# Datenschutzfolgenabschätzung gemäß Artikel 35 EU-DSGVO im Bezug auf die Daten der Studenten an der HSF Meißen (FH)

**B a c h e l o r - A r b e i t**
**an der Hochschule für öffentliche Verwaltung und Rechtspflege (FH),**
**Fortbildungszentrum des Freistaates Sachsen**
**zum Erwerb des Hochschulgrades**
**Bachelor of Laws (LL.B.)**

**vorgelegt von**
**Tom Rajko Hauwetter**
**aus Plessa**

**Meißen, 27.08.2018**

# Inhaltsverzeichnis

## Darstellungsverzeichnis

## Abkürzungsverzeichnis

| Abkürzung | Erläuterung |
|---|---|
| BDSG | Bundesdatenschutzgesetz |
| DSB | Datenschutzbeauftragter |
| DSFA | Datenschutzfolgenabschätzung |
| EGL | Ermächtigungsgrundlage |
| EU | Europäische Union |
| EU-DSGVO | Europäische Datenschutzgrundverordnung |
| HSF Meißen (FH) | Hochschule für öffentliche Verwaltung und Rechtspflege (FH), Fortbildungszentrum des Freistaates Sachsen |
| ILIAS | Integriertes Lern-, Informations- und Arbeitskooperations-System, hier als Software für die digitale Lehre an den Hochschulen für den öffentlichen Dienst, insbesondere die E-Learning Plattform der HSF Meißen (FH) |
| SächsDSDG | Sächsisches Datenschutzdurchführungsgesetz |
| ZIT | Zentrum für Informationstechnologie |

**Abstract**

Das Thema der Arbeit soll die Datenschutz-Folgenabschätzung darstellen. Hierbei soll der Sinn und Zweck sowie die Anwendung dieses Instrumentes verdeutlicht werden. Weiterhin ist das Ziel die Datenschutz-Folgenabschätzung anhand der Daten, welche die Hochschule Meißen über die Studierenden gespeichert hat durchzuführen. Dabei soll vom allgemeinen Aufbau bis hin zu den Feinheiten der Ablauf durchgespielt werden. Das Ziel der Arbeit besteht in einer im Rahmen der Bachelorarbeit möglichst vollständigen Datenschutz-Folgeabschätzung für personenbezogene Daten der Studenten[1] an der Hochschule Meißen (FH).

Die Datenschutz-Folgeabschätzung richtet sich nach dem Art. 35 der Europäischen Datenschutzgrundverordnung, die am 08. Mai 2018 Rechtswirkung entfaltet. In diesem Artikel sind die Mindestanforderungen und die Tatbestände festgeschrieben, sowie wann und wie dieses Instrument einzusetzen ist. Ebenfalls wurde in der deutschen Datenschutz-Konferenz ein Kurzpapier zum Verfahren als auch zum Umgang verfasst.

In meiner Arbeit soll sich mit der Frage des Sinnes und Zweckes einer Datenschutz-Folgeabschätzung befasst werden. Welche Möglichkeiten und Gefahren/Risiken ergeben sich daraus. Was ist mit großen Restrisiken, die nicht vermieden werden können?

Für die Erstellung meiner Arbeit habe ich größtenteils Internetquellen verwendet, da sich die Anzahl von aussagekräftiger Literatur noch in Grenzen hält und weitere Beispiele aus der Praxis noch nicht vorliegen. Dies ist der Aktualität des Themas geschuldet. Insgesamt habe ich mit dieser Bachelorarbeit feststellen können, dass die Hochschule Meißen die Daten ihrer Studenten sehr gut und sicher aufbewahrt und dabei die Vorgaben der EU-DSGVO einhält. Einige Aspekte im Bereich der Datenschutzfolgenabschätzung sind noch nicht ganz ausgeprägt, jedoch in Ansätzen vorhanden und können ausgebaut werden.

Ich vermute, dass die HSF Meißen in der nahen Zukunft keine weiteren Probleme mit der neuen EU-DSGVO im Hinblick auf die Datenschutzfolgenabschätzung haben wird, da der Datensicherheitsstandard sehr hoch angesetzt ist und viele Maßnahmen von der Hochschule als auch vom Freistaat Sachsen unternommen

[1] Aus Gründen der leichteren Lesbarkeit wird in der gesamten Bachelorarbeit auf die Nennung beider Geschlechter verzichtet. Als geschlechtsneutrale Formulierung wird die männliche Bezeichnung verwendet, gemeint sind beide Geschlechter.

werden, um Angriffe auf diese öffentlichen Einrichtungen zu unterbinden bzw. denen entgegenzuwirken.

# 1 Einleitung

In meiner Bachelorarbeit mit dem Thema „Datenschutzfolgenabschätzung gemäß Artikel 35 EU-DSGVO im Bezug auf die Daten der Studenten an der HSF Meißen (FH)“ beschäftige ich mich mit der neuen Datenschutzfolgenabschätzung gemäß Artikel 35 der Europäischen Datenschutzgrundverordnung. Hierbei wird ein kurzer Einblick in die Europäische Datenschutzgrundverordnung gewährt, mit deren Absichten für den Datenschutz in Europa und den Änderungen im Vergleich zum bis jetzt geltenden Bundesdatenschutzgesetz. Das Hauptaugenmerk liegt auf der Datenschutzfolgenabschätzung, einem bereits bekannten Verfahren aus dem § 67 Bundesdatenschutzgesetz „in neuem Gewand“. Für die deutschen Unternehmen und Verwaltungen ergibt sich daraus keine komplette Umstellung, jedoch der Zwang sich genauer mit diesem Instrument auseinanderzusetzen und mehr Zeit dafür zu investieren. Nachdem die Theorie abgehandelt und die Voraussetzungen geklärt sind, wird das Verfahren der Datenschutzfolgenabschätzung anhand der Daten der Studenten, welche die HSF Meißen (FH) von ihren Studenten erhebt, durchgeführt. Hierbei liegt der Fokus auf den Datenverarbeitungsvorgängen mit den Studentenakten.

Mit dieser Arbeit möchte ich vor allem die folgenden Fragen beantworten: Welche Relevanz hat die neue Datenschutzfolgenabschätzung für die Verwaltung? Welche Vorteile und Nachteile ergeben sich aus der Durchführung? Wie gestaltet sich der genaue Ablauf vom Begründen des Zweckes über die Datenerhebung bis hin zur Löschung der Daten? Ebenfalls ziehe ich einen Vergleich von der alten Folgenabschätzung nach dem deutschen BDSG und der neuen Datenschutzfolgenabschätzung nach der EU-DSGVO. Als Abschluss der Arbeit steht die Betrachtung der Folgen für die Hochschule Meißen und die Erstellung eines Vorschlagkataloges.

Der Dreh- und Angelpunkt meiner Bachelorarbeit stützt sich auf die Datenschutzfolgeabschätzung an der Hochschule Meißen. Überprüft wird dabei die Relevanz für die Hochschule eine solche Abschätzung durchzuführen. Im gleichen Atemzug werden Vor- und Nachteile, die daraus resultieren, aufgedeckt und bewertet. Ein weiterer relevanter Punkt der Bachelorarbeit erfolgt in der Bewertung des Sinnes und Zweckes der DSFA für die Daten der Studenten. Ich möchte dabei herausstellen, inwieweit die Sicherheit von der Seite der Hochschule gewährleistet wird und welche Verbesserungsmöglichkeiten bestehen. Der Grund für meine Betrachtungen liegt in der, durch die Europäische Union, gesteigerten Bedeutung für die Datenschutzfolgenabschätzung. Im Vergleich zur alten Folgenabschät-

zung sind bei einem Fehlverhalten schwerwiegendere Strafen festgelegt, weitreichende Meldepflichten bestimmt und den betroffenen Personen mehr Rechte eingeräumt. Insgesamt zielt die Regelung auf einen einheitlichen Umgang mit den Daten von natürlichen Personen in der gesamten Europäischen Union ab.

Das Ziel meiner Bachelorarbeit ist es eine beispielhafte Datenschutzfolgeabschätzung für die HSF Meißen (FH) zu erstellen, bei der die Daten der Studenten in den Akten betrachtet werden sollen. Hierbei beschränke ich mich nur auf die Datenverarbeitung, die mit den Daten aus der Studentenakte vorgenommen wird. Für die vorhandenen Daten der Studenten achte ich auf die Notwendigkeit der Erhebung, wo die Ermächtigungsgrundlage für die Erhebung und Verarbeitung geregelt ist und welche Risiken im Moment bestehen. Aufbauend darauf möchte ich zum Schluss dieser Arbeit Verbesserungsvorschläge präsentieren, welche von der HSF Meißen (FH) zur Konformität ihrer Datenschutzfolgenabschätzung führen.

# 2 Aufbau der EU-DSGVO

## 2.1 Definition

Die Europäische Datenschutzgrundverordnung ist eine durch die Europäische Union erlassene Verordnung, die zu einem einheitlichen Datenschutzrecht im gesamten Gebiet führen soll. Hierbei wurde eine große Anzahl von datenschutzrelevanten Aspekten aus den Jahren 1995 bis heute aufgenommen, sodass die Richtline 95/46/EG zum Datenschutz aus dem selbigen Jahr ersetzt werden kann. Die EU-DSGVO wurde am 14. April 2016 beschlossen und ist seit dem 25. Mai 2018 wirksam. Das verfolgte Ziel der EU ist eine Harmonisierung des europäischen Binnenmarktes, damit jedes Land faire und einheitliche Grundsätze im Bereich des Datenschutzes bietet. Ebenfalls wird versucht ein ausgeglichenes Verhältnis zwischen den Interessen von Unternehmern und Privatpersonen herzustellen. Mit der EU-DSGVO werden den betroffenen natürlichen Personen mehr Rechte eingeräumt, sich auf ihre Daten zu berufen und die Strafen für Unternehmen sind deutlich erhöht worden, sodass ein Verstoß zu finanziellen Schäden führen kann.[2]

Für Deutschland galt das Bundesdatenschutzgesetz in Verbindung mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und die einzelnen Landesrechte. Dabei stützen sich alle auf die Grundprinzipien des Datenschutzes, welche sich in sieben Säulen zusammenfassen lassen.

Das Fundament für den Datenschutz bildet hierbei das Recht auf informationelle Selbstbestimmung. Damit wird geregelt, dass jeder Mensch selbst bestimmen darf, welche Informationen über ihn aufgenommen, gespeichert, verarbeitet und weitergegeben werden dürfen. Insofern kein rechtlicher Zwang zur Abgabe von Informationen besteht, kann jeder verweigern Daten über seine Person preiszugeben, ohne einen Nachteil erwarten zu müssen.

Im Artikel 5 der EU-DSGVO werden die Prinzipien erläutert nach denen personenbezogene Daten behandelt werden müssen. Die sechs im Art. 5 Abs. 1 EU-DSGVO genannten Aspekte sind die Rechtmäßigkeit, die Zweckbindung, die Datenminimierung, die Richtigkeit, die Speicherbegrenzung sowie Integri-

[2] vgl. o. V.: Europäische Datenschutz-Grundverordnung, Datum unbekannt

tät und Vertraulichkeit. Des Weiteren ergeben sich aus dem Art. 5 Abs. 2 EU-DSGVO die Rechenschaftspflichten für den Verantwortlichen der Datenverarbeitung.

Eine genauso wichtige Säulen sind die Korrekturrechte der Betroffenen. Damit soll es jedem Betroffenen freistehen seine eigenen Daten einzusehen, zu korrigieren und bei Bedarf eine gewährte Einwilligung zur Verwendung zurückzuziehen. Bei einem Widerruf der Daten gilt dies jedoch nicht rückwirkend, sondern erst ab dem Zeitpunkt des Widerrufes. Informationen können auch gesperrt oder gelöscht werden.

Als nächster Punkt stellt sich die Sicherung der Daten heraus. Hierbei muss durch die verwaltende Stelle sichergestellt werden, dass die gespeicherten Informationen nicht verloren gehen, gestohlen werden oder anderweitig in Umlauf geraten. Ebenfalls bedürfen diese eines Schutzes vor Manipulation und Zugriffsrechte sollen definiert werden, sodass nur berechtigte Mitarbeiter auf Daten zugreifen dürfen, mit denen sie selber arbeiten müssen.

Die letzten beiden Aspekte sind die Kontrolle und die Sanktionen. Dabei sollen alle die eben genannten Punkte eingehalten werden und bei einem Verstoß zuerst gemeldet werden und weiterhin Bestrafungen nach sich ziehen.

Aus allen aufgezählten Prinzipien hat sich das Bundesdatenschutzgesetz aufgebaut und legt fest, wann Daten erhoben, verarbeitet, genutzt und weitergegeben werden dürfen. Sie enthält auch Regelungen zum Datenschutzbeauftragten, der Verarbeitung im Einzelnen und im letzten Abschnitt zu Bußgeldern und anderen Strafen.[3]

## 2.2 Grundsätze der EU-DSGVO

Alle aktuell geltenden Grundsätze finden sich in der EU-DSGVO im Artikel 5 und im § 47 BDSG.

