Richtlinie
der Pädagogischen Hochschule Weingarten

Az. 0550 20. Februar 2019

Datenschutzrichtlinie für den Umgang mit personenbezogenen Daten der Pädagogischen Hochschule Weingarten

vom 20. Februar 2019

Präambel

Die in der Hochschule vorhandenen Daten sind für die Sicherstellung von reibungslosen internen und externen Abläufe von großem Wert. Diese Daten sind daher gegen unbefugte Zugriffe und andere Gefährdungen zu schützen. Gleichzeitig erwarten die Studierenden, Beschäftigten und Partner der Hochschule, dass die der Einrichtung anvertrauten Daten besonders geschützt werden und ein sorgsamer Umgang mit ihnen erfolgt. Die verantwortliche Stelle bekennt sich auch im Rahmen ihres gesellschaftlichen Engagements zu ihrer Verantwortung für den sorgsamen Umgang mit personenbezogenen Daten.

Die Datenschutzrichtlinie gilt für alle Mitglieder und Angehörigen der Hochschule und muss daher für diese jederzeit leicht zugänglich sein.

Allgemeines

§ 1 Ziel der Datenschutzrichtlinie

Mit dieser Datenschutzrichtlinie sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden. Mit dieser Richtlinie sollen zudem einheitliche Standards für den Datenschutz in der Hochschule geschaffen werden. Die Richtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten in der verantwortlichen Stelle.

§ 2 Anwendungsbereich der Datenschutzrichtlinie

Diese Datenschutzrichtlinie gilt für jegliche Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten einschließlich der Weitergabe innerhalb der Institution sowie die Übermittlung an Dritte. Sie regelt umfassend alle datenschutzrechtlichen Aspekte, die sich im Rahmen der Datenverarbeitung ergeben können. Sie findet Anwendung auf sämtliche Arten von personenbezogenen Daten, insbesondere Daten von Mitgliedern und Angehörigen, Lieferanten und Partnern der Hochschule. Die Herkunft der Daten ist für die Anwendbarkeit dieser Richtlinie nicht maßgeblich; entscheidend ist die Verwendung der Daten in der Hochschule. Bestehende gesetzliche Verpflichtungen werden von dieser Datenschutzrichtlinie nicht berührt und sind somit zu erfüllen. Es ist daher stets zu prüfen, welche gesetzlichen Regelungen einschlägig sind; deren Beachtung ist sicherzustellen. Sofern sich aus den gesetzlichen Bestimmungen geringere Anforderungen ergeben, gelten die Regelungen dieser Datenschutzrichtlinie.

§ 3 Definitionen

(1) Personenbezogene Daten im Sinne dieser Datenschutzrichtlinie und im Sinne des Gesetzes sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Daten, die ausschließlich Informationen über juristische Personen beinhalten, sind keine personenbezogenen Daten. Auch diese Daten sollen gleichermaßen geschützt werden. Für besonders schutzbedürftige Daten gelten erhöhte Sorgfaltsanforderungen. Welche personenbezogenen Daten besonders schutzbedürftig sind, ergibt sich dabei aus Artikel 9 Absatz 1 DSGVO (Verordnung (EU) 2016/679). Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder

der sexuellen Orientierung einer natürlichen Person.

(2) Betroffene sind die identifizierten oder identifizierbaren natürlichen Personen, deren personenbezogene Daten in bzw. von der Hochschule verarbeitet werden.

(3) Dritter ist jede Stelle außerhalb der Hochschule. Einzelne Stellen oder Abteilungen innerhalb der verantwortlichen Stelle sind nicht Dritte. Gleichwohl ist auch innerhalb der Einrichtung zu prüfen, inwieweit personenbezogene Datenstellen intern zur Verfügung gestellt werden müssen. Dienstleister und Partner, mit denen eine Vereinbarung zur Auftragsdatenverarbeitung besteht, gelten ebenfalls nicht als Dritte, da diese unter der Verantwortung der Hochschule tätig werden.

(4) Verarbeitung stellt 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.

(5) 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;

(6) Verantwortliche Stelle ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dies ist innerhalb der Hochschule die juristische Person, einschließlich sämtlicher Untergliederungen und unselbständiger Zweigstellen, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt.

(7) Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Grundsätze der Datenverarbeitung

§ 4 Zulässigkeit der Datenverarbeitung

(1) Bei jedem Vorgang der Datenverarbeitung ist zu prüfen, ob die beabsichtigte Verarbeitung von Daten zulässig ist. Bestehen Zweifel an der Zulässigkeit, muss die oder der Datenschutzbeauftragte kontaktiert werden.

