Anlage 1: Merkblatt zur Belehrung zur Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten

Datenschutz schützt das Persönlichkeitsrecht

Ihre Belehrung zur Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten dient – wie das gesamte Datenschutzrecht – dem Schutz des Persönlichkeitsrechts derjenigen Menschen, auf die sich die Daten beziehen. Diese Menschen nennt das Gesetz „betroffene Personen". Das können unsere Studierenden sein, Ihre Kolleginnen und Kollegen – oder auch Sie als unser/e Mitarbeiter/in.
Das Persönlichkeitsrecht gibt jedem Menschen das Recht, grundsätzlich selbst darüber zu entscheiden, wer was über ihn wissen darf. So dürfen Sie beispielsweise entscheiden, wer Ihren Gesundheitszustand kennen darf. Es ist Ihre Entscheidung, ob das geheim bleibt oder Sie jemandem, wie z.B. Ihrem behandelnden Arzt, dazu Informationen geben.

Jede Verarbeitung personenbezogener Daten ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung und darf nur auf der Basis einer Rechtsvorschrift oder mit Einwilligung des Betroffenen erfolgen. Der/die Beschäftigte muss deshalb bevor er/sie Daten verarbeitet (z. B. erhebt, speichert, übermittelt oder nutzt) immer prüfen, aufgrund welcher Rechtsnorm er/sie handelt. Die betroffene Person hat einen Anspruch darauf, dass mit ihren personenbezogenen Daten sorgsam umgegangen wird.

Ihre Vertraulichkeitspflichten

Sie müssen personenbezogene Daten nicht nur vertraulich behandeln, d.h. Sie dürfen sie zum Beispiel nicht an Dritte weitergeben oder offen herumliegen lassen, so dass andere, unberechtigte Personen sie einsehen können, sondern das Gesetz verpflichtet Sie vielmehr auch dazu, nur dann mit personenbezogenen Daten zu arbeiten, wenn dies erlaubt ist – unabhängig davon, ob Sie diese Daten beispielsweise lesen, notieren, löschen oder weitergeben. Diese Erlaubnis muss einerseits die Bauhaus-Universität als Organisation und Arbeitgeber haben, andererseits aber auch Sie persönlich nach unserem Geschäftsverteilungsplan bzw. Ihrer Tätigkeitsdarstellung.

Die gesetzlichen Vertraulichkeitspflichten einzuhalten, ist also auch Ihre ganz persönliche Verpflichtung. Diese Pflicht ergibt sich übrigens bereits aus dem Gesetz (unter anderem § 49 ThürDSG und Art. 29 DS-GVO). Ihre heutige förmliche Belehrung zur Vertraulichkeit dient dazu, Ihnen deutlich zu machen, wie wichtig diese Pflicht ist.

Bitte beachten Sie: Ihre Pflicht zur Wahrung der Vertraulichkeit gilt zeitlich unbefristet, und zwar selbst dann, wenn Sie nicht mehr für uns tätig sind. Sie gilt gegenüber allen Personen, die nicht dienstlich für die jeweilige Sache zuständig sind – also auch gegenüber allen anderen Kolleginnen und Kollegen, Ihrer Familie und der Presse.

Der Begriff „personenbezogene Daten"

Das Datenschutzrecht gilt für alle „personenbezogenen Daten". Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, also einen Menschen, beziehen (Art. 4 Nr. 1 DS-GVO). Das kann die Angabe sein, dass jemand Mitglied in einem Verein ist, wo jemand wohnt oder welche persönliche E-Mail-Adresse jemand hat.

Auch wenn Sie selbst denken, dass bestimmte Daten niemandem zuzuordnen sind, dürfen Sie diese nicht ohne Zustimmung Ihrer/s Vorgesetzten an Dritte weitergeben oder veröffentlichen – abgesehen davon, dass es sich auch um Betriebsgeheimnisse handeln könnte, die Sie ebenfalls streng vertraulich behandeln müssen.

Für welche Daten das Datenschutzrecht gilt

Das Datenschutzrecht gilt für digital und analog vorgehaltene Daten. Es gilt somit auch für „die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen" (Art. 2 Abs. 1 DS-GVO). Wobei unter einem Dateisystem jede geordnete Ablage zu verstehen ist (Art. 4 Nr. 6 DS-GVO) – etwa eine alphabetische Sammlung ausgefüllter Formulare. Das Datenschutzrecht gilt zudem auch dann, wenn die Daten später in eine Datei gespeichert werden sollen oder aus einer Datei stammen – etwa eine ausgedruckte Liste mit Beschäftigtendaten.