Die Rechtmäßigkeit als ein unbestimmter Rechtsbegriff wird im Art. 6 EU-DSGVO näher beschrieben und es wird festgelegt, wann eine Datenverarbeitung legitim ist. Hierfür wurde im Art. 6 Abs. 1 EU-DSGVO ein abschließender Katalog erstellt, welcher Bedingungen enthält, von denen wenigstens eine erfüllt sein muss. Als Rechtsgrundlage für die Verarbeitung von Daten dient

[3] vgl. Brünen, et. al., 2018

dabei entweder das Unionsrecht oder spezifisches Recht der Mitgliedsstaaten, wofür die EU-DSGVO einen Rahmen vorgibt.[4]

Im Bereich der Verarbeitung nach Treu und Glauben wird sich auf das Prinzip der Sittlichkeit berufen. Die Daten der betroffenen Person werden dabei anständig, im allgemeinen Sinne, verarbeitet. Dabei gibt es keine Pauschalisierung, sondern jeder Fall muss einzeln betrachtet und die gegebenen Umstände berücksichtigt werden.

Mit dem Grundsatz der Transparenz wird dem Betroffenen sein Recht auf informationelle Selbstbestimmung Rechenschaft getragen. Mit der EU-DSGVO sind zwei neue Wege eingebracht wurden, diesen Grundsatz zu bestärken, zum einen der „Datenschutz durch Technik“ und zum anderen datenschutzfreundliche Voreinstellungen.

Dabei wird dem Betroffenen versichert, dass die erhobenen Daten mit gutem Gewissen erhoben sowie verarbeitet und nur für die genannten Zwecke verwendet werden, dies entspricht der Zweckbindung. Die Datenverarbeitung kann durch jedermann nachvollzogen werden und ist transparent dargestellt. Bei diesem Grundsatz handelt es sich um die Zuordnung von erhobenen Daten mit einem festgelegten, eindeutigen und legitimen Zweck. Somit kann sich der Betroffene sicher sein, dass seine Daten nur für die ihn bekannten Verfahren eingesetzt werden. Eine Ausnahme dazu besteht in Artikel 89 EU-DSGVO für eine Weiterverarbeitung im öffentlichen Interesse, für wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke.[5]

Im Hinblick auf die Datenminimierung sollen nur Daten erhoben werden, die erheblich und angemessen sind den Zweck zu erfüllen. Es sollen nur so viele Daten erhoben werden wie nötig sind und gleichzeitig so wenige wie möglich.

Durch die Richtigkeit der Datenverarbeitung sollen falsche bzw. unrichtige Daten nicht weiter verarbeitet werden, sondern unverzüglich gelöscht oder berichtigt werden. Die Daten müssen von dem Verantwortlichen immer auf dem neuesten Stand gehalten werden, sodass keine Verarbeitung mit unrichtigen personenbezogenen Daten erfolgt.[6]

[4] vgl. Härting, 2016, S. 26
[5] vgl. Datenschutz, Dr., 2017
[6] vgl. Härting, 2016, S. 28f.

Hiermit wurde durch die EU-DSGVO festgelegt, dass sobald der Zweck der Datenverarbeitung erreicht wurde, alle Daten, die eine Identifikation der Person zulassen, gelöscht werden müssen. Jedoch gibt es einige Ausnahmen, bei denen die öffentlichen Interessen, die des Einzelnen überwiegen.

Das Unternehmen oder die Verwaltung versichert die personenbezogenen Daten mit angemessenen Sicherheitsmaßnahmen zu speichern, zu sichern und zu verarbeiten. Vor allem werden damit ein Zugriff von Unberechtigten und ein Verlust der Daten durch den Verantwortlichen ausgeschlossen, womit die Vertraulichkeit und Integrität gewährleistet wird. Damit dieses Ziel erreicht werden kann, sind die Unternehmen und die Verwaltung angehalten entsprechende technische und organisatorische Maßnahmen einzurichten. Mit einem solchen Verhalten wird dem Grundsatz der Speicherbegrenzung entsprochen. [7]

Unter den Rechenschaftspflichten verstehen sich die neuen Grundsätze, dass ein Betroffener jederzeit das Recht hat, sich über die vorliegenden Daten zu informieren nach Art. 15 EU-DSGVO, seine Einwilligung für die Verwendung seiner Daten in Zukunft zu untersagen nach Art. 18 EU-DSGVO und auch die Datenportabilität nach Art. 20 EU-DSGVO.

### 2.3 Vergleich der EU-DSGVO zum BDSG

In der EU-DSGVO sind viele Aspekte aus dem BDSG immer noch enthalten, wobei in einigen Bereichen Neuregelungen getroffen, bestehendes Recht verschärft und bestimmte Regelungen entfernt wurden. Die Änderung durch die Europäische Union beruht auf den Erfahrungen der letzten 20 Jahre und gilt nicht nur für europäische Unternehmen/Verwaltungen auf Grund des Marktortprinzips.

Des Weiteren sind zwei komplett neue Grundsätze eingefügt worden, welche sich vor allem mit den Online-Geschäften und Online-Handel auseinandersetzen. Zudem ist der Begriff der personenbezogenen Daten, welcher zuvor nach § 3 BDSG geregelt war, im Art. 4 EU-DSGVO im weiter gefasst. In der Zukunft werden noch mehr Bereiche, in denen es um Informationen über natürliche Personen handelt, von dieser Verordnung umfasst.

Insgesamt wurde die Position der natürlichen Personen gestärkt und ein weitreichender Schutz realisiert. Mit den Verschärfungen der Auflagen in Form der

[7] vgl. Datenschutz, Dr., 2017

gesteigerten Bedeutung der Datenschutzfolgenabschätzung, der Erweiterung von Grundsätzen, den verschärften Meldepflichten und vor allem den erhöhten Strafen, sind die Unternehmen/Verwaltungen dazu angehalten, die Bestimmungen der EU-DSGVO einzuhalten. [8]

Der Punkt der DSFA wurde besonders gestärkt und mit mehr Auflagen sowie Mindestanforderungen versehen. Damit soll insgesamt ein gestärktes Bewusstsein der Unternehmen/Verwaltung für die Verarbeitungsvorgänge, die technischen und organisatorischen Maßnahmen und die Risiken geschaffen werden. Das Prinzip einer Folgenabschätzung ist im deutschen BDSG bereits enthalten gewesen, jedoch in einer milderen Form. Die Voraussetzungen wurden angepasst, sodass nun mehr Datenverarbeitungsvorgänge umfasst werden, die Relevanz dieses Verfahrens erhöht wurde und durch die Meldepflichten auch der Betroffene schneller und genauer informiert werden muss.

Trotz des größeren Aufwandes für die Unternehmen/Verwaltung soll dieses Instrument ein Vorteil für beide Parteien darstellen. Es kann eine bessere Übersicht innerhalb des Unternehmens/der Verwaltung geschaffen werden, mit der weniger „Datenunfälle“ passieren. Ebenfalls können alte und unsichere Technologien sowie Verfahren ersetzt werden und eine Überprüfung im gleichen Atemzug stattfinden. Somit sind die Unternehmen/Verwaltung angehalten, mit der Zeit im Sinne des Standes der Technik zu gehen und sie wahren in allen Bereichen der Datenverarbeitung den Überblick.

In Zusammenhang mit der DSFA kann ebenfalls die bestehende Technik aktualisiert werden. Da eine Datenverarbeitung erst vollzogen werden darf, wenn die bestehende Technik geprüft wurde. Für die Unternehmen/Verwaltung wäre dieser Zeitpunkt sehr günstig, um neue Verfahren einzuführen oder alte Technologien auszuwechseln, sodass nicht doppelt, für alte und neue Technologien, eine EU-DSGVO-Kompatibilität besteht.

### 2.4 Ermächtigungsgrundlage der HSF Meißen (FH)

Die Hochschule selbst benennt auf ihrer Webseite unter dem Punkt Datenschutz alle für sie selbst zutreffenden rechtlichen Grundlagen. Darunter zählen die EU-DSGVO, das BDSG, das SächsDSDG, das Sächsische Datenschutzgesetz, das Fachhochschule-Meißen-Gesetz, das Sächsische Hochschulfreiheitsgesetz und die Sächsische Hochschulpersonendatenverordnung.[9] Für

[8] vgl. Bentz, 2017
[9] vgl. o. V.: Datenschutzerklärungen, Datum unbekannt

meine Betrachtung der Verarbeitung der Daten der Hochschulstudenten fällt jedoch die Sächsische Hochschulpersonendatenverordnung heraus, weil sich diese auf das Personal an der HSF Meißen (FH) bezieht, welche nicht zu meinem eingeschränkten Bereich zählen. In der kompletten Aufzählung findet sich jedoch keine genaue Beschreibung einer expliziten Ermächtigungsgrundlage für die Erhebung von Daten, wie sie von dem EU-DSGVO gefordert wird. Somit sind alle Gesetzlichkeiten nacheinander zu prüfen, ob sich eine Grundlage finden lässt.

Das Bundesdatenschutzgesetz, als auch die neue Datenschutz-Grundverordnung, legen fest, dass Daten von natürlichen Personen nur mit einer gesetzlichen Grundlage erhoben werden dürfen. Somit ist es von besonderer Bedeutung für die Hochschule Meißen, ein legitimes Interesse an den Daten zu begründen und dies in einem Gesetz oder einer Verordnung festzuhalten. Sowohl im BDSG als auch in der EU-DSGVO schreiben die Gesetzgeber den Erlaubnisvorbehalt nieder, geben aber keine Grundlage, um Daten erheben zu dürfen. Somit ist der nationale Gesetzgeber angehalten eigene Regelungen in Bezug auf die Datenerhebung aufzustellen. Für die Hochschule Meißen gibt es eine Vielzahl an Gesetzen die in Frage kommen, in denen eine solche Möglichkeit eröffnet werden kann.

Zum einen könnte es eine Ermächtigungsgrundlage im SächsDSDG geben. In diesem findet sich keine Grundlage für eine Erhebung von Daten. Es werden nur die Regelungen für eine rechtmäßige und legitime Datenverarbeitung im Abschnitt 2 mit den §§ 2 bis 6 SächsDSDG festgeschrieben. Im § 5 des SächsDSDG ist eine Regelung zur Erhebung von Daten von Dritten oder anderen Stellen außerhalb des öffentlichen Bereiches. Dies trifft bei der Erhebung von Daten für die HSF Meißen nicht zu, da diese eine rechtsfähige Körperschaft des öffentlichen Rechtes ist. Daraus könnte eine Ermächtigung zur Datenerhebung abgeleitet werden, da Daten nur verarbeitet werden können, wenn diese dem Verantwortlichen vorliegen. Des Weiteren ist eine Erhebung von Daten durch Dritte ein Sonderfall, welcher im Allgemeinen vermieden werden sollte und teilweise nicht gestattet ist.

Ein weiteres mögliches Gesetz ist das Sächsische Hochschulfreiheitsgesetz, in dem es der Hochschule ermöglicht werden kann Daten zu erheben. Ähnlich zum SächsDSDG finden sich im Sächsischen Hochschulfreiheitsgesetz erneut nur Regelungen zur Verarbeitung von personenbezogenen Daten. Da die Er-

hebung von Daten jedoch unerlässlich für die Aufgaben der Hochschule ist, könnte auch hieraus eine Grundlage zur Datenerhebung abgeleitet werden. Ohne die persönlichen Daten der Studenten, kann keine eindeutige Zuordnung von Prüfungsleistungen, Anwesenheit und Zugangsberechtigungen für die Studenten erstellt werden. Es liegt somit auch hier keine explizite EGL vor.

Zum Schluss ist das Fachhochschule-Meißen-Gesetz in Betracht zu ziehen und darin eine Möglichkeit zur Datenerhebung zu prüfen. Dabei wird geregelt, dass die Hochschule Meißen dazu befähigt wird, eigene Satzungen zu erlassen. Im Bezug auf eine Rechtsgrundlage für die Erhebung von Daten findet sich hier jedoch auch keine Aussage. Somit kann zusammengefasst werden, dass die Hochschule Meißen kein explizites Recht hat die Daten der Studenten zu erheben. Aus dem allgemeinen gesetzlichen Rahmen der verschiedenen Gesetze könnte jedoch eine implizite Erlaubnis hervorgehen. Da auf Grund der Gesetze, sowohl des SächsDSDG, als auch des Sächsischen Hochschulfreiheitsgesetzes, eine legitime Datenverarbeitung, welche EU-DSGVO konform ist, erlaubt ist. Darauf wird sich im Folgenden ebenfalls gestützt. Für die Datenschutzfolgenabschätzung der Daten der Studenten wird als Ermächtigungsgrundlage zur Erhebung von Daten das Sächsisches Datenschutzdurchführungsgesetz mit den §§ 2 bis 6 SächsDSDG gesetzt.