(2) Die Zulässigkeit der Datenverarbeitung kann sich aus verschiedenen Gesichtspunkten ergeben. Für Hochschulen ergibt sich diese grundsätzlich aus der gesetzlichen Ermächtigungsgrundlage in § 4 LDSG. Weitere Ermächtigungsgrundlagen können sich aus Artikel 6 Absatz 1 DSGVO (Verordnung (EU) 2016/679) ergeben.

§ 5 Gesetzliche Ermächtigungsgrundlagen

(1) Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen gemäß Art. 6 Abs. 1 e) EU-DSGVO (EU-Datenschutzgrundverordnung) in Verbindung mit Art. 6 Abs. 3 DS-GVO und § 4 LDSG (Landesdatenschutzgesetz Baden-Württemberg in der ab 21.06.2018 geltenden Fassung) und § 12 LHG BW (Landeshochschulgesetz Baden-Württemberg in der ab dem 30.3.2018 geltenden Fassung) sowie weiteren Spezialgesetzen wie der HSchulDSV BW (Hochschul-Datenschutzverordnung des Landes Baden-Württemberg) zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der Pädagogischen Hochschule als öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der Pädagogischen Hochschule als öffentlichen Stelle übertragen wurde, erforderlich ist.

(2) Zulässig ist die Verarbeitung zudem, wenn der oder die Betroffene in die Verarbeitung der sie oder ihn betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt hat.

(3) Die Verarbeitung personenbezogener Daten kann erforderlich sein für die Begründung, Durchführung oder Beendigung eines Vertrags mit der

oder dem Betroffenen (bspw. Immatrikulation/Exmatrikulation etc.).

(4) Eine Notwendigkeit und Ermächtigung zur Datenverarbeitung kann sich ergeben aufgrund einer gesetzlichen Verpflichtung der Hochschule oder einer verbindlichen behördlichen Entscheidung, bspw. einem Auskunftsersuchen von Ermittlungsbehörden.

(5) Zulässig ist die Verarbeitung personenbezogener Daten auch, wenn sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich ist. Gleiches gilt für die Wahrung lebenswichtiger Interessen der oder des Betroffenen selbst.

(6) Denkbar ist eine Datenverarbeitung schließlich in den Fällen, bei denen ein öffentliches Interesse der Hochschule besteht und gleichzeitig kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der oder des Betroffenen an dem Ausschluss der Datenverarbeitung überwiegt. Das Ergebnis einer solchen Interessenabwägung soll dabei schriftlich protokolliert werden.

§ 6 Umgang mit personenbezogenen Daten

(1) Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn eine gesetzliche Norm erlaubt explizit den Datenumgang.
Personenbezogene Daten dürfen nach dem LDSG grundsätzlich verarbeitet werden, wenn:

- sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.

- eine weitere Rechtsgrundlage aus Art. 6 Absatz 1 DSGVO (Verordnung (EU) 2016/679) vorliegt, wie

    - indem der oder die Betroffene eingewilligt hat. Beispiel: Betroffene melden sich zum Erhalt eines Newsletters an. Studierende geben personenbezogene Daten im Zuge einer Studierendenbefragung an.

    - indem die Daten zur Erfüllung der Pflichten aus einem bestehenden Vertragsverhältnis mit der oder dem Betroffenen verarbeitet werden. Beispiele: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen von Beschäftigungsverhältnissen oder während Studierende an der Hochschule eingeschrieben sind.

    - im Zuge der Vertragsanbahnung oder Vertragsabwicklung mit Betroffenen bzw. der anstehenden Immatrikulation/Exmatrikulation von Studierenden.

    - Wenn eine spezielle Rechtsvorschrift außerhalb des LDSG die eine rechtliche Pflicht zu Verarbeitung vorschreibt. Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch oder Abgabenordnung.

(2) Personenbezogene Daten sind für einen zuvor festgelegten Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit dem ursprünglich festgelegten Zweck vereinbar ist.
Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist unbeschadet der Bestimmungen der DSGVO (Verordnung [EU] 2016/679) gemäß § 5 Absatz1 LDSG zulässig, wenn

- sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,

- sie zum Schutz der betroffenen Person oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist,

- sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung ergeben und die Unterrichtung der für die Verhütung, Verfolgung oder Vollstreckung zuständigen Behörden erforderlich ist oder

- Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

soweit die Verarbeitung notwendig und verhältnismäßig ist.

(3) Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist ebenfalls nur mit einer gesetzlichen Erlaubnisnorm oder der Einwilligung der oder des Betroffenen zulässig.

(4) Personenbezogene Daten sollen grundsätzlich direkt bei der oder dem Betroffenen erhoben werden. Eine Erhebung aus anderen Quellen (Internet, Warndienste, Auskunfteien) ist ohne ein zwingendes gesetzliches Erfordernis unzulässig. Besteht ein gesetzliches Erfordernis, ist die oder der Betroffene unverzüglich über die Datenerhebung zu informieren, soweit eine gesetzliche Regelung dem nicht entgegensteht.

