezogenen Daten auf Grundlage eines berechtigten oder öffentlichen Interesses, auch darauf, die Abwägung zwischen unseren Interessen und Euren/Ihren

Schutzrechten in ausführlicher Darlegung zu verlangen, unabhängig davon, ob diese Ausführungen Euch/Ihnen bereits vorher schon übermittelt wurden.

Nach Art. 16 DS-GVO habt Ihr/Sie das Recht unrichtige personenbezogene Daten zu Eurer/Ihrer Person korrigieren und unvollständige personenbezogene Daten vervollständigen zu lassen.

Nach Art. 17 DS-GVO habt Ihr/Sie das Recht auf Löschung Eurer/Ihrer Daten. Dieses Recht besteht jedoch nur beschränkt und betrifft vorrangig Daten, die uns freiwillig wurden. Ihr/Sie könnt eine Löschung von personenbezogenen Daten, die auf Grundlage einer gesetzlichen Verpflichtung oder zur Durchführung einer Leistung gesammelt und verarbeitet wurden und weiterhin werden, in der Regel nicht verlangen. Näheres zu einer rechtswirksam möglichen Löschung enthält Art. 17 DS-GVO.

Sofern wir von Euch/Ihnen personenbezogene Daten auf Grundlage Ihrer freiwilligen Einwilligung speichern und verarbeiten, könnt Ihr/Sie diese Einwilligung jederzeit widerrufen. Der Widerruf kann auch teilweise oder für bestimmte Verarbeitungszwecke begrenzt erfolgen. Der Widerruf einer Einwilligung stellt keine Ausübung des Rechts auf Löschung nach Art. 17 DS-GVO dar. Sofern Ihr/Sie mit dem Widerspruch auch die Löschung von Daten verlangen wollt, müsst Ihr/Sie diese separat erklären. Eine solche Erklärung kann zusammen mit der Ausübung des Widerspruchs erfolgen.

Nach Art. 18 DS-GVO habt Ihr/Sie das Recht die Einschränkung der Verarbeitung Eurer/Ihrer personenbezogenen Daten zu verlangen, wenn eine der hierfür im Art. 18 DS-GVO bestimmten Voraussetzungen vorliegt. Eine Speicherung Ihrer personenbezogenen Daten ist uns sodann weiterhin erlaubt, obliegt aber engen Beschränkungen in der Verarbeitung, die sich aus der Art der Sachumstände ergeben.

Nach Art. 20 DS-GVO könnt Ihr/Sie die Übertragung Ihrer Daten an eine dritte verantwortliche Stelle verlangen. Hierzu können wir Euch/Ihnen die Daten wahlweise in einer gängigen strukturierten digitalen Form zur Verfügung stellen oder, gemäß einem vorliegenden Auftrag, direkt an eine dritte Partei übermitteln. Eine andere Form der Übertragung, sofern es uns technisch möglich ist, wäre im individuellen Fall zu besprechen. Art. 20 DS-GVO enthält weitere Regelungen zu Art und Umfang der diesbezüglichen Rechte und unserer Pflichten.

Nach Art. 21 DS-GVO habt Ihr/Sie das Recht Widerspruch auszuüben, wenn wir Eure/Ihre personenbezogenen Daten nach Art. 6 Abs. 1. lit e.) oder

(Stand November 2021)

f.), sprich auf Grundlage eines berechtigten eigenen oder öffentlichen Interesses, verarbeiten. Sofern wir keine zwingenden Gründe, welche Eure/Ihre schutzbedürftigen Rechte überwiegen, zum Beispiel die Ausübung oder Abwehr von Rechtsansprüchen, hiergegen anführen können, werden wir die Erhebung und Verarbeitung dieser personenbezogenen Daten umgehend einstellen. Sofern Sie weitere Rechte ausüben, zum Beispiel das Recht auf Löschung, werden wir diese Löschung umgehend vornehmen.

Soweit nicht nach Art. 12 Abs. 5 Satz 2 DS-GVO bestehende Umstände vorliegen, ist die Ausübung Eurer/Ihrer Rechte kostenlos. Umstände im Sinne des Art. 12 DS-GVO wären offenkundig unbegründete oder, insbesondere im Fall von häufiger Wiederholung, exzessive Anträge einer betroffenen Person. In diesem Fall kann der Verantwortliche entweder ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung, die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder sich weigern, aufgrund des Antrags tätig zu werden.