# 3 Datenschutzfolgenabschätzung nach Artikel 35 EU-DSGVO

## 3.1 Allgemeine Funktionsweise

„Eine Datenschutz-Folgenabschätzung (DSFA) ist ein Instrument, um das Risiko zu erkennen und zu bewerten, das für das Individuum in dessen unterschiedlichen Rollen (als Bürger, Kunde, Patient etc.) durch den Einsatz einer bestimmten Technologie oder eines Systems durch eine Organisation entsteht.

Ziel einer DSFA ist es, Kriterien des operationalisierten Grundrechtsschutzes zu definieren, die Folgen von Datenverarbeitungspraktiken möglichst umfassend zu erfassen sowie objektiv und nachvollziehbar mit Blick auf die verschiedenen Rollen und damit verbundenen Interessen so zu bewerten, dass typischen Angriffen durch Organisationen mit adäquaten Gegenmaßnahmen begegnet werden kann.“[10]

Vorab ist zu sagen, dass die Datenschutzfolgenabschätzung für das deutsche Recht keine komplette Neuheit darstellt. Bereits aus dem § 67 Bundesdatenschutzgesetz ist eine Abschätzung von Folgen für die Rechte und Freiheiten der Betroffenen gefordert. Diese leicht abgeschwächte Form war weniger umfassend, als der Art. 35 der Europäischen Datenschutzgrundverordnung, jedoch von Sinn, Zweck und Umsetzung sehr ähnlich.

Das allgemeine Ziel der Datenschutzfolgenabschätzung ist die Machtasymmetrie zwischen Unternehmen/Verwaltung und einer natürlichen Person auszugleichen. Hierbei soll angestrebt werden, dass die notwendigen Daten vorliegen, aber nur solange diese auch benötigt werden. Die DSFA kann damit als ein Instrument angesehen werden, welches die Datenverarbeitung beschreibt, die Rechtmäßigkeit dieser belegt und den Umgang mit Gefahren sowie Abhilfemaßnahmen dokumentiert. Es dient damit nicht nur dem Schutz der Betroffenen, sondern gleichzeitig zur Absicherung der Unternehmen/Verwaltung im Falle eines Datenverlustes. [11]

Das Prinzip der Datenschutzfolgenabschätzung ist schon länger im deutschen Recht verankert und mit Hilfe der EU-DSGVO sowie dessen Art. 35 nun weit-

[10] Bieker, et. al., White Paper Datenschutz-Folgenabschätzung. 2016, S. 5
[11] vgl. Bieker, et. al., 2016, S. 5

reichender beschrieben. Vor allem der Anwendungsbereich und die Durchführung wurden angepasst und verschärft.

Ob eine DSFA notwendig ist, kann aus der Verordnung abgelesen werden. Im Art. 35 Abs. 3 EU-DSGVO ist eine nicht abschließende Liste beschrieben, wann eine Abschätzung der Folgen unumgänglich ist. Als Erstes sind alle Datenverarbeitungen umfasst, die sich mit einer Bewertung von persönlichen Aspekten einer natürlichen Person beschäftigen, sobald daraus Rechtswirkungen gegenüber dieser Person erfolgen.

Weiterhin sind alle umfangreichen Verarbeitungen besonderer Kategorien von personenbezogenen Daten genannt, ebenfalls erwähnt werden strafrechtliche Verurteilungen und Strafen von natürlichen Personen. Als letzter Punkt der Aufzählung wird die Überwachung öffentlich zugänglicher Bereiche als erforderlich aufgeführt.

Ein Vorteil der neuen DSFA ist das Zusammenfassen von gleichen und ähnlichen Datenverarbeitungsvorgängen. Sobald zwei oder mehr Verfahren sich so gleich sind, dass in den Punkten der technischen und organisatorischen Maßnahmen, der Risiken und dem Umgang mit den Restrisiken in gleicher Weise umgegangen wird, kann dies in einer DSFA beschrieben werden.[12]

Im Art. 35 Abs. 7 EU-DSGVO sind die Mindestanforderungen einer Datenschutzfolgenabschätzung aufgezählt. Im Vergleich zur älteren Version müssen nun neben der systematischen Beschreibung des Verarbeitungsvorganges und dem Zweck der Verarbeitung ebenfalls die verfolgten Interessen des Verantwortlichen aufgelistet werden. Die Notwendigkeit und Verhältnismäßigkeit muss im Bezug auf den Zweck nachgewiesen werden. Einer der wichtigsten Punkte ist die Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person. Folglich sind die Abhilfemaßnahmen und getroffenen Sicherheitsvorkehrungen aufzulisten sowie der Nachweis zu erbringen, dass alles rechtmäßig eingehalten wurde. Neu hinzugekommen sind die umfangreichen Rechenschaftspflichten des Verantwortlichen der Datenverarbeitung gegenüber dem Betroffenen.[13]

In den folgenden Abschnitten werden weitere Schritte beschrieben, welche nicht immer zwangsläufig notwendig sind, jedoch bei besonderen Umständen

[12] vgl. Härting, 2016, S. 10f.
[13] vgl. Härting, 2016, S. 12

Beachtung finden müssen. Die DSFA wird vom Art. 40 EU-DSGVO nochmals eingeschränkt. Es müssen die darin aufgeführten Verhaltensregeln beachtet werden und immer wieder auf den Zweck und die Notwendigkeit der Datenerhebung sowie der Datenverarbeitung verwiesen werden. In einigen Fällen kann es vorkommen, dass der Standpunkt der betroffenen Person eingeholt werden muss. Zum Schluss muss immer, wenn eine Änderung in den Risiken eintritt, geprüft werden, inwieweit dies die DSFA beeinflusst. Haben sich die Risiken in solch einer Art und Weise geändert, dass die getroffenen Abhilfemaßnahmen nicht mehr zielführend sind, muss eine Anpassung stattfinden. Sollten die Risiken sinken, sind zumeist keine weiteren Änderungen notwendig, bei einer Erhöhung können jedoch neue Maßnahmen und ein veränderter Umgang mit Restrisiken folgen.

## 3.2 Ablauf einer DSFA

Für den Ablauf einer Datenschutzfolgenabschätzung sind vier Schritte einzuhalten. Zuerst muss die DSFA vorbereitet werden, anschließend findet mit der Durchführung der zweite Schritt statt. In der anschließenden dritten Phase spricht man von der Umsetzung und abschließend erfolgt eine Überprüfung. Diese vier Punkte sind jedoch keineswegs linear aufeinander aufgebaut, sondern viel mehr als ständiger Kreislauf zu betrachten. Nach der Überprüfung folgt, insofern sich Änderungen ergeben, erneut die Vorbereitung einer neuen DSFA. Hierbei kann auf die alten Sachverhalte, Maßnahmen und Dokumentationen zurückgegriffen werden, jedoch müssen die geänderten Bereiche angepasst werden.[14]

*Schritt 1: Vorbereitung*

Für die Durchführung einer Datenschutzfolgenabschätzung müssen einige Punkte vorbereitet werden. Als Erstes sollte klar sein, wer für die Erstellung zuständig ist. Daher sollte der erste Schritt die Bildung eines DSFA-Teams sein, welches sowohl aus Mitgliedern mit Datenschutzwissen besteht, als auch aus Mitgliedern, die Kenntnisse von den benötigten Fachprogrammen besitzen. Anschließend sollte die Prüfplanung erfolgen, bei der alle Mitwirkenden und benötigten Methoden des Projektmanagements niedergeschrieben werden und für den Verlauf der DSFA geordnet werden. Daraufhin ist es sinnvoll den Beurteilungsumfang festzulegen. Es sollten dabei die wichtigsten

[14] vgl. o. V.: Kurzpapier Nr. 5, 2018, S. 2

Verarbeitungsvorgänge herausgearbeitet werden, die im folgenden Beachtung finden müssen. Eventuell besteht die Notwendigkeit die betroffenen Personen, von denen die personenbezogenen Daten verarbeitet werden, mit einzubeziehen und sich deren Standpunkt einzuholen. Als nächster Punkt steht die Bewertung der Notwendigkeit bzw. Verhältnismäßigkeit der Datenverarbeitung in Bezug auf ihren Zweck. Zu achten ist dabei darauf, dass die erhobenen Daten zielführend für den angegebenen Zweck sind und inwieweit der bewirkte Eingriff die Rechte und Freiheiten des Betroffenen beeinflussen. Ein weiterer wichtiger Aspekt ist die Rechtsgrundlage, auf der die Datenerhebung beruht. Für die Datenerhebung von natürlichen Personen gilt weiterhin der Grundsatz des Erlaubnisvorbehaltes. Somit dürfen keine Daten erhoben werden, sofern nicht ein Gesetz dies erlaubt.[15]

*Schritt 2: Durchführung*

Im Schritt der Durchführung werden die Daten und Verarbeitungsvorgänge konkreter betrachtet und vor allem die Gefahren für mögliche Verluste oder von Angriffe identifiziert sowie geeignete Abhilfemaßnahmen gesucht, um den notwendigen Schutz zu gewährleisten. Die Risikoquellen sollten vorab grob umrissen und potentielle Gefahren begründet werden, ebenso sind die Wahrscheinlichkeiten für ein Eintreten abzuschätzen. Ableitend aus der Modellierung der Risikoquellen sollte das Risiko für die Rechte und Freiheiten der Betroffenen eingeschätzt werden. Die Schäden für die natürlichen Personen können dabei in physischer, materieller oder immaterieller Form auftreten. Nach der Identifikation der Risiken werden geeignete Abhilfemaßnahmen gesucht, damit die ermittelten Risiken nicht eintreten können. Ein besonderer Fokus liegt hier auf den technischen und organisatorischen Maßnahmen, welche seitens der Unternehmen/Verwaltung getroffen werden können.

Insofern all diese Schritte abgehandelt sind, wird dies im DSFA-Bericht festgehalten. Darin befinden sich eine systematische Beschreibung der geplanten Verarbeitungsvorgänge, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und die Beurteilung der Risiken mit den Abhilfemaßnahmen zur Risikoeindämmung.

Er dient damit als eine Zusammenfassung mit einer gezielten Darstellung der Verfahren. Des Weiteren spielt er eine wichtige Rolle für den Nachweis sei-

[15] vgl. o. V.: Kurzpapier Nr. 5, 2018, S. 2f.

tens der Unternehmen/Verwaltung, damit man den neuen Anforderungen der EU-DSGVO gerecht wird.[16]

*Schritt 3: Umsetzung*

In der Phase der Umsetzung werden die Vorüberlegungen und beschlossenen Änderungen nach und nach verwirklicht. Alle Schritte befinden sich zeitlich vor der eigentlichen Datenverarbeitung, damit ein sicheres System für die zu schützenden Daten bereitsteht und keine Datenverluste auftreten. Gemäß der Regelungen aus der EU-DSGVO dürfen die Daten nicht eher verarbeitet und genutzt werden, bis die Risiken bekannt sind, die notwendigen Maßnahmen getroffen worden und der Umgang mit den Restrisiken geklärt ist. Als Erstes steht die Umsetzung der Abhilfemaßnahmen gegen die Risiken auf dem Plan. Folgend werden diese dann getestet und auf ihre Wirksamkeit geprüft. Bei Fehlern oder Lücken im System muss nochmals nachgebessert werden, bis dann die Dokumentation folgt. In die Dokumentation kommen alle Nachweise, welche zur Einhaltung der EU-DSGVO dienen, damit auf Nachfrage der Rechenschaftspflicht seitens der Unternehmen/Verwaltung Folge geleistet werden kann. Insofern alle Schritte ordnungsgemäß ausgeführt sind, kann die Freigabe für die Verarbeitungsvorgänge durch die zuständige Aufsichtsbehörde erteilt werden.[17]

*Schritt 4: Überprüfung*

Zum Abschluss der DSFA steht eine komplette Überprüfung aller Maßnahmen und Verfahren an. Sinnvoll kann dabei das Einbeziehen von Dritten sein, damit alle Einzelheiten durch einen Unabhängigen überprüft werden. Ebenso muss der Datenschutzbeauftragte in das ganze Verfahren involviert werden.