(5) Die oder der Betroffene ist bei der Erhebung seiner personenbezogenen Daten über die Zweckbestimmung, die Identität der verantwortlichen Stelle sowie die Empfänger ihrer oder seiner personenbezogenen Daten zu informieren.

(6) Personenbezogene Daten müssen sachlich richtig und, wenn möglich, auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die Hochschulleitung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

(7) Falls möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen. Beispielsweise muss es im Rahmen einer statistischen Auswertung von Daten nicht erforderlich sein, den Vollnamen einer oder eines Studierenden zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrundeliegenden Information ebenfalls gewährleisten kann.

(8) Besondere personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung der oder des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

(9) Personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke dürfen von der Hochschule verarbeitet werden, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Interessen der Hochschule an der Durchführung des Forschungs- oder Statistikvorhabens die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. Auch zu diesen Zwecken sind die Daten soweit möglich zu anonymisieren. Diese Daten dürfen außer bei Einwilligung des oder der Betroffenen nur veröffentlicht werden, soweit dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist. Die Rechte des oder der Betroffenen sind in diesen Fällen nach § 13 Absatz 4 LDSG beschränkt.

(10) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Die Rechte der oder des Betroffenen sind hierbei entsprechend der Regelungen in § 14 Absatz 2 bis 4 LDSG beschränkt und die Löschung dieser Daten nach § 14 Absatz 5 LDSG.

§ 7 Einwilligung und Protokollierung

(1) Eine Einwilligung der oder des Betroffenen ist als Grundlage für die Datenverarbeitung ausreichend, wenn die oder der Betroffene zuvor ausreichend informiert wurde und seine Einwilligung anschließend freiwillig erteilt hat.

(2) Von einer ausreichenden Information ist auszugehen, wenn die wesentlichen Abläufe der Datenverarbeitung erläutert werden und insbesondere erklärt wird, zu welchem Zweck die Daten erhoben, gespeichert und verwendet werden. Die oder der Betroffene muss darauf hingewiesen werden, dass ihre oder seine Einwilligung frei widerruflich ist. Außerdem ist darauf zu achten, dass Einwilligungserklärungen gegenüber anderen Erklärungen optisch hervorgehoben werden und in einer verständlichen und leicht zugänglichen Form und in klarer und einfacher Sprache formuliert werden.

(3) Eine Einwilligung kann nur dann freiwillig abgegeben werden, wenn die oder der Betroffene im Falle einer Verweigerung der Einwilligung keine Nachteile zu befürchten hat. Wird die Inanspruchnahme oder Erbringung von Leistungen von einer

Einwilligung abhängig gemacht, ist die erteilte Einwilligung regelmäßig dann freiwillig, wenn sie der Vertragsbegründung oder Vertragserfüllung dient und wenn die Inanspruchnahme dieser Leistungen auch in anderer zumutbarer Weise möglich wäre.

(4) Die Einwilligungserklärung der oder des Betroffenen in schriftlicher oder elektronischer Form eingeholt werden. Die entsprechenden Einwilligungserklärungen sind für den Fall einer späteren Überprüfung zu protokollieren.

(5) Bei einer schriftlich erteilten Einwilligung kann es zulässig sein, die Erklärung einzuscannen und das Original anschließend zu vernichten.

(6) Sofern eine Einwilligung online eingeholt wird, ist darauf zu achten, dass eine Überprüfung erfolgt, bspw. über ein Double-Opt-in-Verfahren.

(7) Eine von Betroffenen erteilte Einwilligung in die Verarbeitung von Daten ist jederzeit frei widerruflich. Die oder der Betroffene ist auf die Möglich-keit des Widerrufs hinzuweisen. Der Widerruf gilt mit Wirkung für die Zukunft.

§ 8 Zweckbindung

(1) Personenbezogene Daten dürfen nur für den Zweck gespeichert und verarbeitet werden, für den sie ursprünglich erhoben wurden. Bei Einholung einer Einwilligung von der oder dem Betroffenen ist auf den konkreten Zweck hinzuweisen. Es muss sich stets um einen rechtmäßigen Zweck der Datenverarbeitung handeln.

(2) Eine Datenverarbeitung zu einem anderen Zweck soll nur in den Fällen des § 5 LDSG erfolgen und dann muss auch hierfür eine Einwilligung eingeholt werden oder einer der aufgeführten Gründe aus § 5 Absatz 1 Nummer 1 bis 4 vorliegen und die Verarbeitung notwendig und verhältnismäßig sein.