Unsere und Ihre Pflichten

Wir als Organisation und Sie als unser/e Beschäftigte/r dürfen personenbezogene Daten nur dann verarbeiten, wenn es dafür eine Rechtsgrundlage gibt. Art. 4 Nr. 2 DS-GVO beschreibt den Begriff der Verarbeitung äußerst weit, so dass er letztlich jeden Kontakt mit personenbezogenen Daten umfasst: „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche 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".

Wann bzw. unter welchen Umständen die Verarbeitung personenbezogener Daten zulässig ist, ist in Art. 6 Abs. 1 der DS-GVO festgelegt. Personenbezogene Daten dürfen demnach nur verarbeitet werden, wenn

a) eine Einwilligung vorliegt;
b) die Erforderlichkeit zur Erfüllung von Verträgen oder vorvertraglichen Verpflichtungen besteht;
c) die Erfüllung einer gesetzlichen Verpflichtung dies erfordert;
d) sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder von Dritten erforderlich ist;
e) sie zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt;
f) sie zur Wahrnehmung berechtigter Interessen des Verantwortlichen oder von Dritten erforderlich ist, sofern nicht die Interessen der betroffenen Person am Schutz ihrer personenbezogenen Daten überwiegen (Interessensabwägung).

Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
e) 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;

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Als wichtigste Regel sollten Sie sich hier merken, dass Sie personenbezogene Daten nie aus eigener Entscheidung heraus weitergeben oder für sich selbst nutzen dürfen.

Außerdem müssen personenbezogene Daten geschützt werden, so dass Unbefugte keine Kenntnis von ihnen nehmen, sie nicht manipuliert werden und auch nicht versehentlich verloren gehen können. Hierfür werden – wie durch die DS-GVO gefordert - vielfältige technische und organisatorische Maßnahmen ergriffen. So müssen beispielsweise personenbezogene Daten verschlüsselt werden, wenn sie über das Internet übertragen werden sollen. Dem Verlust gespeicherter Daten wird durch die regelmäßige Erstellung von Sicherungskopien (Backups) entgegengewirkt. Ausdrucke mit personenbezogenen Daten oder Datenträger wie CDs, USB-Sticks oder Festplatten mit personenbezogenen Daten dürfen keinesfalls einfach weggeworfen oder weggegeben werden, sondern müssen ordnungsgemäß vernichtet werden. Einzelheiten finden Sie in der Richtlinie zur Entsorgung, Veräußerung Ausgabe und Weitergabe von Datenträgern und IT-Geräten an der Bauhaus-Universität Weimar:
https://www.uni-weimar.de/fileadmin/user/uni/universitaetsleitung/kanzler/mdu/08/27_2008.pdf

Dass Sie Ihr Passwort nicht an Kolleginnen und Kollegen oder an Dritte weitergeben oder gar auf einem Zettel an den Computer kleben dürfen, sollte sich von selbst verstehen – es ist Ihr persönliches Passwort, und wenn es jemand missbraucht, sind Sie persönlich dafür verantwortlich (siehe „Folgen von Verstößen"). Es ist aber zusätzlich auch eine Forderung der an der Bauhaus-Universität Weimar verbindlichen Passwortregeln:
https://www.uni-weimar.de/de/universitaet/struktur/zentrale-einrichtungen/scc-rechenzentrum/it-sicherheit/passwort/

Weitere an der Bauhaus-Universität Weimar verbindliche Regelungen, die den Datenschutz insbesondere bei der IT-Nutzung, berühren sind:

