

Datenschutzhinweise und Erklärungen für neue Mitarbeiter und Mitarbeiterinnen sowie Lehrbeauftragte an der FH Aachen

Datenschutzhinweise

§ 1 | Die verantwortliche datenführende Stelle an der FH Aachen ist das Dezernat I - Personal.

> **Anschrift:** FH Aachen - Dezernat I - Bayernallee 11 - 52066 Aachen

§ 2 | Rechtsgrundlage für die mit Ihrer Einstellung verbundene Datenerhebung sind:

- > das Gesetz über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) vom 16. September 2014,
- > Gesetz über die Statistik für das Hochschulwesen sowie für die Berufsakademien vom 2. November 1990,
- > das Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen - DSGVO NRW vom 17. Mai 2018),
- > die Netzordnung der Fachhochschule Aachen vom 22. Mai 2015,
- > sonstige Ordnungen und Satzungen der FH Aachen.

§ 3 | Personenbezogene Daten sind Einzelangaben über Ihre persönlichen und sachlichen Verhältnisse und unterliegen dem Datengeheimnis. Eine Weiterleitung Ihrer Daten erfolgt nur in den gesetzlich zulässigen Fällen und nur im unbedingt notwendigen Umfang.

§ 4 | Nach Beendigung des Dienstverhältnisses werden nur die gesetzlich geforderten personenbezogenen Daten des Mitarbeiters oder der Mitarbeiterin für die gesetzlich vorgegebenen Fristen vorgehalten.

§ 5 | Soweit dies für die Aufgabenerfüllung unabdingbar ist, werden einzelne persönliche Daten an die Datenverarbeitungszentrale der FH Aachen (DVZ) weitergeleitet. Die Daten werden dort ausschließlich im Rahmen ihrer Zweckbestimmung gespeichert und verarbeitet. Die DVZ richtet für jeden Mitarbeiter und jede Mitarbeiterin eine persönliche Benutzer-ID zur Nutzung der IT-Dienste der FH Aachen ein. Im „Welcome Process“, den Sie über Ihren IT-Support vor Ort initiieren, werden Ihre persönlichen Zugangsdaten aktiviert und Ihnen dort ausgehändigt.

§ 6 | Die FH Aachen stellt jedem Mitarbeiter und jeder Mitarbeiterin ein E-Mail-Konto zur Verfügung. Über dieses E-Mail-Konto kommuniziert die Hochschule mit ihnen. Jeder Mitarbeiter und jede Mitarbeiterin ist verpflichtet, dieses E-Mail-Konto regelmäßig abzufragen. Das Mailsystem wird gemeinsam von der FH Aachen und der RWTH Aachen im Rechenzentrum der RWTH betrieben. Weitere Informationen zum Mailsystem und zur E-Mail-Nutzung finden Sie auf den Internetseiten der DVZ.

§ 7 | Im Rahmen der Bearbeitung von Beihilfeanträgen werden einzelne persönliche Daten (Bankverbindung, Beschäftigungszeitraum, Name und Adresse) zur Berechnung der Erstattungsleistungen an die Beihilfestelle der RWTH weitergeleitet.

Merkblatt zum Datenschutz

Dieses Merkblatt hilft Ihnen, den Datenschutz zu verstehen und im Arbeitsalltag anzuwenden.

Was ist Datenschutz?

Jeder Bürger hat das Grundrecht auf informelle Selbstbestimmung. Damit dieses Recht gewahrt bleibt, reglementiert der Datenschutz die Verarbeitung personenbezogener Daten. Artikel 4 Nr. 2 der EU-Datenschutzgrundverordnung (EU-DSGVO) definiert, welche Handlungen im Zusammenhang mit personenbezogenen Daten durch den Begriff „Verarbeitung“ eingeschlossen sind.

Was sind personenbezogene Daten?

Im Sinne der EU-DSGVO bezeichnet der Ausdruck „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (siehe Artikel 4 Nr. 1 EU-DSGVO).

Es geht also um Informationen, anhand dessen Menschen identifiziert werden können. Dazu gehören auch Angaben, die mit zusätzlichen Informationen eine Identifikation ermöglichen.

Beispiele für personenbezogene Daten:

Name, Alter, Familienstand, E-Mail-Adresse, Login-Daten, Anschrift, Krankendaten, Religionszugehörigkeit, Zeugnisse, Gewerkschaftszugehörigkeit, biometrische Daten, Kontodaten, Personalnummer, Matrikelnummer, Autokennzeichen oder IP-Adresse.