§ 9 Verhältnismäßigkeit

(1) Bei der Verarbeitung personenbezogener Daten ist der Grundsatz der Verhältnismäßigkeit zu beachten. Der Grundsatz der Verhältnismäßigkeit ist beachtet, wenn die Datenverarbeitung dazu geeignet ist, einen legitimen Zweck zu erreichen. Weiter darf kein milderes, gleichermaßen geeignetes Mittel zur Erreichung des vorgesehenen Zwecks zur Verfügung stehen. Schließlich ist zu prüfen, ob der Datenverarbeitung keine überwiegenden schutzwürdigen Interessen der oder dem Betroffenen entgegenstehen.

(2) Als milderes Mittel kann bspw. die Verarbeitung von aggregierten Daten oder sonstigen Daten ohne Personenbezug in Betracht kommen.

(3) Bei der Prüfung der Verhältnismäßigkeit kann insbesondere der Ursprung der personenbezogenen Daten (geschäftlich, privat oder intim) zu berücksichtigen sein. Weiter ist das mit der Datenverarbeitung verbundene Risiko einer Beeinträchtigung von Persönlichkeitsrechten abzuschätzen.

§ 10 Datenvermeidung und Datensparsamkeit

(1) Die Datenverarbeitung in der Hochschule ist so zu organisieren, dass so wenig personenbezogene Daten wie möglich verarbeitet werden. Wenn personenbezogene Daten nicht mehr benötigt werden, müssen diese gelöscht werden.

(2) Für die in der Hochschule gespeicherten Daten ist festzulegen, für welchen Zeitraum eine Aufbewahrung bzw. Speicherung zu erfolgen hat. Gesetzliche Aufbewahrungspflichten sind hierbei zu beachten. Nach Ablauf der Aufbewahrungsfrist bzw. Speicherdauer ist für eine Löschung der Daten zu sorgen, idealerweise durch ein automatisiertes Verfahren.

(3) Im Rahmen der Datenverarbeitung ist immer zu überprüfen, ob es zur Erfüllung der vorgesehenen Zwecke ausreichend ist, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren. Bei entsprechenden Maßnahmen ist darauf zu achten, dass bei den entsprechend bearbeiteten Daten für die Empfängerin oder den Empfänger der Daten kein Personenbezug mehr hergestellt werden kann, jedenfalls nicht mit verhältnismäßigem Aufwand.

(4) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern („Privacy by design“).

§ 11 Direkterhebung und Information von Betroffenen

(1) Personenbezogene Daten sind grundsätzlich bei der oder dem Betroffenen mit ihrer oder seiner Kenntnis direkt zu erheben. Eine Erhebung bei Dritten ist nur dann zulässig, wenn dies gesetzlich vorgesehen ist, das Vorgehen im Interesse der oder des Betroffenen ist oder eine Direkterhebung nur mit unverhältnismäßigem Aufwand möglich wäre.

(2) Die oder der Betroffene ist grundsätzlich umfänglich gemäß Artikel 13 und 14 DSGVO (Verordnung [EU] 2016/679) darüber zu informieren, wenn personenbezogene Daten über sie oder ihn verarbeitet werden. Eine gesonderte Information kann unterbleiben, wenn ihr oder ihm die Datenverarbeitung bekannt ist. Hiervon ist bspw. auszugehen, wenn eine Einwilligung der oder des Betroffenen eingeholt wurde und die oder der Betroffene in diesem Zusammenhang vorab informiert wurde.

(3) Die Informationspflichten der Hochschule sind gemäß § 8 LDSG in den dort genannten Fällen eingeschränkt. Dies ist der Fall, wenn:

- die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
- die Information die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung gefährden würde,
- die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde,
- die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte und Freiheiten anderer Personen geheim gehalten werden müssen oder
- die Information voraussichtlich die Verwirklichung des wissenschaftlichen oder historischen Forschungszwecks unmöglich macht oder ernsthaft beeinträchtigt

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

§ 12 Datenqualität

(1) Alle Beschäftigten haben darauf zu achten, dass personenbezogene Daten richtig sind und auf dem neuesten Stand gehalten werden.

(2) Unzutreffende oder unvollständige Daten müssen berichtigt oder gelöscht werden.

§ 13 Datensicherheit

(1) Für die Hochschule ist von großer Bedeutung, dass die Sicherheit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind die Daten u.a. ausreichend gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren zu schützen.

(2) Es ist daher dafür zu sorgen, dass angemessene Maßnahmen getroffen werden, um personenbezogene Daten zu schützen. Der Schutz hat durch technische und organisatorische Maßnahmen zu erfolgen.