- IT-Sicherheitsordnung für die Hochschule für Musik FRANZ LISZT Weimar und die Bauhaus-Universität Weimar (zukünftig Gemeinsame IT-Sicherheits-Leitlinie der Bauhaus-Universität Weimar sowie der Hochschule für Musik FRANZ LISZT Weimar):
  https://www.uni-weimar.de/fileadmin/_migrated/content_uploads/10_2005_01.pdf
- IT-Grundschutz für die Bauhaus-Universität Weimar und die Hochschule für Musik FRANZ LISZT Weimar:
  https://www.uni-weimar.de/fileadmin/_migrated/content_uploads/Grundschutz_bu_weimar_v1_1.pdf
- Ordnung für die Nutzung der Infrastruktur der Informationsverarbeitung der Bauhaus-Universität Weimar (zukünftig Gemeinsame IT-Nutzungsordnung der Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT Weimar):
  https://www.uni-weimar.de/fileadmin/user/uni/zentrale_einrichtungen/scc/regelungen/nutzungsordnung.pdf
- Richtlinie für die dienstliche Nutzung externer IT-Services:
  http://www.uni-weimar.de/fileadmin/user/uni/universitaetsleitung/kanzler/mdu_akad/14/28_2014.pdf
- Dienstanweisung zur Einhaltung der technischen und organisatorischen Maßnahmen laut IT-Sicherheitskonzept - Dezentrale Komponenten der Bauhaus-Universität Weimar für das ThüringerERP

Rechte der betroffenen Personen

Einer der wichtigsten Aspekte des Persönlichkeitsrechts ist es, zu wissen, was andere über einen wissen. Wenn eine Organisation Daten über jemanden sammelt, muss sie daher fast

immer die betroffene Person informieren (Art. 13 DS-GVO). Jeder Mensch kann zudem von jeder Organisation eine Kopie der Daten verlangen, die die Organisation über ihn/sie gespeichert hat (Art. 15 DS-GVO). Das Auskunftsrecht ist ein spezielles Recht des/der Betroffenen: An andere Personen und Stellen dürfen wir normalerweise keine Auskünfte geben – das wäre eine Übermittlung, für die wir eine Erlaubnis bräuchten.

Benötigen wir bestimmte Daten nicht mehr, müssen wir sie löschen (Art. 17 DS-GVO); falsche Daten müssen wir berichtigen (Art. 16 DS-GVO). Wenn Sie feststellen, dass nicht mehr benötigte Daten weiterhin gespeichert bleiben, sprechen Sie bitte Ihre/n Vorgesetzten oder den betrieblichen Datenschutzbeauftragten darauf an.

Sollte ein Auskunftsersuchen, ein Widerspruch oder ein anderer Wunsch oder Hinweis mit Datenschutzbezug bei Ihnen eingehen, so informieren Sie bitte Ihren Vorgesetzten und den betrieblichen Datenschutzbeauftragten. Selbstständig dürfen Sie solche Dinge nur bearbeiten, wenn wir Ihnen diese Aufgabe ausdrücklich zugewiesen haben. In Zweifelsfällen fragen Sie den betrieblichen Datenschutzbeauftragten. Beachten Sie bitte, dass auch Behörden oder die Polizei nicht ohne Weiteres Daten von uns erhalten können. Wir benötigen hier einen förmlichen Beschlagnahmebeschluss oder, in bestimmten Fällen, ein förmliches Auskunftsersuchen. Wenn Sie von der Polizei oder einer anderen Behörde kontaktiert werden, informieren Sie bitte sofort Ihre/n Vorgesetzte/n und den betrieblichen Datenschutzbeauftragten.

Folgen von Verstößen

Verstöße gegen das Datenschutzrecht können als Ordnungswidrigkeit oder als Straftat geahndet werden. Geben Sie beispielsweise ohne eine entsprechende Anweisung personenbezogene Daten weiter oder nutzen Sie sie für Ihre eigenen Zwecke, können Sie persönlich mit einer Geldbuße bis zu 50.000 EUR (§ 61 ThürDSG) belegt werden.

Verstöße gegen das Datenschutzrecht können zudem nach anderen Gesetzen strafbar sein, z. B. nach § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen), § 202 a StGB (Ausspähen von Daten) oder § 263 a StGB (Computerbetrug).

Jede betroffene Person kann Schadensersatz für eine unzulässige Verarbeitung ihrer Daten verlangen, und zwar einschließlich Schmerzensgeld für die Persönlichkeitsrechtsverletzung (Art. 82 DS-GVO, §§ 823 ff. BGB). Unter Umständen müssen Sie persönlich diesen Schadensersatz ganz oder teilweise bezahlen, wenn Sie mittlere oder schwere Verstöße begangen oder personenbezogene Daten weisungswidrig verarbeitet haben, etwa für Ihre eigenen Zwecke genutzt haben. Fragen Sie daher lieber einmal zu viel als zu wenig.