Merksätze

- > Die Verarbeitung personenbezogener Daten ist grundsätzlich nicht erlaubt, außer
 - eine Rechtsgrundlage erlaubt oder fordert die Verarbeitung der Daten, oder
 - die betroffene Person willigt wirksam in die Verarbeitung der Daten ein (Verbot mit Erlaubnisvorbehalt)Die verantwortliche Stelle ist verpflichtet, die Rechtsgrundlage für die Datenverarbeitung zu benennen und zu dokumentieren.
- > Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden (Zweckbindung).
- > Aktionen oder Transaktionen mit personenbezogenen Daten müssen unabstreitbar und nachvollziehbar sein (Transparenz, Revisionsfähigkeit).
- > Es sind nur die personenbezogenen Daten zu verarbeiten, die zur Erfüllung des vorgesehenen Zwecks unbedingt erforderlich sind (Datenminimierung, Erforderlichkeit). Die Verarbeitung dieser Daten ist auch nur zu diesem Zweck zulässig (Nichtverkettung).
- > Der Datenschutz räumt der betroffenen Person das Recht auf Auskunft, Berichtigung, Widerruf, Widerspruch, Löschung oder Sperrung seiner Daten ein (Betroffenenrechte, Intervenierbarkeit).
- > Informationen und Mitteilungen zur Verarbeitung müssen dem Betroffenen in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache bereitgestellt werden (Verständlichkeit, Transparenz).
- > Datenschutzpannen sind unverzüglich, spätestens innerhalb eines Zeitraums von 72 Stunden, gegenüber der Aufsichtsbehörde (LDI NRW) zu melden (siehe Artikel 33 EU-DSGVO).

Datenschutzkonformes Verhalten

Jeder Beschäftigte ist für den Umgang mit personenbezogenen Daten nach den Vorgaben des Datenschutzes an seinem Arbeitsplatz und seinem Aufgabenbereich verantwortlich. Beachten Sie folgende einfache Verhaltensregeln, um die Ihnen anvertrauten Informationen vor dem Zugriff unbefugter Dritter zu schützen.

Am Kopierer, Drucker, Fax	Am Telefon	Am Arbeitsplatz
<ul style="list-style-type: none"> > Lassen Sie keine Originale bzw. Ausdrücke am bzw. im Gerät liegen. > Prüfen Sie, ob personenbezogene Daten geschwärzt werden müssen. > Kontrollieren Sie die eingetippte Nummer, bevor Sie das Fax absenden. > Überprüfen Sie bei vertraulichen Faxmitteilungen, dass der Empfänger das Fax persönlich entgegennimmt (vorheriges Telefonat zur Klärung). > Versenden Sie nur das, was der Empfänger benötigt. > Bewahren Sie Sende- und Empfangsprotokolle auf. > Löschen Sie regelmäßig den Zwischenspeicher des Geräts. > Kopieren Sie so wenig wie möglich. > Entsorgen Sie missglückte oder überflüssige Kopien bzw. Ausdrücke sicher (Shredder). 	<ul style="list-style-type: none"> > Achten Sie darauf, dass Sie keine unberechtigten Zuhörer haben. > Mithören Dritter (z. B. per Lautsprecher) nur mit ausdrücklicher Einverständniserklärung des Gesprächspartners. > Können Sie den Gesprächspartner eindeutig identifizieren (z. B. Stimme)? > Geben Sie keine Informationen zu Mitarbeiterinnen und Mitarbeitern oder Studierenden (Krankheit, Aufenthalt, Urlaub usw.). > Geben Sie keine Informationen zu eingesetzter Soft- und Hardware oder sonstigen Hochschulinterna. 	<ul style="list-style-type: none"> > Versenden Sie personenbezogene Daten nicht unverschlüsselt per E-Mail (siehe Regelungen für den Einsatz von E-Mail in der FH Aachen). > Berücksichtigen Sie bei der Verarbeitung von personenbezogenen Daten die internen Richtlinien und Vorgaben der Hochschule zur Informationssicherheit (siehe Merkblatt zur Informationssicherheit). > Sorgen Sie dafür, dass unbefugte Dritte über Ihren Arbeitsplatz keinen Zugriff auf personenbezogene Daten erlangen. > Sperren Sie Ihren PC, wenn Sie das Büro verlassen. > Halten Sie nur die Unterlagen an Ihrem Arbeitsplatz vor, die Sie gerade bearbeiten. > Am Ende des Arbeitstages schalten Sie Ihren PC aus, schließen Sie alle Unterlagen ein und verschließen Fenster und Türen Ihres Büros. > Shreddern Sie zu vernichtende Dokumente mit sensiblen Daten.