(3) Für die einzelnen Vorgänge der Datenverarbeitung sind die konkreten Schutzmaßnahmen zu dokumentieren und auf ihre Angemessenheit zu überprüfen.

(4) Die IT-Abteilung kann weitergehende Vorgaben im Interesse der Datensicherheit erlassen, insbesondere in Bezug auf die Nutzung von IT-Systemen in der Hochschule.

§ 14 Werbemaßnahmen und Kontaktaufnahme vor Studienbeginn

(1) Die werbliche Ansprache von Studieninteressierten etc. z. B. per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn diese zuvor in die Verwendung ihrer Daten zu Werbezwecken eingewilligt haben. Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig.

(2) Im Vorfeld eines Vertrags bzw. des Studiums ist es während der Phase der Vertragsanbahnung/Immatrikulation zulässig, Daten zur Erstellung von Informationsmaterial, zur Vorbereitung von Vertrags-/Studienunterlagen und zur Erfüllung

sonstiger auf den Vertrag oder das Studium gerichtete Wünsche zu verarbeiten.

(3) Soweit potentielle Studierende oder Lehrkräfte ihre Einwilligung erteilt haben, können sie auch unter Verwendung der Daten, die sie mitgeteilt haben, kontaktiert werden. Etwaige Einschränkungen der oder des Betroffenen sind hierbei zu beachten.

(4) Für die Kommunikation während eines laufenden Vertragsverhältnisses mit der oder dem Studierenden oder der Lehrkraft, ist eine Einwilligung zur Datenverarbeitung nicht erforderlich, soweit die Datenverarbeitung zur Erfüllung der vertraglichen Verpflichtungen erforderlich ist.

§ 15 Erstellung von Nutzerprofilen

(1) Nutzerprofile mit Personenbezug dürfen nur mit Einwilligung der oder des Betroffenen erstellt werden. Andernfalls ist durch organisatorische und technische Maßnahmen sicherzustellen, dass Nutzerprofile nur ohne Personenbezug erstellt werden.

(2) Ohne Einwilligung der oder des Betroffenen und ohne eine besondere Ermächtigungsgrundlage bleiben statistische Auswertungen und Untersuchungen auf Basis anonymisierter oder pseudonymisierter Daten möglich. Soweit jedoch pseudonymisierte Nutzerprofile angelegt werden, muss die oder Betroffene hierüber informiert werden und eine Widerspruchsmöglichkeit haben.

§ 16 Auftragsverarbeitung

(1) Wenn Dienstleister der Hochschule in deren Auftrag personenbezogene Daten verarbeiten, ist zu beachten, dass die gleichen Sorgfaltsanforderungen wie bei der verantwortlichen Stelle auch für den Dienstleister gelten.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang.
- Technisch-organisatorische Sicherheitsmaßnahmen.
- Erfahrung des Anbieters im Markt.
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.).
- Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist die oder der Datenschutzbeauftragte vorab zu informieren.
- Der Dienstleister wird im Auftrag und auch unter der Verantwortung der Hochschule tätig. Trotz der Durchführung der Datenverarbeitung durch den Dienstleister bleibt die Hochschule verantwortlich, so dass der Dienstleister sorgfältig auszuwählen ist.
- Spätestens mit Beginn der Tätigkeit für die Hochschule ist dafür Sorge zu tragen, dass der Dienstleister einen gesonderten Vertrag zur Auftragsdatenverarbeitung unterzeichnet hat und die Einhaltung der Pflichten aus dem Vertrag zur Auftragsdatenverarbeitung kontrolliert wird.
- Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

§ 17 Übermittlung/Weitergabe von Daten

(1) Die Übermittlung personenbezogener Daten ist ein Fall der Verarbeitung von Daten im Sinne dieser Datenschutzrichtlinie und nach Maßgabe des Gesetzes. Auch die Übermittlung ist daher nur mit Einwilligung der oder des Betroffenen oder aufgrund einer anderen gesetzlichen Ermächtigungsgrundlage zulässig.

(2) Bei der Übermittlung in das Ausland ist zusätzlich zu prüfen, ob hierdurch die Interessen und Rechte der oder des Betroffenen beeinträchtigt werden. Unproblematisch ist insoweit die Übermittlung in einen Vertragsstaat des Europäischen Wirtschaftsraums (alle Mitgliedsländer der Europäischen Union, Island, Liechtenstein und Norwegen). Bei allen anderen Staaten ist vorab zu prüfen, ob ein vergleichbarer Datenschutzstandard besteht. Ein vergleichbarer Standard kann unter anderem durch den Abschluss zusätzlicher vertraglicher Vereinbarungen erreicht werden, etwa durch Nutzung der EU-Standardvertragsklauseln oder auch durch das Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission für den jeweiligen Staat. Jede Übermittlung von

personenbezogenen Daten in einen Staat außerhalb des Europäischen Wirtschaftsraumes ist mit der oder dem Datenschutzbeauftragten abzustimmen.