Abschließend ist eine Fortschreibung der DSFA unumgänglich, da diese kein einmaliger Prozess ist, sondern ein begleitender Prozess. Es ist wichtig, dass bei Änderungen im Bereich der Technik oder der Risiken eine Anpassung stattfindet. Ebenfalls muss der Umgang mit den Restrisiken geklärt sein. Im Falle eines immer noch hohen Risikos trotz aller technischen und organisatorischen Maßnahmen muss die zuständige Aufsichtsbehörde konsultiert werden. Hier können verschiedene Resultate folgen, einerseits wird das Risiko als annehmbar eingeschätzt und in Kauf genommen oder andererseits eine Un-

[16] vgl. o. V.: Kurzpapier Nr. 5, 2018, S. 3f.
[17] vgl. o. V.: Kurzpapier Nr. 5, 2018, S. 4

tersagung für diese spezifischen Datenverarbeitungsvorgänge ausgesprochen werden. Bei einer Untersagung muss gegebenenfalls ein neues Verfahren oder neue Technik eingeführt werden, um den Ansprüchen an den Datenschutz gerecht zu werden. [18]

### 3.3 Umgang mit Restrisiken

Im Umgang mit hohen Restrisiken muss in jedem Fall die Aufsichtsbehörde nach Art. 36 EU-DSGVO mit einbezogen werden. Dieser werden dabei alle bestehenden hohen Gefahren offengelegt und jede Einzelheit des Verarbeitungsvorganges dargestellt. Danach wird zusammen besprochen, welche Möglichkeiten bestehen das Verfahren abzuändern, die Gefahren weiter zu minimieren oder ob die Risiken akzeptiert werden können. Als Resultat gibt es nur zwei Möglichkeiten, entweder wird der Prozess der Datenverarbeitung gestattet und die verbleibenden Restrisiken hingenommen oder der Verarbeitungsvorgang wird durch die Aufsichtsbehörde solange untersagt, bis ein akzeptables Maß an Restrisiken besteht. Hierbei übt die Aufsichtsbehörde ihre Befugnisse nach Art. 58 EU-DSGVO aus und kann den Verantwortlichen des Datenverarbeitungsvorganges verwarnen, anweisen etwas zu ändern oder auch den Vorgang untersagen.[19]

### 3.4 Folgen bei Verstößen

Die Folgen bei Verstößen gegen die EU-DSGVO sind vor allem finanziell angesetzt. Dabei wurden die Strafzahlungen im Vergleich zum BDSG deutlich erhöht und somit vor allem für große Unternehmen innerhalb und außerhalb der Europäischen Union verschärft. Alle Verstöße gegen das Datenschutzrecht werden im Art. 83 EU-DSGVO aufgelistet und mit Strafen beziffert. Die höchste zu verhängende Geldstrafe beträgt dabei nach Art. 83 Abs. 5 und 6 EU-DSGVO 20.000.000 Euro oder 4% des gesamten weltweiten erzielten Jahreseinkommens des vorangegangenen Geschäftsjahres, je nachdem was höher ist. Ein essentieller Grund für die Erhöhung der Geldstrafen liegt in dem Verhalten der Unternehmen in den letzten Jahren, wobei immer wieder datenschutzrechtliche Verstöße in Kauf genommen worden, da die Strafen nicht den Profit geschmälert haben.[20]

[18] vgl. o. V.: Kurzpapier Nr. 5, 2018, S. 4f.
[19] vgl. o. V.: Kurzpapier Nr. 5, 2018, S. 5
[20] vgl. Härting, 2016, S. 65

Die Absicht hinter der drastischen Erhöhung der Strafzahlungen liegt vor allem darin, dass in der gesamten Europäischen Union ein einheitlicher Standard für den Datenschutz geschaffen werden soll. Den Unternehmen soll die Möglichkeit genommen werden, sich in Länder innerhalb und außerhalb der EU zurückzuziehen, in denen niedrigere Anforderungen an den Schutz der Daten herrschen. Mit Hilfe des Marktortprinzips sind auch ausländische Unternehmen, die aber einen Markt im Bereich der EU besitzen, gefordert an ihren Datenschutzbestimmungen zu arbeiten. Somit soll erzielt werden, dass Verstöße nicht mehr in Kauf genommen werden, um durch Einsparungen im Bereich des Datenschutzes einen größeren Profit auf Kosten der Betroffenen zu erlangen.

# 4 Durchführung einer Datenschutz-Folgenabschätzung an der HSF Meißen mit den Daten der Studenten

## 4.1 Art der gespeicherten Daten

Für ein Studium an der Hochschule Meißen muss ein Bewerbungsverfahren durchlaufen werden, in dem die zukünftigen Studenten sich über ein Online-Bewerbungsverfahren anmelden können. Dabei werden die Daten von den Bewerbern selbstständig in das Formular[21] eingetragen und an dich Hochschule gesendet, um sich aus allen Bewerbungen die in Frage kommenden heraus zu suchen. Es müssen für ein Studium an der HSF Meißen einige Voraussetzungen erfüllt sein, welche dadurch herausgestellt werden. Ebenfalls werden die persönlichen Daten abgefragt, um eine eindeutige Identifizierung der Person bei dem Auswahlverfahren und den Bewerbungsgesprächen zu garantieren. Ein weiterer Punkt sind die Fragen zu einer Behinderung des Bewerbers, damit alle Regelungen des Allgemeinen Gleichbehandlungsgesetzes eingehalten werden können und ein Nachteilsausgleich möglich ist.

Besonders kritische Daten, wie beispielsweise die ethnische Herkunft, Religion, politische Meinung oder auch Sexualität, sind für die Hochschule nicht von Bedeutung und werden auch nicht abgefragt. Damit schützt sich die HSF Meißen (FH) selbst vor Verstößen gegen die EU-DSGVO. Bei dieser werden solche Daten als eine besondere Kategorie eingeordnet, welche besonders zu schützen sind. Indem diese Art von Daten nicht erfragt wird, müssen diese auch nicht geschützt werden.

Die abgefragten Daten aus dem Bewerbungsverfahren sind vor allem persönliche Daten, welche die Hochschule von den Studenten benötigt. Hinzu kommen im Verlauf des Studiums noch die Prüfungsergebnisse und die Krankenbescheinigungen, welche die Hochschule aufbewahrt.[22]

Alle diese Daten erfüllen ihren eigenen Zweck im Verlauf des Studiums. Vor allem die persönlichen Daten, wie Name, Vorname, Adresse und Geschlecht dienen dem Abgleich der Person für die Prüfungen. Bei diesen besteht ein gesteigertes Interesse eindeutig bestimmen zu können, dass wirklich der Studierende im Prüfungsraum sitzt und beispielsweise selbst die Klausur bearbei-

[21] siehe Anhang 1: Online-Bewerbungsformular der HSF Meißen (FH)
[22] vgl. Vetter, 2016

tet. Dadurch kann ein Betrug, der sich auf das spätere Arbeitsverhältnis auswirken kann, vermieden werden. Ein weiterer Punkt bezieht sich auf die Nachvollziehbarkeit bei Verstößen gegen die Haus- und Prüfungsordnung. In solchen Fällen sollen die Verantwortlichen bestraft werden können und gegebenenfalls entstandene Schäden ersetzt werden. Eine gesteigerte Relevanz gilt im Falle der Hochschule Meißen für die Hardware in den Informationstechnik-Räumen. Da die Computerkabinette durch ein eigenes System gesichert sind, müssen auch die Ein- und Ausgänge aus diesen Räumen überwacht werden. Mit einem Chip, der definitiv einem bestimmten Studenten zugewiesen werden kann, wird dies nachvollzogen. Um in einen solchen Raum oder in die Hochschule bei Nacht eintreten zu können, muss dieser Chip als Schlüssel verwendet werden. Die gesamten Bewegungen der Studenten in den nicht offiziellen Zeiten (16:30 bis 7:00 Uhr) werden dabei aufgezeichnet und bei Auffälligkeiten entgegengewirkt.

Die Adresse, Telefonnummer und E-Mail Adresse werden von den Studierenden aufgenommen, damit diese dauerhaft erreichbar sind. Die Bescheide, welche für die Zulassung, die nicht bestandenen Prüfungen oder Verstöße gegen die Studenten erlassen werden, müssen einer Postadresse zugesandt werden können. Die E-Mail und Telefonnummer sind eher im Bereich einer schnellen Kommunikation und der Vernetzung im Studentenportal „Antrago“ nützlich. Hier wird es sowohl der Verwaltung und den Dozenten ermöglicht kurzfristige Änderungen bekannt zu geben als auch den Studenten sich selbst zügig Informationen von selbigen einzuholen. Ebenfalls ist es den Studenten selbst überlassen, welche E-Mail und Telefonnummer diese angeben, womit auch die Möglichkeit einer Dienstanschrift eröffnet wird. In der heutigen Zeit der Digitalisierung zählen solche Daten unter die Kategorie unerlässlich, weil sonst eine Verzögerung in Dienstwegen auftreten kann und ein großer Teil der Flexibilität wegfällt. Des Weiteren werden in den Bereichen des öffentlichen und wirtschaftlichen Sektors immer Wege zur Steigerung von Effektivität und Effizienz gesucht, worunter vor allem die schnelle und unkomplizierte Kommunikation einen essentiellen Anteil bereitstellt.

In der Studentenakte befinden sich alle abgefragten Daten und werden auf einem Stammdatenblatt[23] zusammengefasst. Dieses Blatt wird am Anfang jeden Studienjahres aktualisiert und kann auch durch den Studenten jederzeit angepasst werden.

[23] siehe Anhang 2: Stammdatenblatt aus der Studentenakte der HSF Meißen (FH)

## 4.2 Verwendung der gespeicherten Daten

An der Hochschule in Meißen werden die erhobenen Daten auch verarbeitet und genutzt. In meiner Bachelorarbeit gehe ich dabei nur auf die Verarbeitungsprozesse in der Studentenakte und der Prüfungsakte ein. Weitere Betrachtungen an Verfahren der Bibliothek oder der Mensa lasse ich außen vor. In der Handakte befinden sich erstmal alle Daten, die zu Beginn des Studiums, in der Phase der Bewerbung abgefragt wurden. Diese werden dabei am ersten Tag des Studiums erneut abgefragt und auf Aktualität geprüft, welches selbstständig durch die Studierenden durchzuführen ist. Alle Punkte werden gemeinsam auf einem allgemeinen Datenblatt zu einer bestimmten Person als Deckblatt für die Akte abgelegt. In der Prüfungsakte gibt es ebenfalls dieses Datenblatt mit den wichtigsten Informationen zur Person, um eine eindeutige Zuordnung garantieren zu können. Im Verlauf des Studiums kommen in die Handakte die Krankenbescheinigungen der Studenten hinzu und besondere Anträge für beispielsweise freie Tage, die Sommerfakultät oder sportliche Wettbewerbe. Im Bereich der Prüfungsakte werden alle Prüfungsergebnisse, welche sich im Studium ansammeln, abgelegt und daraus am Ende das Abschlusszeugnis erstellt.

Unter die wichtigsten Verwendungszwecke der personenbezogenen Daten der Studenten, zählt die Zuordnung von geschriebener Prüfung zum jeweiligen Studierenden. Damit werden die Prüfungsleistungen nicht verfälscht und Verwechslungen oder sogar Betrug kann ausgeschlossen werden. Des Weiteren ist sichergestellt, dass die Ergebnisse nach der Auswertung richtig adressiert sind. Bei den bestanden Prüfungen werden diese den einzelnen Personen über die ILIAS-Lernplattform freigeschaltet, sodass jeder nur seine eigenen Leistungen einsehen kann. Bei einer nicht bestandenen Prüfung wird der Student per Bescheid an seine Wohnadresse darüber informiert, dass eine Nachprüfung stattfindet. Darin befinden sich erstmal eine allgemeine Informationen für den Betroffenen, dass eine unzureichende Punktzahl in einer oder mehreren Modulprüfungen erlangt wurde und eine Rechtsbehelfsbelehrung. In einem zweiten Schreiben werden die Termine mit Ort und Datum für die Nachprüfung mitgeteilt, in der dem Studierenden die Möglichkeit gegeben wird, die genannten Prüfungen zu wiederholen.

Ein weiterer Verwendungszweck ist die Zuordnung der Studenten mit dem Chip, welcher Zugang zur Hochschule außerhalb der offiziellen Zeiten gewährt

und den Eintritt in die Computerräume ermöglicht. Hierbei wird auf dem Chip vermerkt, welcher Studierende diesen ausgeteilt bekommen hat und von ihm im Gegenzug eine Unterschrift entgegengenommen. Damit stellt die Hochschule Meißen sicher, dass Unberechtigte nicht unbeaufsichtigt in die Einrichtung und die IT-Räume eintreten und eventuell Schäden anrichten. Somit dient dies dem Schutz der Institution und der darin befindlichen Gegenstände sowie der Daten der Studenten und Dozenten.