Schwere Schäden für die Organisation kann es verursachen, wenn eine so genannte Datenpanne öffentlich bekannt wird. Nach Art. 34 Abs. 1 und Abs. 3 lit. c DS-GVO können wir verpflichtet sein, eine Datenpanne allen Betroffenen mitzuteilen oder gar öffentlich bekanntzumachen. Bitte helfen Sie mit, dass es niemals dazu kommt.

Unabhängig davon kann ein Verstoß auch zu dienst- oder arbeitsrechtlichen Konsequenzen führen.

Neue Verfahren mit personenbezogenen Daten

Sie sind an einem Projekt beteiligt, bei dem personenbezogene Daten eine Rolle spielen? Dann sorgen Sie bitte dafür, dass der betriebliche Datenschutzbeauftragte von Anfang an einbezogen wird. Er kann Ihnen sagen, ob es überhaupt rechtlich möglich ist, was Ihr Projektteam plant, und Tipps geben, was Sie verbessern könnten, insbesondere, welche Anforderungen wir zu „Privacy by Design“ und „Privacy by Default“ (Art. 25 DS-GVO) oder zur Sicherheit (Art. 32 DS-GVO) einhalten müssen. Wenn Sie diese Fragen rechtzeitig mit dem

betrieblichen Datenschutzbeauftragten klären, können Sie von Anfang an das richtige Verfahren entwickeln. Wenn Sie ihn erst kurz vor Schluss einbeziehen, kann es sein, dass Ihr Projekt komplett scheitert, weil es rechtlich nicht oder nur unter aufwendigen Änderungen umzusetzen ist.

Wichtig ist, dass wir jederzeit beweisen können, dass wir das Gesetz vollständig einhalten (Art. 5 und 24 DS-GVO). Können wir diesen Nachweis nicht vollständig erbringen, haften wir auf Schadensersatz und Geldbußen – auch Sie persönlich, wenn Sie das Verfahren ohne Genehmigung eingeführt haben.

Besondere Hinweise für Nutzer von E-Mail und Online-Diensten

Das Internet und die E-Mail-Kommunikation sind in datenschutzrechtlicher Hinsicht unsichere Kommunikationsmittel. Beachten Sie deshalb bitte folgende Grundregeln:

Vertrauliche Daten – insbesondere auch personenbezogene Daten – dürfen Sie niemals per normaler (unverschlüsselter) E-Mail versenden. Wenden Sie sich an das SCC, wenn Sie regelmäßig vertrauliche Daten per Mail versenden müssen. Bitte prüfen Sie aber in jedem Fall vorher, ob Sie die Daten überhaupt an den/die Empfänger/in weitergeben dürfen!

Bevor Sie eine E-Mail versenden, achten Sie bitte unbedingt darauf, ob der/die richtige Empfänger/in im Adressfeld steht. Hier liegt eine große Fehlerquelle, wenn mehrere Personen einen ähnlichen Namen oder eine ähnliche E-Mail-Adresse haben und das E-Mail-Programm bei der Eingabe automatisch nach dem/r potentiellen Empfänger/in sucht. Prüfen Sie die Korrektheit des/r Empfängers/in vor dem Versenden bitte noch einmal. Durch unbeabsichtigte Verwechselungen sind schon mehrfach vertrauliche Informationen an die Öffentlichkeit gelangt.

Beachten Sie den Unterschied zwischen „To:/An:" (Empfänger), „CC:" (Kopie) und „BCC:" (Blindkopie): Alle, die im To:- bzw. CC:-Feld stehen, sind für sämtliche anderen Empfänger/innen sichtbar. Soll jemand für die anderen nicht sichtbar sein, müssen Sie ihn/sie ins BCC:-Feld schreiben. Die Daten aller To:-/CC:-Empfänger/innen übermitteln Sie im rechtlichen Sinne an die anderen Empfänger/innen. Und dafür benötigen Sie eine Erlaubnis. Wenn Sie Nachrichten an viele Empfänger/innen senden müssen, sprechen Sie deshalb bitte mit dem SCC, ob dafür eine Mailing-Liste o. ä. eingerichtet werden sollte, oder ob die Versendung über das BCC:-Feld ausreichend ist. Es wurden bereits Bußgelder gegen Mitarbeiter/innen verhängt, die alle Empfänger/innen ins To:-Feld geschrieben haben!