Innerbetriebliche Prozesse

§ 18 Anforderungen an die Beschäftigten

(1) Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Alle Beschäftigten der Hochschule sind vor Aufnahme ihrer Tätigkeit auf das Datengeheimnis nach § 3 Absatz 2 LDSG zu verpflichten. Sie sind darüber zu belehren, dass es untersagt ist, personenbezogene Daten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder sie Unbefugten zugänglich zu machen. Die Beschäftigten sind darüber zu belehren, dass die Pflicht zur Wahrung der Vertraulichkeit über das Ende der Tätigkeit für die verantwortliche Stelle fort gilt.

(2) Beschäftigte mit besonderen Geheimhaltungsverpflichtungen (z. B. Fernmeldegeheimnis nach § 88 TKG) werden von der Hochschule ergänzend darauf schriftlich verpflichtet.

(3) Auch innerhalb der Hochschule ist darauf zu achten, dass nur die Beschäftigte Zugriff auf personenbezogene Daten erhalten, die sie zur Erledigung ihrer Aufgaben für die Hochschule benötigen.

(4) Alle Beschäftigten sollen zu Beginn ihrer Tätigkeit und nachfolgend regelmäßig in Datenschutzthemen geschult werden.

§ 19 Dokumentationspflichten

(1) Die Hochschule führt ein Verzeichnis über ihre Verfahren zur Verarbeitung personenbezogener Daten (Verfahrensverzeichnis).

(2) Um das Verfahrensverzeichnis vollständig und aktuell zu halten, haben die Beschäftigten entsprechend den Vorgaben der oder des Datenschutzbeauftragten alle Verfahren unter Nutzung entsprechender Vordrucke zu melden.

§ 20 Einführung neuer Systeme zur Datenverarbeitung

Die Einführung neuer Systeme Verarbeitung personenbezogener Daten ist der oder dem Datenschutzbeauftragten vorab anzuzeigen, damit dieser die datenschutzrechtliche Zulässigkeit prüfen kann.

§ 21 Schulung

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Der Datenschutzbeauftragte entscheidet über Form und Turnus der entsprechenden Schulungen.

§ 22 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art der Daten und deren Schutzbedürftigkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Risikoanalyse zu erfolgen. Dies gilt insbesondere für besondere personenbezogene Daten.

(2) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-To-Know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

(3) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(4) Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

(5) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten

sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

§ 23 Unrechtmäßige Kenntniserlangung von Daten („Datenpanne“)

(1) Sollten vertrauliche Informationen der Hochschule unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich die oder der Datenschutzbeauftragte zu informieren.

(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(3) Die Erfüllung einer etwaigen Informationspflicht gegenüber Betroffenen oder Aufsichtsbehörden erfolgt ausschließlich durch die oder den Datenschutzbeauftragten.

Rechte der Betroffenen

§ 24 Recht auf Auskunft

(1) Auf Anfrage ist einem Betroffenen Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten zu erteilen. Die oder der Betroffene soll dabei die Art der Daten, zu denen er eine Auskunft wünscht, näher bezeichnen.

(2) Die Auskunftserteilung soll schriftlich in einer für die oder den Betroffenen verständlichen Form und Sprache erfolgen. Bei der Auskunftserteilung sind die vorhandenen personenbezogenen Daten und der Zweck der Speicherung mitzuteilen. Weiter soll, soweit verfügbar, die Herkunft der Daten, Empfänger der Daten, die geplante Dauer der Speicherung, das Beschwerderecht bei der Aufsichtsbehörde und das Bestehen einer automatisierten Entscheidungsfindung erläutert werden.

(3) Bei der Auskunftserteilung ist sicherzustellen, dass die Identität der oder des Betroffenen verifiziert wird.

(4) Über alle Anfragen auf Auskunftserteilung ist die oder der Datenschutzbeauftragte zu informieren, damit diese oder dieser die weiteren Aktivitäten koordinieren oder übernehmen kann. Soweit die oder der Datenschutzbeauftragte nicht ausdrücklich die Bearbeitung übernimmt, bleibt die jeweilige Fachabteilung für die Beantwortung der Anfrage zuständig.

(5) Wenn eine Anfrage nicht umgehend beantwortet werden kann, ist der oder dem Betroffenen zumindest eine Zwischeninformation zu übermitteln, in der die voraussichtliche Bearbeitungszeit mitgeteilt wird.

(6) Die Auskunft kann aus den in § 9 Absatz 1 i.V.m. § 8 Absatz 1 Nummer 1 bis 4 LDSG genannten Gründen abgelehnt werden.