Ebenfalls werden die Daten dazu verwendet die Profile auf ILIAS, insbesondere das Studentenportal „Antrago“ für die Studierenden einzurichten. Diese sind für einen modernen Unterricht unerlässlich. Es wird den Studenten die Chance eröffnet außerhalb des Unterrichtes und zu selbst gewählten Zeiten das Selbststudium anzutreten und sich durchgängig fortzubilden. Weiterhin wird eine unkomplizierte Kommunikation zwischen Studenten und anderen Studenten als auch den Dozenten ermöglicht. Von beiden Seiten können Inhalte, welche dem Studium dienlich sind, bereitgestellt werden. Die Prüfungsergebnisse und die Auswahl der Module im fünften Semester werden ebenfalls über diese Portale bereitgestellt. Damit sind nach der Auswertung für alle Studenten ihre eigenen Ergebnisse einzusehen und für die Auswahl der Wahlmodule ist es nicht notwendig an der Hochschule zu sein, sondern diese können bequem vom heimischen Rechner abgehandelt werden.

Weitere Verwendungen sind die Bibliotheken-Karte und der Mensachip, welche ebenfalls auf eine bestimmte Person zugeschnitten sind. Auf diese möchte ich im Folgenden nicht weiter eingehen, da diese nicht zwangläufig mit der Studentenakte und der Prüfungsakte in Verbindung stehen.

Meine Bachelorarbeit und die damit verbundene Datenschutz-Folgenabschätzung beziehen sich ausschließlich auf die Daten der Studierenden, damit der Rahmen eingehalten werden kann und eine genaue Betrachtung ermöglicht wird. Dabei lasse ich die Daten der Mitarbeiter der Hochschule Meißen (FH) außen vor, sowie die Daten der Dozenten, welche haupt- und nebenamtliche Tätigkeiten verrichten. Ebenfalls lasse ich die Verarbeitungsvorgänge, die in der Bibliothek, Mensa und weiteren Nebeneinrichtungen stattfinden, nicht mit in meine Betrachtungen einfließen. Alle hier aufgeführten Daten dienen der Erfüllung der eben genannten Zwecken. Daten die nicht mehr gebraucht werden, werden ohne lange Aufbewahrungszeiten gelöscht und nicht ohne Recht einbehalten. Zum Schluss des Studiums werden alle Daten

vernichtet, die nicht benötigt werden, um ein Zeugnis zu erstellen. Jene Informationen zur Person, die eine eindeutige Identifizierung von Student und Zeugnis erlauben, müssen jedoch nach der § 32 Abs. 2 Sächsische Ausbildungs- und Prüfungsordnung allgemeiner Verwaltungsdienst und sozialwissenschaftlicher Dienst für 50 Jahre aufbewahrt werden. Unter diese zählen der Name, der Vorname, der Geburtsort und der Geburtstag.

Außer dem ZIT haben alle zuständigen Mitarbeiten des jeweiligen Fachbereiches Zugriff auf die Studentenakte und die Prüfungsakte. Dies ermöglicht ein flexibles Reagieren der Angestellten an der Hochschule und eine Vorkenntnis von Behinderungen, welche den gegenseitigen Umgang erleichtern. Ebenfalls kann bei Beschwerden genauer darauf geachtet werden, welche Besonderheiten vorliegen. Für die Raum- und Kursplanung, für die das ZIT zuständig ist, braucht es keinerlei Informationen über Behinderungen der Studenten. Die Hochschule ist größtenteils barrierefrei errichtet und stellt Mittel und Wege zur Verfügung mit jeglichen Behinderungen alle Räume zu erreichen.

Unter die folgenden externen Empfänger fallen nur Einrichtungen und Institutionen des Freistaates Sachsen. Es sind die Einstellungsbehörden der einzelnen Studenten und Fachbereiche, die Aufsichtsbehörde der Hochschule Meißen, das Landesamt für Steuer- und Staatsfinanzverwaltung und die Staatsministerien, jeweils für die spezifischen Fachbereiche, Allgemeine Verwaltung, Finanz- und Steuerverwaltung, Rechtspflege, Sozialverwaltung und Sozialversicherung.

Eine Datenübermittlung in ein Drittland oder eine internationale Organisation findet nicht statt. Jegliche Datenübertragungen bleiben dabei im Freistaat Sachsen und den damit verbundenen sächsischen Verwaltungsnetz. Hierbei gelangen die Daten nicht in den öffentlichen Bereich und sind somit zusätzlich geschützt.

Die Datenlöschung richtet sich für die Studenten der Hochschule Meißen nach den allgemeinen Ausbildungs- und Prüfungsordnungen, den Vorschriften des Archivgesetzes und der Registraturordnungen mit Ausnahme der Daten, die für eine erneute Ausstellung eines Zeugnisses benötigt werden. Die personenbezogenen Daten der betroffenen werden somit gelöscht, sobald der Zweck der Speicherung für die Hochschule Meißen entfällt. Dabei gelten diese Regelungen für alle Fachbereiche zu gleichen Teilen und ohne Ausnahmen. Mit den Maßnahmen wird eine unberechtigte Speicherung von Daten vermie-

den und dem Grundsatz der Datenminimierung entsprochen. Für die Daten der Studenten bedeutet dies, dass sofort nach der Zeugnisübergabe die Handakten aussortiert werden. Es werden alle nicht mehr notwendigen Daten vernichtet und gelöscht. Lediglich ein kleines Datenblatt mit den Informationen zur eindeutigen Zuordnung von Bachelor- oder Diplomarbeit zum jeweiligen Studenten wird aufgehoben.[24]

### 4.3 Vorbereitung der DSFA

Für meine Datenschutz-Folgenabschätzung nehme ich mir das Verfahren der Studentenakten der Hochschulstudenten. Auf Grund des ähnlichen Aufbaues mit der Prüfungsakte und den ähnlichen Inhalten, können hier einige Punkte zusammengefasst werden und es bietet sich eine Möglichkeit des Vergleiches.

Im Folgenden muss zuerst die Frage gestellt werden, ob diese beiden Verfahren überhaupt einer DSFA bedürfen und die gegebenen Voraussetzungen erfüllen. Alle Bedingungen, wann eine DSFA notwendig ist, finden sich im Artikel 35 EU-DSGVO. Die Hochschule Meißen nimmt bereits bei der Bewerbung der Studenten deren Daten auf, worunter auch personenbezogene Daten fallen und speichert diese ab, um daraus die geeignetsten Bewerber auszuwählen. Somit liegt ein Verarbeitungsprozess in Form des Profiling bzw. eine umfangreiche Verarbeitung von personenbezogenen Daten vor, womit zwangsläufig für diese Prozesse eine DSFA durchzuführen ist. Hierbei werden die Daten in einem Online-Formular abgefragt und auf den Servern der Hochschule gespeichert. Somit werden von allen, die sich an der Hochschule Meißen für ein Studium bewerben, die eben aufgeführten Daten abgefragt und im Verlauf des Bewerbungsprozesses analysiert und ausgewertet. Hinzu kommen die Daten aus dem Bewerbungstest, in dem allgemeine Fähigkeiten geprüft werden. Zum Schluss des Bewerbungsverfahrens kommen noch die Bewertungen aus den Bewerbungsgesprächen. Aus allen gesammelten Informationen zu den zukünftigen Studenten werden die Besten für die jeweiligen Fachbereiche herausgesucht. Ebenfalls befinden sich alle diese Daten in den Studentenakten und werden dort aufbewahrt, bis das Studium endet. Die Daten der nicht angenommenen Bewerber werden sofort und unverzüglich gelöscht. Eine weitere Verarbeitungsform ist die Personalisierung der Chips mit denen die Studenten Zugang zur Hochschule und den IT-Räumen bekommen.

[24] siehe Anhang 3: Verarbeitungstätigkeiten an der HSF Meißen (FH)

Dabei wird jedem einzelnen Studenten ein Chip zugewiesen, für welchen er die Entgegennahme per Unterschrift bestätigt.

Damit steht außer Frage, dass für die Verarbeitungsprozesse der Studentenakte eine DSFA notwendig ist. Unter den Daten, welche die Hochschule von all ihren Studenten speichert, sind auch personenbezogene Daten, die besonders schützenswert sind. Im gleichen Schritt muss ein Verfahrensverzeichnis[25] erstellt werden, in dem alle relevanten Informationen zum Verarbeitungsprozess und Teile des Datenschutzes aufgeführt werden.

Ein weiterer Punkt der Vorbereitung der DSFA für die Daten der Studenten an der Hochschule Meißen ist es, den Anspruch an diese Datenschutz-Folgenabschätzung zu klären. Im Rahmen meiner Bachelorarbeit soll diese eine Standard-Datenschutz-Folgenabschätzung[26] werden. Mit dieser soll der EU-DSGVO und den damit verbundenen Zweck der Dokumentation und des Nachweises nachgekommen werden. Hierbei werden die praxisrelevanten Gefahren dargestellt und alle getroffenen Maßnahmen vom Verantwortlichen aufgelistet, damit nachvollziehbar ist, wie viel für den Schutz der Daten unternommen wurde und welche Folgen für die Betroffenen bei einem Verlust auftreten.

Zum Punkt der Teambildung, wie in Punkt 3.2 im Schritt 1 Vorbereitung angesprochen, bin ich als Verfasser dieser Bachelorarbeit allein zu benennen. Ich habe dabei Gespräche mit den jeweiligen zuständigen Mitarbeitern geführt und versucht deren Wissen hier zu bündeln. Somit ist eine explizite Benennung eines Teams im Rahmen der Bachelorarbeit nicht möglich.

Weiterhin sind auch die Betroffenen nicht weiter einzubeziehen, da diesen eine umfangreiche Information zu diesem Thema durch die Hochschule zugekommen ist und bei Bedarf mit den für den jeweiligen Fachbereich Verantwortlichen ein Gespräch geführt werden kann.

Im Bereich der rechtlichen Grundlage habe ich in meinen Recherchen eine Lücke gefunden, da es für die Hochschule Meißen keine explizite Ermächtigungsgrundlage zur Datenerhebung gibt. In allen einschlägigen Gesetzen wird nur die Datenverarbeitung erlaubt und eingeschränkt, jedoch keine Information zur Erhebung der notwendigen Daten geliefert. Im Umkehrschluss kann

[25] siehe Anhang 6: Verfahrensverzeichnis für die Studentenakte der HSF Meißen (FH)
[26] vgl. Bieker, et. al., 2016, S. 21

davon ausgegangen werden, dass eine Datenerhebung gerechtfertigt ist, wenn die Verarbeitung erlaubt wird, weil ohne vorhandene Informationen über die Studenten keine Verarbeitung stattfinden kann. Auf Grund dessen kann eine implizite EGL aus den Gesetzen herausgelesen werden.

### 4.4 Durchführung der DSFA

Nachdem die Vorbereitungen für die Datenschutz-Folgenabschätzung abgeschlossen sind und die benötigten Informationen eingeholt worden, kann die eigentliche Durchführung starten. Hierbei ist es vor allem wichtig, die Einzelheiten genau zu differenzieren und alles zu dokumentieren, damit der Nachweispflicht Folge geleistet werden kann. Die komplette DSFA wäre nicht sinnbringend, wenn diese nicht von einem Dritten im Fall eines Datenverlustes nachvollzogen werden kann oder lückenhaft ist.

Der erste Schritt besteht in der Festlegung der Schutzziele. Für meine Arbeit begrenze ich mich dabei auf die Integrität, die Vertraulichkeit und die Verfügbarkeit[27] der Daten der Studenten an der Hochschule Meißen, da diese auch den allgemeinen Schutz in der Informationssicherheit dienen. Für diese Schutzziele werden im Weiteren die Wahrscheinlichkeiten für den Eintritt einer Verletzung beschrieben und festgelegt. In meiner Arbeit möchte ich vier Stufen für die Wahrscheinlichkeiten prognostizieren. Diese sind in Anlehnung an eine beispielhafte Durchführung einer DSFA von „privacy officers“, einem Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter: vernachlässigbar, eingeschränkt, signifikant und maximal.

[27] vgl. Czernik, 2016

| Beurteilung der Eintrittswahrscheinlichkeit | |
|---|---|
| **Vernachlässigbar** | Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle eines unterstützenden Wertes[8] auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist). |
| **Eingeschränkt** | Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützendes Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist). |
| **Signifikant** | Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle eines unterstützenden Werts auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat). |
| **Maximal** | Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einer öffentlich zugänglichen Lobby). |

**Abbildung 1: Stufen zur Beurteilung der Eintrittswahrscheinlichkeit[28]**

Anhand dieser Tabelle sollen die Begriffe definiert sein und eine Orientierung bieten. Nach dem gleichen Schema werde ich auch die Auswirkungen für die Studenten der Hochschule einordnen. In folgender Grafik werden gleich zu den Eintrittswahrscheinlichkeiten die Einschätzung für die möglichen Auswirkungen aufgelistet und kategorisiert. Zum Schluss der Arbeit werden diese dann in ein Verhältnis gesetzt, um herauszustellen, welche Maßnahmen getroffen werden müssen. Ein großer Fokus wird auf Gefahren mit einer hohen Eintrittswahrscheinlichkeit und die signifikanten Auswirkungen liegen.

| Einschätzung der Auswirkungen | |
|---|---|
| **Vernachlässigbar** | Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können. |
| **Eingeschränkt** | Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können. |
| **Signifikant** | Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können. |
| **Maximal** | Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können. |

**Abbildung 2: Stufen der Beschreibung der Auswirkung[29]**

[28] vgl. o. V.: Datenschutz-Folgenabschätzung : Durchführung einer DSFA am Beispiel Videoüberwachung, 2018, S. 12
[29] vgl. o. V.: Datenschutz-Folgenabschätzung : Durchführung einer DSFA am Beispiel Videoüberwachung, 2018, S. 13

Nachdem die Bewertungsmaßstäbe für die möglichen Gefahren mit deren Auswirkungen geklärt sind, folgen nun die eigentlichen Gefahren für die Daten der Hochschulstudenten.