Als betroffene Person habt Ihr/Sie ferner, nach Art 77 DS-GVO i.V.m. § 19 BDSG, unbeschadet weiterer und anderer, auch gerichtlicher Rechtsmittel, das Recht auf Beschwerde bei einer zuständigen Datenschutz-Aufsichtsbehörde, wenn Sie einen Verstoß gegen den Datenschutz bei uns vermuten. Zuständige Aufsichtsbehörde ist:

Die Landesbeauftragte für den
Datenschutz in Niedersachsen
Prinzenstr. 5
30159 Hannover
Tel. 0511 / 120 45 00
Fax. 0511 / 120 45 99
E-Mail: poststelle@lfd.niedersachsen.de
Website: www.lfd.niedersachsen.de

Sofern Ihr/Sie einen Datenschutzverstoß, der mit uns in einem Zusammenhang steht, feststellt, ohne dass Ihr/Sie selbst persönlich Betroffener hierbei seid, könnt Ihr/Sie diesen Verstoß zur Bearbeitung von Amts wegen an die zuständige Aufsichtsbehörde melden.

Technische und organisatorische Maßnahmen zu Ihrem Schutz:

In allen unseren Prozessen liegt uns die Sicherheit, die Verfügbarkeit und die Richtigkeit Eurer/Ihrer personenbezogenen Daten am Herzen. Wir haben daher umfangreiche Maßnahmen getroffen, um dieses für Euch/Sie sicherzustellen. Gleichmaßen ist es unser Ziel, nicht mehr benötigte und nicht

mehr aufbewahrungspflichtige personenbezogene Daten final zu löschen.

Zu jedem Prozess von Verarbeitungstätigkeiten personenbezogener Daten führen wir eine Risikoanalyse durch, in welcher wir die Schutzwürdigkeit unter Aspekten von Verlust, Verfälschung, unberechtigter Einsicht durch Dritte oder Veröffentlichung beurteilen. Für Eure/Ihre Gesundheitsdaten, die wir im Rahmen der Durchführung der Härtefallanträge sammeln und verarbeiten, gilt grundsätzlich ein hohes Schutzniveau.

Wir praktizieren manuelle und automatisierte Verfahren, welche eine Löschung Eurer/Ihrer nicht mehr benötigten und nicht mehr aufbewahrungspflichtigen Daten sicherstellen. Hiermit verwirklichen wir Ihr Recht auf „digitales Vergessenwerden“ und minimieren so Risiken, denn nicht mehr vorhandene Daten können auch nicht verloren werden. Die endgültige Löschung von digitalen Daten oder Papierdokumenten erfolgt nach den hierfür vorgeschriebenen Vorschriften durch Schreddern gemäß DIN-Norm 66399.

Wir haben unsere Räumlichkeiten durch Alarmsysteme, Sicherheitsschlösser sowie Zutrittsbeschränkungen und Zutrittskontrollen in angemessenem Maße gegen Diebstahl und Einbruch gesichert.

Die von Euch/Ihnen bei uns gesammelten Daten, sofern diese in Papierform vorliegen, werden in verschlossenen und vor Feuer und Wasser geschützten Schränken sicher verwahrt. Wir sind bestrebt Papierdokumente zeitnah und vollständig zu digitalisieren, um so eine zusätzliche Sicherung gegen Verlust vorzuhalten. Sofern Papierunterlagen nach einer Digitalisierung nicht mehr erforderlich sind, vernichten wir diese durch ein zertifiziertes Aktenvernichtungsunternehmen oder durch Schreddern nach vorgeschriebener DIN-Norm 66399.

Sofern wir für die Vernichtung von personenbezogenen Daten, gleich ob digital oder in Papierform, dritte Unternehmen (Aktenvernichter) beauftragen, schließen wir mit diesen Unternehmen bei Auftragsvergabe grundsätzlich einen Auftragsverarbeitungsvertrag (AVV) ab.

Digital gespeicherte Daten werden nach dem allgemeinen Stand der Technik nur verschlüsselt aufbewahrt. Sofern eine Verarbeitung eine Übertragung der digitalen Daten an Mitarbeiter*innen oder andere berechnete Personen

(Stand November 2021)

oder Institutionen erforderlich macht, erfolgt diese Übertragung verschlüsselt.