§ 25 Recht auf Berichtigung

(1) Unvollständige oder unrichtige personenbezogene Daten sind auf Verlangen des Betroffenen zu korrigieren. Die Korrektur ist dabei auch im Interesse der Hochschule, da der gesamte Datenbestand möglichst richtig und von hoher Qualität sein soll.

(2) Soweit eine Beschäftigte oder ein Beschäftigter Kenntnis davon hat, dass bei der Hochschule gespeicherte Daten unvollständig und unrichtig sind, soll diese oder dieser die jeweilige Fachabteilung hierüber informieren, damit eine Korrektur veranlasst werden kann.

§ 26 Recht auf Löschung

(1) Der oder die Betroffene hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer in Artikel 17 Absatz I lit. a) – f) DSGVO (Verordnung (EU) 2016/679) aufgeführten Gründe zutrifft.

(2) Das Recht auf Löschung ist nach den in § 10 LDSG genannten Fällen beschränkt. Es besteht nicht, wenn durch die Löschung der Daten schutzwürdige Interessen des Betroffenen eingeschränkt würden oder wenn die Löschung nur mit einem unverhältnismäßig hohen Aufwand möglich ist.

§ 27 Recht auf Einschränkung der Verarbeitung

Der oder die Betroffene hat auch das Recht die Einschränkung der Verarbeitung in den in Artikel

18 DSGVO (Verordnung (EU) 2016/679) genannten Fällen zu verlangen.

§ 28 Recht auf Datenübertragbarkeit

Der oder die Betroffene hat gemäß Art. 20 DSGVO (Verordnung (EU) 2016/679) das Recht die ihn betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen, sofern die Verarbeitung auf Grundlage einer Einwilligung oder einem Vertrag beruht und die Verarbeitung mittels automatisierter Verfahren erfolgt.

§ 29 Recht Widerspruch und Beschwerde

(1) Der oder die Betroffene hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von § 4 LDSG oder Artikel 6 Absatz 1 lit. f) erfolgt, Widerspruch einzulegen.

(2) Widerspricht die oder der Betroffene der Datenverarbeitung, ist zu prüfen, inwieweit auf die Datenverarbeitung zukünftig verzichtet werden kann. Ist dies nicht möglich, ist der oder dem Betroffenen dies entsprechend zu erläutern. Die Hochschule verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, sie kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(3) Die oder der Betroffene hat die Möglichkeit, sich über den Umgang mit seinen personenbezogenen Daten in der Hochschule zu beschweren. Die Beschwerde ist unverzüglich an die oder den Datenschutzbeauftragten weiterzuleiten, sofern sie nicht an ihn direkt gerichtet war. Die oder der Datenschutzbeauftragte wird die Beschwerde beantworten und ggf. angemessene Maßnahmen zur Verbesserung des Datenschutzniveaus vorschlagen.

(4) Gemäß Art. 77 DSGVO (Verordnung (EU) 2016/679) hat der oder die Betroffene das Recht sich bei einer Aufsichtsbehörde zu beschweren.

Zuständigkeit

§ 30 Verantwortung

(1) In erster Linie sind diejenigen Beschäftigten für die Einhaltung der Vorgaben dieser Datenschutzrichtlinie verantwortlich, die jeweils mit der Datenverarbeitung betraut sind.

(2) Alle Beschäftigten der Hochschule haben auf die Einhaltung dieser Datenschutzrichtlinie zu achten und auf diese Weise dazu beizutragen, dass in der gesamten verantwortlichen Stelle einheitlich hohe Datenschutzstandards etabliert werden.

(3) Die Leitung der Hochschule hat darauf zu achten, dass die Beschäftigten über die Datenschutzrichtlinie informiert werden. Zu der Information gehört auch der Hinweis, dass Verstöße gegen die Vorgaben dieser Datenschutzrichtlinie straf-, haftungs- oder arbeitsrechtliche Konsequenzen nach sich ziehen können.

(4) Die Hochschule bleibt gegenüber den Betroffenen die verantwortliche Stelle im Sinne des Gesetzes. Die oder der einzelne Beschäftigte handelt daher für die Institution und hat deren Vorgaben zu beachten.

§ 31 Datenschutzbeauftragte oder Datenschutzbeauftragter als Ansprechpartner

(1) Die Hochschule hat eine oder einen Datenschutzbeauftragten nach Maßgabe des Artikel 37 Absatz 1 lit. a) DSGVO (Verordnung (EU) 2016/679) bestellt.