Für eine ordnungsgemäße Datenschutz-Folgenabschätzung ist es wichtig von vornherein zu wissen, welche Gefahren und Risiken für die Daten der Hochschulstudenten bestehen. Dabei muss darauf geachtet werden, dass die Hochschule eine öffentliche Einrichtung darstellt und somit besonders zu schützen ist. Bei den Gefahren können verschiedene Formen auftreten. Es gibt Gefahren, welche durch Menschen verursacht werden, wie beispielsweise durch einen physischen Einbruch, Diebstahl von Daten bzw. Geräten oder auch Zerstörungen. Weiterhin müssen gleichfalls Angriffe auf die Netzwerke Beachtung finden. Gerade in der Zeit der Digitalisierung gehen physische Attacken immer weiter zurück und verschieben sich in Richtung Hackerangriffe oder Social Engineering. Bei solchen Gefahren liegt der Fokus der Angreifer darauf, möglichst anonym und schnell so viele Daten wie möglich zu beschaffen oder mit gezielten punktuellen Stichen eine spezielle Information zu bekommen. Daraus resultiert die dritte große Gruppe der Risiken, welche bei den Mitarbeitern selbst liegt. Jeder Beschäftigte, der mit den Daten der Studenten arbeitet, muss sich immer absichern, mit wem er spricht und welche Daten er weitergeben darf. Gerade da Mitarbeiter nicht durchgängig überwacht werden, können durch diese auftretenden Fehler und Datenverluste nicht sofort bemerkt und denen entgegengewirkt werden. In diesen Fällen ist der Arbeitgeber in der Pflicht schon bei der Einstellung darauf zu achten, wen er anstellt und während der gesamten Arbeitszeit immer wieder durch Schulungen und Belehrungen solchen Gefahren entgegen zu wirken. Die letzte Gruppe der Gefahren liegt in Naturkatastrophen oder ähnlichen Gegebenheiten, wie Hochwasser, Feuer oder Stromausfälle. Natürlich ist die Eintrittswahrscheinlichkeit für solche speziellen Sachverhalte bedeutend geringer als für andere Risiken, jedoch nicht unbedeutend. Gerade der Standort Meißen mit seiner Nähe zur Elbe, den zahlreichen Überschwemmungen in den letzen Jahren und dem Klimawandel, schließt solche Sachverhalte nicht aus.

Für meine Betrachtung der DSFA mit den Daten der Studenten an der HSF Meißen (FH) möchte ich mich bei den Gefahren vor allem am Gefahrenkatalog des Bundesamtes für Sicherheit in der Informationstechnik orientieren. Daraus werde ich die allgemeinen und wahrscheinlichsten Gefahren, sowie einige speziell für die Hochschule als öffentliche Einrichtung zutreffenden Ge-

fahren heraussuchen. Dabei kann und werde ich nicht auf jedes Detail eingehen, da öfter ähnliche Sachverhalte mit einer einzigen Maßnahme umfasst werden.

Bei den Maßnahmen ziehe ich den BSI-Maßnahmenkatalog[30] heran, in dem für die eben genannten Gefahren Empfehlungen zum Entgegenwirken gegeben werden. Alle Maßnahmen, welche darin verankert sind, gelten nur als grobe Richtlinien und sind nicht abschließend. In der heutigen Zeit wandeln sich viele Faktoren sehr schnell, gerade im Bereich der Technik und der Methoden der Angreifer. Damit sind alle Verantwortlichen selber in der Pflicht für sich passende Vorkehrungen zu treffen, sodass die Daten der Mitarbeiter, Studenten oder Bürger sicher gestellt werden. Dennoch möchte ich im Fall der Hochschule Meißen darauf eingehen, inwieweit sich am BSI-Standard orientiert wird und welche Maßnahmen weitreichend sind. Gerade Punkte in denen die Hochschule extra Arbeit leistet, möchte ich herausstellen und begründen, warum diese betrieben wird.

Aus diesem Katalog habe ich aus meiner Sichtweise die wichtigsten Gefahren für die Hochschule und die Daten der Studenten herausgesucht. Diese beispielhafte Auflistung der Risiken befindet sich im Anhang 4: Gefahren und Maßnahmen nach BSI-Katalog.

Den größten Schutzbedarf haben die personenbezogenen Daten der Studenten, die in beiden Formen von Akten abgespeichert werden. Ein Verlust oder ein Diebstahl kann weitreichende Konsequenzen für den Betroffenen und den Verantwortlichen nach sich ziehen. Zum einen sind die Studenten darin geschädigt, dass ihre komplette Anschrift mit Telefonnummer und E-Mailadresse an Unbefugte gerät und damit die Optionen eines Einbruches, Spamnachrichten oder anderer Angriffe eröffnet wird und gleichzeitig die wichtige Informationen über die Identität preisgegeben sind. Gezielte Angriffe auf die betroffenen Personen sind damit bedeutend einfacher durchzuführen und somit das persönliche Wohl der Studierenden gefährdet. Noch schlimmer ist, wenn dadurch die Familie oder andere nahe stehende Personen mit involviert werden. Ebenfalls kann in manchen Fällen durch das Erlangen von persönlichen Informationen ein Rückschluss auf Passwörter nachvollzogen werden. Sobald

[30] vgl. o. V.: IT-Grundschutz-Kataloge, Datum unbekannt, Gefährdungs- und Maßnahmenkataloge

eine E-Mailadresse für den Angreifer zugänglich ist, können darauf aufbauend andere Accounts, wie zum Beispiel die Konten der sozialen Medien, Einkaufsplattformen bis hin zum Online-Banking-Account gehackt werden. Insofern der Betroffene keine sicheren Passwörter verwendet und nicht rechtzeitig darauf reagiert, kann diesen die Existenzgrundlage geraubt werden.

Zum anderen ist bei einem Verlust der Daten der Verantwortliche in der Pflicht dies zu melden und alles zu unternehmen, um die Daten zurück zu bekommen. Hierbei drohen nach der neuen EU-DSGVO hohe Strafen, insofern nicht alles Mögliche unternommen wurde, damit die Daten nicht verloren gehen bzw. schnellstmöglich die Auswirkungen eingeschränkt werden. Ebenfalls von Bedeutung ist der Krankenverlauf, der sich in der Zeit an der Hochschule ansammelt. Auf Grund der Anwesenheitspflicht in dem dualen Studium sind die Studenten dazu verpflichtet sich bei Fehlstunden oder Fehltagen abzumelden und dies durch ein ärztliches Attest bestätigen zu lassen. Diese Informationen zur Anwesenheit können ein schlechtes Licht auf die Betroffenen werfen und müssen aus diesem Grund genauso sicher verwahrt werden. Gleiches gilt für den Grad der Behinderung der betreffenden Studenten. Solche persönlichen Informationen sind nicht für die breite Öffentlichkeit gedacht und dienen lediglich dem Arbeitgeber zur gerechten Arbeitsplatzgestaltung und damit im Bewerbungsverfahren eine Gleichberechtigung möglich ist.

Somit muss sich die Hochschule Meißen gegen eine Vielzahl an möglichen Gefahren, von denen ich im Folgenden exemplarisch einige aufzählen möchte, wehren. Hierunter zählen vor allem der Diebstahl von Daten durch externe Einflüsse im Sinne von Einbrüchen in die Häuser oder Angriffe auf das Netzwerk, das Erschleichen von Daten durch sogenanntes Social Engineering, bei dem sich Unberechtigte über Anrufe, E-Mails oder persönliche Gespräche Informationen einholen, die nicht für sie bestimmt sind oder auch das Weitergeben von Daten durch nicht geschultes Personal an Unberechtigte.[31]

[31] vgl. o. V.: IT-Grundschutz-Kataloge, Datum unbekannt, Gefährdungs- und Maßnahmenkataloge

| **Beurteilung von Eintrittswahrscheinlichkeiten** | |
|---|---|
| Vernachlässigbar | Zerstörung von Servern / Akten |
| Eingeschränkt | Einbrüche, Diebstahl, physische Angriffe |
| Signifikant | Hackerangriffe, Social Engineering |
| Maximal | Spam |

**Abbildung 3: Beurteilung von Eintrittswahrscheinlichkeiten für die HSF Meißen (FH)**

| **Beurteilung der Auswirkung** | |
|---|---|
| Vernachlässigbar | Verlust der Daten |
| Eingeschränkt | Diebstahl von Namen und Adressen |
| Signifikant | Diebstahl von E-Mailadressen und persönlichen Informationen |
| Maximal | Diebstahl von personenbezogenen Daten mit Abwesenheitsverlauf |

**Abbildung 4: Beurteilung der Auswirkung für die HSF Meißen (FH)**

Die Einordnung der jeweiligen Eintrittswahrscheinlichkeiten und Auswirkungen bezieht sich auf die eben genannten Möglichkeiten zur Verwendung der einzelnen Daten. Somit ist es für die Betroffenen das schlimmste, wenn alle Daten, welche die Hochschule von ihnen speichert, gestohlen werden. Damit sind Angreifer in der Lage sehr genau diese Person nachzustellen und sich Zutritt zu den meisten Accounts zu verschaffen. Weniger schlimm ist der reine Verlust oder Diebstahl von Namen und Adressen, da die Angreifer nicht die gleichen Möglichkeiten haben der Person zu schaden. Gerade ein reiner Verlust von Daten kann meist mit einer erneuten Befragung der Studenten schnell und ohne große Umstände überwunden werden.

Damit liegt das Hauptaugenmerk dieser DSFA auf Angriffen von externen und internen Quellen und wie sich die HSF Meißen (FH) dagegen wehren kann.

## 4.5 Maßnahmen der HSF Meißen (FH)

Die Hochschule Meißen hat viele Maßnahmen getroffen, um jegliche Form des Verlustes von Daten der Studierenden zu vermeiden. Hierbei möchte ich anschließend die Maßnahmen zu den Schutzzielen: Integrität, Vertraulichkeit und Verfügbarkeit zuordnen. Da manche Maßnahmen mehrfachen Schutz generieren, werden diese ihrem Hauptziel zugeordnet, um eine Übersichtlichkeit zu wahren.

Außerdem sind zwei komplett neue Anforderungen an den Datenschutz hinzugefügt worden in Form von Art. 25 EU-DSGVO, der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Unter diesen Punkten verstehen sich die technischen und organisatorischen Maßnahmen, um Verstößen gegen die Datenschutzgrundsätze zu vermeiden. Allen voran steht dabei die Vermeidung von Daten, sodass nur die nötigsten Daten erhoben und gespeichert werden. Weiterhin soll die Transparenz im Bezug auf die Verarbeitung von Anfang an vorliegen.

Bei dem Datenschutz durch datenschutzfreundliche Voreinstellung ist das Ziel, bereits in der Entwicklungsphase von neuen Verfahren oder Technologien darauf zu achten, dass diese allen Anforderungen des Datenschutzes gerecht werden. Ebenfalls sollen die Voreinstellung bereits im Sinne der Sicherheit der Daten sein und nicht erst vom Nutzer von gering auf ausreichend oder maximal erhöht werden.

Diesen beiden Anforderungen wird die Hochschule vor allem damit gerecht, dass sie ein Informationsschreiben herausgegeben hat, in dem alle Ansprechpartner für die einzelnen Fachbereiche und auch alle Maßnahmen ihrerseits zum Schutz der Daten der Studenten aufgelistet sind. Mit diesem Schreiben werden sowohl die Interessen der Hochschule genannt, als auch alle relevanten Informationen hinsichtlich der Speicherung, Verarbeitung und Löschung der Daten.