Wir protokollieren jede Veränderung an digitalen Daten in einem Logfile. Ein solcher Logfile enthält mindestens Tag und Uhrzeit der Änderung, das Gerät, auf welches diese Änderung vorgenommen wurde, den Benutzer, der die Änderung getätigt hat, und Informationen zu Art und Umfang der Änderung. Derartige Logfiles werden automatisiert erstellt und sind nur den ASTa Sprecher*innen zugänglich.

Wir haben EDV-Geräte zur Speicherung und Verarbeitung von Daten angeschafft, die in Ihrer Funktionalität und in ihrem Umfang den Notwendigkeiten Rechnung tragen. Die EDV-Ausstattung stellt sicher, dass unter rein technischen Aspekten Eure/Ihre Daten angemessen sicher und jederzeit verfügbar gespeichert werden. Dieses ist auch dann sichergestellt, wenn eine maximale Belastbarkeit der EDV-Systeme praktiziert wird.

Wir schützen Eure/Ihre Daten gegen technische und vorsätzlich rechtswidrige Einwirkungen, sowie Fälle von Naturkatastrophen oder anderen Unfällen, einschließlich Feuer, durch die Anfertigung von Sicherungskopien. Hierbei erstellen wir interne sowie auch externe Sicherungskopien. Sicherungskopien werden nur in verschlüsselter Form erstellt. Sofern es sich um externe oder offline Sicherungen handelt, stellen wir sicher, dass die physischen Träger unter angemessenen Schutzvorkehrungen an sicheren Orten verwahrt werden.

Sofern wir für die Herstellung von Sicherungskopien, die Wartung unserer EDV-Anlagen oder die Wahrnehmung sonstiger IT-Dienstleistungen mit Zugriff auf unsere EDV-Systeme dritte Unternehmen beauftragen, dann erfolgt dieses nur, nachdem wir mit diesen Unternehmen einen Auftragsverarbeitungsvertrag (AVV) geschlossen haben.

Durch die in unserem Haus intern oder auch extern zuständigen Beauftragten für die Datensicherung wird ein Verfahren, unter Würdigung verschiedenster Szenarien, regelmäßig durchgespielt, welches die Wiedereinspielung von Sicherungskopien in unsere EDV-Systeme praktisch erprobt und sicherstellt. Somit sind wir in der Lage auch bei einer Zerstörung der EDV-Systeme den Geschäftsbetrieb aufrecht zu erhalten oder in kürzester Zeit wieder zu errichten.

Ferner haben wir zusätzliche Maßnahmen zur Sicherung der automatisierten Datenverarbeitung in umgesetzt:

- Serverräume sind separat verschlossen.
- Betriebsfremden Personen ist ein unbegleiteter Aufenthalt in Büroräumen nicht gestattet
- Server und Endgeräte sind passwortgeschützt
- Anmeldungen an unserem EDV-System können nur durch Benutzernamen in Kombination mit sicheren Passwörtern erfolgen und in besonders sensiblen Bereichen ist eine Zwei-Faktoren-Authentisierung eingesetzt
- Benutzerkonten sind so beschränkt, dass die jeweiligen Benutzer nur Zugang auf die für die Ausübung ihrer Tätigkeit absolut notwendigen personenbezogenen Daten haben
- Unser EDV-System ist durch Firewall und Anti-Malware-Software geschützt und nur zugelassene Prozesse können Daten aus dem geschlossenen System heraus übertragen.

Darüber hinaus haben wir weitere geeignete Maßnahmen zur Eingabe-, Übertragungs- und Transportkontrolle getroffen, sowie weitere Maßnahmen zur Zuverlässigkeit der Systeme.

Wir haben für den Fall einer Datenpanne oder eines Vorfalls mit personenbezogenen Daten ein Notfallverfahren erarbeitet, welches auch die Meldung an die zuständige Aufsichtsbehörde einschließt.

Wir haben ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen und zur Gewährleistung der Sicherheit der Verarbeitung eingeführt. Im Rahmen dieser Umsetzung stehen die ASTa-Sprecher*innen im regelmäßigen Austausch mit dem Datenschutzbeauftragten und den IT-Beauftragten/Dienstleistern. Mindestens einmal jährlich wird eine Ist-Aufnahme der Prozesse vorgenommen und mit den Soll-Vorgaben abgeglichen. Die Ergebnisse werden dokumentiert und etwaigen Abweichungen wird durch geeignete Maßnahmen abgeholfen.