Mögliche Rechtsfolgen bei Datenschutzverstößen (abgeleitet aus der EU-Datenschutzgrundverordnung (EU-DSGVO) und dem Landesdatenschutzgesetz DSG NRW)

Artikel 83 der EU-DSGVO regelt die Bedingungen und Tatbestände für die Verhängung von Geldbußen gegen die verantwortliche Stelle bzw. gegen den Auftragsdatenverarbeiter. Im Landesdatenschutzgesetz (DSG NRW) ergänzt § 32 die Verhängung von Geldbußen gegen öffentliche Stellen.

Die EU-DSGVO enthält keine Regelungen zur Verhängung von Geldbußen gegenüber Mitarbeiterinnen und Mitarbeitern der verantwortlichen Stelle. Artikel 84 Absatz 1 DSGVO enthält aber diesbezüglich eine Öffnungsklausel, die im Landesdatenschutzgesetz (DSG NRW) berücksichtigt wird. Danach ist laut § 33 Absatz 1 des DSG NRW die Verhängung von Geldbußen auch gegen die bei der verantwortlichen Stelle beschäftigten Personen möglich. Geahndet wird in Verbindung mit § 2 und § 10 des Gesetzes über Ordnungswidrigkeiten (OWiG) nur vorsätzliches Verhalten von Beschäftigten. § 33 Absatz 2 des DSG NRW begrenzt die Höhe des Bußgeldes auf 50.000 €.

§ 34 des DSG NRW legt fest, in welchen Fällen Verstöße gegen § 33 als Straftat bewertet werden. Straftaten werden mit Freiheitsstrafen bis zu zwei Jahren oder Geldstrafen bestraft.

Ebenso sind Schadensersatzforderungen eines oder einer durch unzulässige oder unrichtige Verarbeitung zu Schaden gekommenen Betroffenen möglich (siehe § 68 DSG NRW).

> **Bei Fragen zum Datenschutz wenden Sie sich an den Datenschutzbeauftragten:**
Thomas Lex | T +49. 241. 6009 51043 | lex@fh-aachen.de

Darüber hinaus finden Sie auf der Webseite des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen LDI NRW www.lidi.nrw.de weitere Informationen zum Datenschutz und eine Fassung des aktuellen Landesdatenschutzgesetzes.

Mit der EU-DSGVO wird die Informationssicherheit elementarer Bestandteil des Datenschutzes.

> **Bei Fragen Zur Informationssicherheit wenden Sie sich an den IT- Sicherheitsbeauftragten:**
Volker Krüger | T +49. 241. 6009 51084 | krueger@fh-aachen.de

Das Merkblatt zur Informationssicherheit finden Sie unter www.fh-aachen.de/hochschule/it-sicherheit/sicherheitshinweise (Login erforderlich)

Erklärungen

1. Ich erkläre hiermit, dass ich die Datenschutzhinweise und das Merkblatt zum Datenschutz zur Kenntnis genommen und verstanden habe.
2. Ich erkläre mich damit einverstanden, dass meine Daten an die DVZ der FH Aachen übermittelt werden.
3. Mir ist bekannt, dass die Nutzung der Hochschul-IT der Netzordnung und den sonstigen hierzu ergangenen Regelungen und Anweisungen unterliegt. Ich habe mich hierüber informiert.
4. Ich bin ebenfalls damit einverstanden, dass durch den Einsatz von technischen Systemen der Hochschul-IT das Aufkommen von Schadsoftware und Werbemails (SPAM) bekämpft wird.
Mir ist bewusst, dass dadurch einzelne E-Mails markiert, blockiert oder zurückgewiesen werden können und die Nutzung eines mit Schadsoftware infizierten Endgerätes (z. B.: Notebook, Tablet, Smartphone) unterbunden werden kann.

Mir wurde eine Ausfertigung dieser Erklärung ausgehändigt.

Unterschrift Aachen, am