Maßnahmen zum Schutz der Verfügbarkeit sind für den Fall, dass Systeme ausfallen oder physisch vorliegende Akten abhanden kommen. Hierbei ist vorab zu nennen, dass alle Daten der Studenten in zweifacher Ausführung

vorliegen, zum einen als Handakte und zum anderen auf einem zentralen Speichersystem.[32]

Die physisch vorliegenden Akten werden durch die Einrichtung selbst und den sorgfältigen Umgang der Mitarbeiter geschützt. Es wird ausgeschlossen, dass Unberechtigte diese entsprechenden Räume betreten können oder gar ein Diebstahl ermöglicht wird. Hierfür sind sowohl die Räume an der Hochschule abschließbar als auch die Schieber und Regale, in denen Informationen über die Studenten zu finden sind. Die Hochschule verfügt über einen Sicherheitsdienst, der außerhalb der Lehrzeiten das Gebäude überwacht. Gleichzeitig sind die Eingänge mit einem Sicherheitssystem ausgestattet, welches bei einem Einbruch Alarm schlägt und sofort Polizei und gegebenenfalls Feuerwehr informiert. Eine weitere Form der Absicherung sind die personalisierten Chips, welche sowohl die Identität des Studenten enthalten, als auch seine Zugangsrechte. Somit ist es einem Studenten möglich die Hochschule und IT-Räume auch außerhalb der Unterrichtszeiten zu betreten, jedoch werden die Zeiten protokolliert.

Damit auch bei einem Ausfall der Hardware kein Stillstand eintritt, werden die Daten hardwareunabhängig gespeichert und defekte Geräte können ohne Umstände ausgetauscht werden. Ebenso werden die Daten nach dem Drei-Generation-Prinzip gesichert. Die Daten werden in Abständen täglich, wöchentlich und monatlich auf verschiedenen Datenträgern gespeichert und gesichert, sodass dauerhaft alle Geräte eine gewisse Aktualität haben und ein Zugriff jederzeit möglich ist.[33] Durch eine dauerhafte Überwachung der Funktionsfähigkeit von Hardware wird weiter die Verfügbarkeit abgesichert. Hierbei wird der Administrator unverzüglich über Fehler im System oder Abbrüchen beim Datenabgleich informiert und kann mit Maßnahmen entgegenwirken. Als letzter Punkt zählen die Protokollierung der Verarbeitung der personenbezogenen Daten in der Web-Schnittstelle und die Stammdatenänderung im Studentenportal „Antrago“ als Sicherheitsmechanismen der Hochschule. Mit Hilfe der eben genannten Maßnahmen geht die Hochschule sicher, dass die Daten der Studenten zu jeder Zeit abgesichert und abrufbar sind.

Als nächster Aspekt soll die Integrität der Daten folgen, welches die Veränderung bzw. Verfälschung der Informationen verhindern soll. In diesem Punkt

[32] vgl. o. V.: Verfügbarkeit, 2017
[33] vgl. Stalla, 2016

wird darauf Wert gelegt, dass keine unautorisierten Änderungen an den Systemen vorgenommen werden können. Damit wird eine ständige Auskunft ermöglicht und deren Richtigkeit garantiert.[34]

Dafür arbeitet die Hochschule vor allem mit einer gezielten Vergabe von Rechten durch einen zentralen Administrator. Die Daten werden nur von berechtigten und belehrten Mitarbeitern, welche die entsprechende Zuständigkeit haben, verarbeitet und überwacht. Zur gleichen Zeit werden im Hintergrund Log-Verzeichnisse geführt und die Transaktionen protokolliert. Damit wird ausgeschlossen, dass eine Veränderung von Daten stattfindet, ohne eine Aufzeichnung davon zu haben. Ebenfalls wird das System der Hochschule durch ein Anti-Virensystem geschützt und befindet sich zudem im Sächsischen Verwaltungsnetz. Dieses Netzwerk wird zusätzlich durch den Freistaat Sachsen überwacht und soll Angriffe von außen abschirmen. Die Übertragung von Daten wird zudem SSL-verschlüsselt und es erfolgt zwei Mal täglich ein Abgleich der Daten, damit keine Veränderungen von außen oder innen auftreten können. Weiterhin werden Veränderungen an Kontaktdaten durch die Studentenkanzlei überprüft und nachvollzogen. Die physischen Handakten werden dabei durch die räumliche Struktur geschützt und können zu jeder Zeit mit den Daten auf den Servern abgeglichen werden.

Im Punkt der Vertraulichkeit wird sichergestellt, dass Daten nur an die berechtigten Personen gesandt und weitergegeben werden. Die Weitergabe an Dritte, für die solche Informationen nicht bestimmt sind, ist ausgeschlossen. Auch eine Veröffentlichung ohne die Einwilligung des Betroffenen ist ausgeschlossen und durch Rechtsnormen geschützt. [35]

Um dies zu gewährleisten hat jeder Mitarbeiter einen eigenen Account in der er sich mit seinen personalisierten Zugriffsdaten einloggt. Damit wird eine Nutzung von anderen unrealistisch, insofern die Sicherheitsstandards eingehalten werden. Darunter zählen vor allem sichere Passwörter, eine Belehrung zum Umgang mit seinen eigenen Zugangsdaten und eine geordnete Vertretungsregelung. Weiterhin sollte bei der Verarbeitung von personenbezogenen Daten immer mit Bedacht und nicht übereilt gehandelt werden. Gerade Spam- oder Phishing-E-Mails sind eine große Gefahr für die Vertraulichkeit der Daten. Es ist in einer Verwaltung immer notwendig zu wissen, wer ein berechtig-

[34] vgl. Rassek, 2017
[35] vgl. o. V.: Definition: vertrauliche Daten, Datum unbekannt

tes Interesse an solchen Daten hat und wer nicht. Ebenso wird durch die verschlüsselte Übertragung ein Abhören bzw. Auslesen von E-Mails vermieden. Des Weiteren ist das Abrufen der Webseiten auf denen Passwörter verwendet werden über HTTPS weiter gesichert.

Eine Testphase der gesamten Maßnahmen benötigt die Hochschule Meißen nicht, da die meisten technischen und organisatorischen Maßnahmen bereits länger im Einsatz sind und größtenteils aktualisiert worden. Die HSF Meißen (FH) als eine Einrichtung des öffentlichen Rechts hegte bereits vor der Veröffentlichung der EU-DSGVO einen sicheren und geschützten Umgang mit den Daten der Studenten. Ein Verstoß gegen das Bundesdatenschutzgesetz hätte die Vorbildwirkung der Hochschule als eine Behörde des Freistaates Sachsen geschmälert.

Mit all diesen aufgezählten Maßnahmen schützt sich die Hochschule gegen Datenverluste jeglicher Art, egal ob intern oder extern, wobei auch die Infrastruktur der Netzwerke im Freistaat Sachsen einen wichtigen Anteil leistet.

### 4.6 DSFA-Bericht

Zum Abschluss der Datenschutzfolgenabschätzung muss eine ordentlich geführte und nachvollziehbare Dokumentation stehen, in der genau aufgelistet ist, welche Verarbeitungsprozesse vorliegen, welche Gefahren diese ausgesetzt sind, welche Maßnahmen dagegen unternommen worden und wie das Restrisiko ausfällt. Ohne eine solche Aufzeichnung sind alle getroffenen Abhilfemaßnahmen vergebens, wenn ein Verstoß vor Gericht angeklagt wird. Denn gibt die Dokumentation Anlass zum Zweifeln, dass alles in der Macht stehende zumutbare unternommen wurde, um Verluste von Daten zu vermeiden, drohen hohe Strafzahlungen.

Gleichzeitig darf dieses Schreiben niemals als endgültig angesehen werden. Bei jeder Änderung der Gegebenheiten oder einem neuen Verfahren, müssen Anpassungen stattfinden. Wie der Datenschutz, die Informationstechnik und die Möglichkeit der Schwachstellenfindung, entwickelt sich die Dokumentation weiter. Gerade falls Lücken in verwendeten den Systemen oder der Software festgestellt wird, muss gehandelt werden, damit die HSF Meißen (FH) abgesichert ist. Dieser DSFA-Bericht muss von dem Verantwortlichen geführt werden, um der Dokumentationspflicht und Rechenschaftspflicht aus Art. 5 Abs. 2 EU-DSGVO nachzukommen.

Um eine Aktualität zu garantieren, sollten direkt im Anschluss an die eigentliche Datenschutzfolgenabschätzung Audits geplant und regelmäßig durchgeführt werden. Ebenso sollten interessierte Parteien, wie die Aufsichtsbehörde oder andere betroffene Behörden regelmäßig unterrichtet werden. Durch diesen dauerhaften Kontakt, kann im Falle einer Änderung schneller reagiert werden und gemeinsam eine Lösung für die bestehenden Probleme gefunden werden.

### 4.7 Umgang mit Restrisiken

Als nächster Punkt in der Abfolge einer Datenschutz-Folgenabschätzung ist die Bewertung der Restrisiken im Bezug von Gefahren zu den getroffenen Maßnahmen durchzuführen. Kein System kann komplett abgesichert werden, da in der heutigen Zeit schneller neue Angriffsmethoden entwickelt werden, als dass sie bekämpft werden können. Ebenfalls sind die Mitarbeiter an der Hochschule Menschen, denen Fehler passieren können. Somit muss sich die HSF Meißen (FH) diesen Restrisiken stellen und beschließen, wie damit umgegangen wird. Die Möglichkeiten für einen Umgang mit diesen Restrisiken liegen in der Akzeptanz, der Änderung von Verfahren bzw. zur Verfügung stehenden Technik oder der Untersagung der Datenverarbeitung durch die Aufsichtsbehörde. Nach der Untersuchung und Feststellung, welche Gefahren nach den getroffenen Maßnahmen noch bestehen, muss der Kontakt mit der Aufsichtsbehörde, welche in diesem Fall das Staatsministerium des Innern ist, für hohe Restrisiken stattfinden. Diese kann dann eine der drei angesprochenen Möglichkeiten vollziehen. Im Bereich der Akzeptanz werden die Verarbeitungsprozesse verstärkt überwacht, damit im Falle des Eintretens der Gefahr schnellstmöglich gehandelt werden kann. Steht eine Änderung des Verfahrens an, ist die Hochschule in der Pflicht ein neues Verfahren aufzubauen, welches das gleiche Ziel auf einem anderen Weg erfüllt. Bei einer Untersagung darf der Verantwortliche keine Daten verarbeiten, bis eine Lösung gefunden wurde, auf eine der anderen beiden Optionen zu gelangen.

Trotz aller Vorkehrungen und Abhilfemaßnahmen können einige Risiken nicht vollkommen ausgeschlossen werden und somit ein Umgang damit festgelegt werden. Solche Risiken sind beispielsweise neue Schadsoftware, gut inszeniertes Social Engineering oder Naturkatastrophen.

Im Punkt der Naturkatastrophen würde für die Hochschule nur ein Hochwasser oder ein schwerer Sturm in Frage kommen. Erdbeben oder weiträumige

Flächenbrände sind für diese Region nicht typisch und werden aus diesem Grund nicht betrachtet. Im Bezug auf ein Hochwasser ist die Position der Hochschule so gewählt, dass keine Gefahr für die Akten und Technik besteht. Aus den vergangenen Jahren ist bekannt, welche Ausmaße ein Hochwasser der Elbe haben kann und wie damit umzugehen ist. Somit ist die Gefahr für die Verfügbarkeit der Daten nur gering einzuschätzen, auch wenn die Archivierung der Akten im Keller stattfindet.

Im Falle eines Sturmes hat die HSF Meißen den Vorteil, dass um sie herum keine großen Bäume stehen, welche das Gebäude insofern beschädigen würden, dass ein Verlust von Daten zustande kommt. Auch sind die Serverräume und Archivräume, in denen sich die Handakten befinden im Keller. Damit ist eine Zerstörung durch einen Sturm fast komplett ausgeschlossen und auf Grund der Bauweise und Raumzuweisung der Einrichtung entgegengewirkt worden.

Als nächstes gilt es das hohe Restrisiko des Social Engineering zu betrachten. Hierbei wird der Schwachpunkt Mensch aktiv angegriffen und die Verantwortlichen selbst müssen auf diese vertrauen. Dabei ist es wichtig, dass die Mitarbeiter immer wieder Hinweise erhalten keine Informationen an Unberechtigte weiterzugeben und Schulungen in diese Richtung zu erhalten. Vorteilhaft zum Entgegenwirken ist es, wenn ein gutes und offenes Arbeitsklima herrscht, indem sich die Mitarbeiter gegenseitig kennen. Hiermit wird vermieden, dass Unberechtigte sich durch nicht Kenntnis eines Angestellten Informationen erschleichen können. Weiterhin sollten personenbezogene Daten niemals am Telefon besprochen werden, vor allem nicht mit Personen, die der Angestellte nicht persönlich kennt. Falls ein Student Fragen über seine Daten an der Hochschule hat, kann dieser sich per E-Mail an die Verantwortlichen wenden oder sich persönlich melden, wobei er gegebenenfalls ein Ausweisdokument vorlegen muss. Insgesamt ist es von größter Bedeutung nach dem Erlassen der EU-DSGVO noch sorgsamer mit personenbezogenen Daten umzugehen. Die Weitergabe an Unbefugte sollte definitiv vermieden werden und von den Verantwortlichen immer wieder überprüft werden. Mitarbeiter können sich bevor Informationen herausgegeben werden beim Betroffenen selbst rückversichern, ob wirklich er etwas abgefragt hat. Auch sollte regelmäßig über E-Mails oder direkte Schulungen über das Thema aufgeklärt werden.