Der Datenschutzbeauftragte und die an der Sicherheit der IT beteiligten Personen bilden sich fortlaufend weiter und treffen geeignete Maßnahmen, die Technik und Organisation im ASTa stets zeitnah an den aktuell geforderten Stand anzupassen oder den ASTa-Sprecherinnen notwendige, erforderliche Maßnahmen zu empfehlen.

Anlage 1 – Risiken in der Veröffentlichung von personenbezogenen Daten im Internet

Grundsätzlich besteht bei einer Veröffentlichung von personenbezogenen Daten, insbesondere Namensdaten und Bildaufnahmen, ein Risiko erkannt und hieraufhin angesprochen zu werden. Insofern wird eine Verbindung zu unserer Universität hergeleitet werden können und andere Personen könnten den Rückschluss ziehen, dass ein Studium an der Universität erfolgt oder Leistungen des AStA in Anspruch genommen werden. Sofern Ihr/Sie mit diesen Daten auch Informationen zu Eurer/Ihrer Person oder den bei uns in Anspruch genommenen Leistungen zur Veröffentlichung freigibt, können

Dritte diese mit Euch/Ihnen in Verbindung bringen und auch in Bezug auf Eure/Ihre Person speichern und verarbeiten (Profiling), ohne dass dieses technisch oder organisatorisch verhindert werden kann. In der Regel ist eine solche Praktik durch dritte Personen oder Unternehmen rechtswidrig und Ihr/Sie könnt hiergegen ggf. auf dem Rechtsweg vorgehen.

Informationen über Euch/Sie, die Dritte durch unsere Veröffentlichungen erlangen, können zu einem gezielten Kontakt zu Euch/Ihnen zu Zwecken von Werbung, Marketing, Stellenvermittlung sowie politi-

(Stand November 2021)

scher/religiöser Werbung oder ideologischer Beeinflussung führen.

Für die Veröffentlichung von Bildaufnahmen im Internet (Online-Veröffentlichungen) gilt grundsätzlich, dass dritte Personen diese Bilder und Videos durch einfache technische Mittel (Screenshot/Videomitschnitt) widerrechtlich in Besitz nehmen und zu eigenen Zwecken nutzen können. Dabei ist eine Veröffentlichung auf anderen Webseiten oder Socialmediaportalen mit unkontrollierter Verbreitung im Internet nicht auszuschließen. Wir können einen solchen Missbrauch weder technisch noch organisatorisch verhindern und auch die Möglichkeiten auf dem Rechtsweg gegen diese Personen vorzugehen, die widerrechtlich Bildaufnahmen vervielfältigen und nutzen, kann erschwert oder ganz unmöglich sein.

Darüber hinaus werden Socialmedia Plattformen und sonstige Portale regelmäßig auf Servern in Ländern außerhalb der Europäischen Union betrieben. Hier gilt die Datenschutzgrundverordnung (DS-GVO) nicht und nur die wenigsten Anbieter haben ein entsprechendes Datenschutzniveau. Sie/Ihr geht daher das Risiko ein, das so veröffentlichte Bildaufnahmen durch die Anbieter zu eigenen Zwecken, insbesondere Werbezwecken, genutzt werden, aber auch an beliebige Dritte weiterverkauft oder übertragen werden. Hierbei könnten auch Bildaufnahmen mit anderen Daten von Ihnen/Euch zu einem Profil Ihrer Person zusammengeführt werden. Dieses auch dann, wenn ein Name zu dem Bild nicht veröffentlicht wurde, da durch technische Methoden eine Identifizierung der Person dennoch erfolgt. In diesem Zusammenhang kann auch eine biometrische Erkennung und Speicherung der Gesichtsdaten nicht ausgeschlossen werden. Möglichkeiten an Rechtsmitteln hiergegen bestehen für Sie/Euch in der Regel nicht, und es wird in einem solchen Fall

Anlage 2 – Risiken im Zusammenhang mit E-Mailadressen

Bei der Verarbeitung von E-Mailadressen ist auch unter der Wahrung einer SSL oder anderen Verschlüsselungsform bei Versand oder Abruf grundsätzlich keine absolute Sicherheit zu gewähren. Eine SSL Verschlüsselung besteht grundsätzlich nur mit dem Abruf- oder Versandserver und stellt keine end-to-end Verschlüsselung dar.