(2) Fragen zu dieser Datenschutzrichtlinie oder dem richtigen Umgang mit personenbezogenen Daten können an die oder den Datenschutzbeauftragten gerichtet werden. Die Kontaktdaten der oder des Datenschutzbeauftragten sind im internen Bereich der Homepage abrufbar und am schwarzen Brett ausgehängt.

(3) Die oder der Datenschutzbeauftragte koordiniert die datenschutzrechtlichen Aktivitäten der Hochschule. Sie oder er ist u.a. Ansprechpartnerin oder Ansprechpartner für die Betroffenen, die mit der Datenverarbeitung betrauten Beschäftigten und die Leitung der verantwortlichen Stelle.

(4) Die oder der Datenschutzbeauftragte überwacht die Einhaltung der gesetzlichen Vorgaben sowie die der Richtlinie. Die oder der Daten-

schutzbeauftragte berät die Leitung der Hochschule zu Fragen des Datenschutzes, ist zuständig bei der Kommunikation mit Betroffenen und Aufsichtsbehörden und berichtet der Leitung regelmäßig über die Umsetzung des Datenschutzes in der Hochschule. Ausgewählte Prozesse werden stichprobenartig und in angemessenen Zeitabständen durch sie oder ihn auf ihre Datenschutzkonformität hin kontrolliert.

(5) Die oder der Datenschutzbeauftragte ist auch befugt, die Einhaltung dieser Datenschutzrichtlinie zu prüfen und die Beachtung der gesetzlichen Bestimmungen des Datenschutzrechts zu überwachen. Die entsprechende Überwachungsbefugnis entbindet aber nicht den einzelnen Beschäftigten von seiner Verantwortung.

(6) Die oder der Datenschutzbeauftragte nimmt ihre oder seine Aufgaben weisungsfrei und unter Anwendung ihrer oder seiner Fachkunde wahr. Sie oder er ist der Leitung der Hochschule unmittelbar unterstellt.

(7) Alle Beschäftigten haben die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben und Aktivitäten zu unterstützen.

(8) Bei Bedarf kann die oder der Datenschutzbeauftragte in Ergänzung zu dieser Datenschutzrichtlinie Handlungsempfehlungen zu speziellen Themen herausgeben.

§ 32 Meldung von Verstößen und Zusammenarbeit mit Aufsichtsbehörden

(1) Die Beschäftigten sollen der Datenschutzbeauftragten oder dem Datenschutzbeauftragten unverzüglich Bericht erstatten, wenn sie Kenntnis von einem Verstoß gegen diese Richtlinie oder gesetzliche Bestimmungen haben, die sich auf den Schutz personenbezogener Daten beziehen. Die oder der Datenschutzbeauftragte prüft ggf., inwieweit auch eine Informationspflicht gegenüber den Aufsichtsbehörden besteht.

(2) Die verantwortliche Stelle arbeitet mit den zuständigen Aufsichtsbehörden kooperativ und vertrauensvoll zusammen. Im Falle einer gesetzlichen Auskunftsverpflichtung wird die Hochschule die geforderten Auskünfte unverzüglich erteilen. Maßnahmen und Feststellungen der Aufsichtsbehörden werden von der verantwortlichen Stelle uneingeschränkt akzeptiert, soweit sie rechtmäßig sind. Die Kommunikation mit den Aufsichtsbehörden soll über die oder den Datenschutzbeauftragten erfolgen.

Schlussbestimmungen

§ 33 Folgen von Verstößen

Ein grob fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

§ 34 Publizität

(1) Diese Datenschutzrichtlinie ist allen Beschäftigten der Hochschule in geeigneter Weise zugänglich zu machen, insbesondere über die Amtlichen Bekanntmachungen sowie den internen Bereich der Homepage.

(2) Eine allgemeine Veröffentlichung dieser Richtlinie ist nicht vorgesehen, da es sich um eine interne Richtlinie der Hochschule handelt.

§ 35 Änderungen dieser Datenschutzrichtlinie

(1) Die Hochschule behält sich das Recht vor, diese Datenschutzrichtlinie bei Bedarf zu ändern. Eine Änderung kann insbesondere erforderlich werden, um gesetzlichen Vorgaben, bindenden Verordnungen, Forderungen der Aufsichtsbehörden oder internen Verfahren zu entsprechen.

(2) Änderungen an der Richtlinie sind formlos wirksam. Die Beschäftigten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben zu informieren.

(3) In regelmäßigen Abständen soll geprüft werden, inwieweit technologische Veränderungen eine Anpassung dieser Richtlinie erforderlich machen.

§ 36 Inkrafttreten

Diese Richtlinie tritt am ersten Tag des auf ihre Bekanntmachung folgenden Monats in Kraft.

Weingarten, 20. Februar 2019

gez.
Prof. Dr. Karin Schweizer
(Rektorin)