Sie dürfen niemals vertrauliche Daten an Ihren privaten E-Mail-Account weiterleiten oder eine automatische Weiterleitung Ihres E-Mail-Accounts an der Bauhaus-Universität Weimar an Ihre private E-Mail-Adresse einrichten. Daten müssen immer innerhalb der Bauhaus-Universität Weimar gespeichert werden, also keinesfalls bei einem der zahlreichen Public-Cloud-Angebote (Amazon, Google, Microsoft, …).

Beim Empfang von E-Mails sollten Sie immer skeptisch sein und niemals leichtfertig externen Links folgen oder Anhänge öffnen. Immer wieder erhalten Beschäftigte E-Mails, die vermeintlich von Stellen oder Beschäftigten der Bauhaus-Universität Weimar stammen und sie auffordern auf einen externen Link zu klicken, einen Anhang zu öffnen oder personenbezogene Daten Preis zu geben. Hierbei handelt es sich in der Regel um eine Fälschung. Das Ziel ist meist entweder personenbezogene oder andere sensible Daten zu stehlen (Phishing) oder ihr System mit Schadsoftware zu infizieren. Bitte beachten Sie unsere Hinweise auf der SCC-Webseite:
https://www.uni-weimar.de/de/universitaet/struktur/zentrale-einrichtungen/scc-rechenzentrum/it-sicherheit/phishing/ .

Warnungen zu aktuell an der Bauhaus-Universität Weimar kursierenden Phishing- oder anderen gefährlichen E-Mails veröffentlichen wir auf der Pinnwand des SCC: https://www.uni-

weimar.de/de/universitaet/aktuell/pinnwaende/bereich/scc/) oder der SCC Webseite im Bereich IT-Sicherheit: https://www.uni-weimar.de/de/universitaet/struktur/zentrale-einrichtungen/scc-rechenzentrum/it-sicherheit/aktuell/.

Leiten Sie derartige E-Mails möglichst mit komplettem E-Mail-Header (Hilfestellung bei der Uni Paderborn: https://hilfe.uni-paderborn.de/Mail_Header_anzeigen) bitte immer sofort über die SCC-Hotline – hotline@scc.uni-weimar.de an den IT-Sicherheitsbeauftragten der Bauhaus-Universität Weimar weiter.

Bitte beachten Sie, dass der anzeigte Absendername und die Absenderadresse einer E-Mail keinerlei Verlässlichkeit besitzen und leicht zu fälschen sind, ohne dass dafür tatsächlich ein E-Mail-Account kompromittiert werden muss. Ein/e Absender/in lässt sich nur zweifelsfrei verifizieren, wenn er/sie eine digitale Signatur verwendet. Eine signierte E-Mail bietet zudem die Gewähr, dass der Inhalt seit dem Versenden nicht modifiziert wurde. Das SCC bietet die Möglichkeit der Generierung von Nutzerzertifikaten für die Erstellung digitaler Signaturen:
https://www.uni-weimar.de/de/universitaet/struktur/zentrale-einrichtungen/scc-rechenzentrum/it-sicherheit/sicherheitszertifikate-pki/.

Auf zentral bereit gestellten IT-Systemen sind vielfältige Sicherheitsmaßnahmen aktiviert und wurden Einstellungen zur Gewährleistung des Datenschutzes vorgenommen. Bitte ändern Sie diese Einstellungen nicht eigenmächtig, sondern halten Sie immer Rücksprache mit Ihren IT-Betreuer/inne/n: https://www.uni-weimar.de/de/universitaet/struktur/zentrale-einrichtungen/scc-rechenzentrum/service/it-ansprechpartner/.
Wenn Sie Änderungsvorschläge haben, sprechen Sie diese bitte an.

Bitte beachten Sie bei der Nutzung von externen Online-Diensten die Richtlinie für die dienstliche Nutzung externer IT-Services: http://www.uni-weimar.de/fileadmin/user/uni/universitaetsleitung/kanzler/mdu_akad/14/28_2014.pdf

Sollten Sie Fragen haben, insbesondere wenn es darum geht, ob ein bestimmter Umgang mit personenbezogenen Daten erlaubt ist, zögern Sie nicht, Ihre/n Vorgesetzte/n oder den betrieblichen Datenschutzbeauftragten, Herrn Jens-Uwe Wagner (Tel. 58-1222, datenschutz@uni-weimar.de) zu fragen.