Da eine end-to-end Verschlüsselung nicht gewährleistet werden kann, ist das Mitlesen von E-Mails durch dritte Personen, insbesondere ein technischer Scan von Inhalten einer E-Mail, nicht auszuschließen. Dieses gilt auch für nicht verschlüsselte oder ungesicherte Anhänge einer E-Mail.

nicht oder nur sehr erschwert möglich sein, die Bildaufnahmen/Daten einer nicht zugestimmten Verarbeitung und unkontrollierten Verbreitung im Internet zu entziehen.

Auf Socialmedia Plattformen (Facebook, Instagram, Twitter etc.) können Bildaufnahmen als auch Textbeiträge durch Teilen weiterverbreitet werden und so sehr schnell eine sehr große Anzahl an Personen und sehr hohe Aufmerksamkeit erreichen. Dabei haben wir in der Veröffentlichung auf Socialmedia Plattformen nur begrenzten Einfluss auf die Kommentare von anderen Personen. Wir können dabei nicht ausschließen, dass es zu Textbeiträgen oder Bildaufnahmen und den darauf zu sehenden Personen auch negative oder missbräuchliche Kommentare gibt. Dieses gilt insbesondere in der Weiterverbreitung durch Teilen als auch im Falle einer widerrechtlichen Vervielfältigung und einer unkontrollierten Verbreitung im Internet durch Dritte.

Bildaufnahmen können im schlimmsten Fall durch technische Mittel (Photoshop etc.) modifiziert oder gänzlich verfälscht werden, so dass Personen in peinlichen, beschämenden oder erniedrigenden Situationen und auch in gänzlich falschen, so nie stattgefundenen Situationen, die ggf. für eine Person kompromittierend sein können, gezeigt werden.

Im Rahmen des vorherig gesagten ist es ebenso möglich, dass E-Mailadressen in einem Einzel-, Gruppen- oder Massenversand technisch abgefangen werden, um diese Adressen zum Übersenden von SPAM jeder Art, einschließlich dem Übersenden von Links oder Anhängen zu/mit Schadware, zu missbrauchen.

Wir können den Schutz Ihrer/Eurer E-Mail nur auf unseren Systemen sicherstellen. Sofern es zu einem berechtigten Versand von Gruppen-E-mails mit der Offenlegung der Adressen an mehrere Empfänger kommt, können wir auf die Sicherheit der geschäftlichen oder privaten Geräte Dritter, die zum Abruf der E-Mails genutzt werden, keinen Einfluss nehmen. Diese Geräte können durch Malware infi-

ziert sein und so E-Mailadressen einer ganzen Gruppe auslesen und zu SPAM Zwecken nutzen.

SPAM E-Mails, die Ihr/Sie möglicherweise durch ein Abgreifen der eigenen E-Mailadresse bei Dritten erhalten, können so gestaltet sein, dass diese von seriösen E-Mails nicht zu unterscheiden sind. Hierbei wird regelmäßig versucht an Passwörter oder Bankdaten von Ihnen zu kommen sowie Malware auf Ihrem Endgerät zu installieren. Letzteres kann insbesondere durch das Öffnen von Anlagen und das Klicken von Links erfolgen. Dieses gilt auch für Links, die vortäuschen zu einer Abmelfunktion des Verteilers oder einem Impressum etc. zu führen.

E-Mailadressen stellen grundsätzlich ein personenbezogenes Merkmal im Sinne des Datenschutzes dar. Sie können bestimmten natürlichen Personen zugeordnet werden. Über den Quellcode kann die IP-Adresse und der Ort sowie das genutzte Endgerät für Versand oder Abruf rückverfolgt werden.

Sofern wir E-Mailadressen auf Grundlage der dafür erteilten Einwilligung veröffentlichen, können wir ein Abgreifen dieser Adressen durch dritte Personen technisch nicht verhindern. Veröffentlichte E-Mailadressen können sich unkontrolliert im Netz und für SPAM-Zwecke jeder Art verbreiten.

E-Mailadressen können ferner zu Zwecken von Profiling verwendet werden als auch zu einer direkten ungewollten Kontaktaufnahme durch dritte Personen führen. Diese Kontaktaufnahme kann zu Zwecken von Werbung, Stellenvermittlung, Glückspiel etc. erfolgen. Es kann dabei nicht ausgeschlossen werden, dass die E-Mailadresse auch zu Zwecken von Stalking, Mobbing oder von Hass und Hetze gegen Euch/Sie genutzt wird.