Als letztes hohes Restrisiko muss sich noch der Schadsoftware gestellt werden. In der Zeit der Digitalisierung steigt die Zahl der neuen Schadsoftware schneller an, als die Anti-Virenscanner dagegen vorgehen können. Damit besteht für alle, die ihr Netzwerk ans Internet anschließen, immer ein gewisses Restrisiko. Damit ist der Verantwortliche für die Datenverarbeitung immer gefordert alles in seiner Macht stehende zu unternehmen, dass sein System sicher und geschützt ist. Für die Hochschule ist ein zentraler Angriffspunkt der E-Mail-Verkehr. Hierbei werden Spamfilter angewandt, mit Anti-Virenprogrammen gearbeitet und die Mitarbeiter sensibilisiert Spam- und Phishing-E-Mails zu erkennen. Außerdem schützt der Freistaat Sachsen seine Behörden zusätzlich mit einer Vielzahl an Virenscannern, welche das gesamte Netzwerk überwachen. Dennoch bestehen Lücken in den Anti-Virusprogrammen und zum Teil auch in den E-Mailprogrammen. Hacker haben sich darauf spezialisiert Lücken in Systemen zu finden, bevor die Hersteller davon Kenntnis haben.

Dieses Risiko ist allgemein bekannt und kann nur durch regelmäßige Kontrolle und eine ständige Aktualisierung der Software entgegengewirkt werden. Eine Arbeit ohne das Internet ist heutzutage jedoch unmöglich und würde zu einer Arbeitsunfähigkeit der Behörden führen. Somit muss dieses Risiko akzeptiert und es müssen geeignete Maßnahmen zur Risikominimierung gefunden werden.

Bei allen genannten Risikofaktoren bleibt immer eine gewisse Gefahr bestehen und kann nicht ausgeschlossen werden. Somit müssen die Behörden diese akzeptieren und versuchen ihnen aktiv zu begegnen. Durch Kommunikation der Führungsebene mit den Mitarbeitern kann eine Reduzierung bezüglich der menschlichen Schwachstellen gelingen.

Für die technischen Schwachstellen ist der Staatsbetrieb Sächsische Informatik Dienste in Kooperation mit der IT-Firma „T-Systems“ für den Freistaat Sachsen verantwortlich, sowie die einzelnen Informationssicherheitsabteilungen der Behörden. Damit werden alle Bereiche in denen Restrisiken vorhanden sind abgedeckt und beobachtet. Die Hochschule Meißen kennt diese Gefahren und stellt sich diesen aktiv.

# 5 Fazit

Als Abschluss meiner Arbeit möchte ich eine Bewertung der Maßnahmen, welche die Hochschule bereits unternommen hat, vornehmen und Verbesserungsvorschläge unterbreiten. Ebenfalls möchte ich meine am Anfang gestellten Fragen nochmals aufgreifen und zusammenfassend beantworten.

Als Erstes steht hier die Relevanz der Datenschutzfolgenabschätzung für die Hochschule Meißen und deren Gewichtung in der EU-DSGVO. Die DSFA wird als eines der wichtigsten Instrumente für den modernen Datenschutz gewertet und soll ein höheres Niveau der Datensicherheit hervorrufen. Durch die Pflicht der Aufsichtsbehörden bei großen Risiken die Datenverarbeitung zu untersagen, müssen alle datenschutzrechtlichen Aspekte bestmöglich abgedeckt werden, weil ansonsten eine Einschränkung der Arbeitsfähigkeit droht. Die Behörden sind damit angehalten und verpflichtet die Risiken so gering wie möglich zu halten und alle Vorkehrungen genau zu dokumentieren. Ohne eine ordentlich durchgeführte DSFA und die dazugehörige Dokumentation, kann es im Falle eines Verstoßes hohe Strafzahlungen geben. Da die Verwaltungen mit Steuergeldern arbeiten und als Vorbilder vorangehen sollten, sind solche Strafzahlungen um jeden Preis zu verhindern. Vor allem die öffentlichen Einrichtungen, deren gesamte Arbeit auf Gesetzlichkeiten beruht, sollten keine großen Sicherheitslücken aufweisen.

Daraus ergeben sich einige Vorteile, aber auch Nachteile für die deutsche Verwaltung. Zum einen ist die Erstellung des Verfahrensverzeichnisses ein gewaltiger Aufwand und mit Kosten verbunden. Zum anderen müssen in einigen Bereichen gegebene Technik, Hardware und Software, ausgetauscht werden, welches wieder Kosten hervorruft. Weiterhin ist die DSFA kein einmaliges Projekt, sondern muss durchgängig weitergeführt werden und ständig auf dem aktuellen Stand sein. Ein ebenso umfangreicher Punkt sind die neuen Meldepflichten der Verantwortlichen gegenüber den betroffenen Personen im Falle eines Datenverlustes oder Diebstahls. Hier müssen bei Vorfällen, welche sich definitiv auf das Leben der Betroffenen auswirken, alle Details des Verlustes genannt werden und umgehend Maßnahmen zum Einschränken getroffen werden.

Trotz aller Nachteile eröffnet dieses Instrument neue Wege für die Verantwortlichen, da sie sich besser absichern können und durch eine lückenlose Doku-

mentation vor Gericht keine Schwierigkeiten beim Nachweisen von Tatsachen haben. Gleichzeitig bietet sich dieser Zeitpunkt an, um neue Techniken einzuführen und Verarbeitungsprozesse zu aktualisieren. Dadurch kann eine Arbeitserleichterung für die Mitarbeiter der Verwaltung erfolgen und die Effektivität als auch die Effizienz gesteigert werden. Gerade in der aktuellen Lage des öffentlichen Bereichs, in dem es überall an Arbeitskräften mangelt, sind effiziente Arbeitsweisen wichtig. Zum Schluss muss die Übersicht erwähnt werden, die durch die DSFA nochmals gesteigert wird. Es werden alle Verarbeitungsprozesse, in denen personenbezogene Daten verwendet werden, aufgeschrieben und der Aufsichtsbehörde präsentiert, woraus das Verfahrensverzeichnis erstellt werden kann.

Insgesamt ist ein Mehraufwand für die Verwaltung zu verzeichnen, welcher jedoch gerade in strittigen Fällen vor Gericht, Sicherheit schafft und das Datenschutzniveau nochmals anhebt.

Die HSF Meißen (FH) ist während der Ausarbeitung meiner Bachelorarbeit gerade in einer Umbruchphase und somit sind noch nicht alle Aspekte der neuen EU-DSGVO perfekt abgestimmt. Aus diesem Grund möchte ich mit meinen Recherchen einige Verbesserungsvorschläge ausgerichtet auf den aktuellen Stand geben. Darunter fällt als Erstes, dass die Hochschule sich Gedanken über eine explizite Ermächtigungsgrundlage zur Erhebung von Daten machen sollte. In allen relevanten Gesetzen wird lediglich die Datenverarbeitung geregelt. Die EU-DSGVO fordert jedoch eine einschlägige Rechtsgrundlage zum Erheben von personenbezogenen Daten, bei denen keine Einwilligung vorliegt.

Weiterhin ist mir aufgefallen, dass bei der Archivierung von den Bachelor- und Diplomarbeiten der Studenten die Adresse mit aufbewahrt wird. Dies entspricht nicht dem Grundsatz der Datenvermeidung und erfüllt in dieser Situation keinen Zweck. Die archivierten Daten werden nicht weiter aktualisiert und die Adresse der Studenten ändert sich innerhalb von 50 Jahren mit Sicherheit mindestens einmal. Somit besteht für die Speicherung einer solchen Information kein berechtigtes Interesse und sollte mit gelöscht werden. Für die eindeutige Zuordnung einer Arbeit sind wichtig: der Name, der Geburtsname, das Geburtsdatum und der Geburtsort. Dies sind die einzigen Informationen, die über diesen langen Zeitraum gespeichert werden dürfen und müssen.

Ebenfalls sollten regelmäßige Schulungen des gesamten Personals im Hinblick auf die Möglichkeiten von Hackern stattfinden. Vor allem bei Mitarbeitern, die täglich im Kontakt mit personenbezogenen und vertraulichen Daten stehen, sollte ein Pflichtbewusstsein dafür hervorgerufen werden. Gerade im Bereich von falschen E-Mails, wie Spam und Phishing, aber auch Hardware, wie USB-Sticks sollte äußerste Vorsicht geboten sein. Für eine Sensibilisierung können interne E-Mails verschickt werden, welche einen Phishing-Angriff simulieren. Dabei werden Mitarbeiter, die darauf reagieren erkannt und können besonders auf solche Sachverhalte mit deren Konsequenzen hingewiesen werden.

Zum Schluss ist die Technik, sowohl Software als auch Hardware, immer auf dem aktuellen Stand der Technik zu halten. Dabei muss nicht immer das neueste Produkt verwendet werden. Wichtig ist, dass die Technik den allgemeinen Standards entspricht, die benötigte Leistung erbringt und ordnungsgemäß gesichert werden kann. Die Anti-Virenprogramme sollten regelmäßig aktualisiert werden und darauf geachtet werden, dass die Systeme sicher sind. Vor allem beim Auftreten neuer Gefahren, müssen Informationen an alle Mitarbeiter weitergeleitet werden und gegebenenfalls Verarbeitungsprozesse stillgelegt werden, insofern eine Gefahr für die Daten der Studenten besteht.

Aus meinen Untersuchungen der Gegebenheiten an der HSF Meißen (FH) habe ich in Anlehnung an diese Quelle[36] eine eigene Checkliste für die Durchführung einer DSFA an der Hochschule erstellt.[37]

Zusammengefasst ist zu sagen, dass die Hochschule mit den getroffenen Maßnahmen einen guten Sicherheitsstandard bietet und die Daten der Studenten ordnungsgemäß und gesetzeslegitim verwahrt werden. Einzelne Punkte bieten die Möglichkeit zur Verbesserung, wie zum Beispiel die Archivierung der Bachelor- und Diplomarbeiten oder die Erstellung einer Ermächtigungsgrundlage zur Datenerhebung. Die Forderungen der neuen EU-DSGVO sind jedoch erfüllt und somit die HSF Meißen (FH) in der Pflicht für alle ihre Verarbeitungsvorgänge eine DSFA durchzuführen und ein Verfahrensverzeichnis zu erstellen. Im Hinblick auf die Sicherheit der Daten bestehen aus meiner Sicht wenige Bedenken.

[36] o. V.: Kompakte Checkliste zur Umsetzung der Datenschutz-Grundverordnung, 2017, S. 5ff.
[37] siehe Anhang 5: Checkliste für die Durchführung einer DSFA für die HSF Meißen (FH)

## Thesen

1. Die EU-DSGVO dient sowohl wirtschaftlichen Unternehmen als auch öffentlichen Einrichtungen einen höheren Datenschutzstandard zu generieren und vor allem sensible Daten von Bürgern und Kunden besonders zu schützen.

2. Die Datenschutz-Folgenabschätzung ist ein Instrument, mit dem die Datenverarbeiter dazu aufgefordert werden einen genauen Blick auf die Datenerhebung und –verarbeitung zu werfen und somit Prozesse nochmals nachzuvollziehen und gegebenenfalls Anpassungen zur Legitimität des Gesetzes vorzunehmen.

3. In einigen Fällen wird die DSFA dazu führen, dass Unternehmen und Behörden veraltete Techniken ersetzen, unsichere Verfahren anpassen oder komplett neue Herangehensweisen an Verarbeitungsprozesse suchen müssen.

4. Die HSF Meißen (FH) hat bereits alle Vorkehrungen getroffen, damit sie eine legitime Erhebung und Verarbeitung von Daten der Studenten gemäß der Anforderungen der EU-DSGVO durchführen kann.

5. Die HSF Meißen (FH) wird sich in nächster Zeit um einen Gesetzesentwurf für eine explizite Ermächtigungsgrundlage zur Erhebung von Daten von Studenten bemühen, damit eine legitimierte Datenerhebung besteht.

# Anhang

## Anhangsverzeichnis

# Anhang 1: Online-Bewerbungsformular der HSF Meißen (FH)



Formular ID:
Prüfsumme:

HOCHSCHULE MEISSEN (FH)
UND FORTBILDUNGSZENTRUM | Freistaat SACHSEN

Geschäftsstelle des Auswahlausschusses/LG 2.1

Hochschule Meißen (FH) und
Fortbildungszentrum

Herbert-Böhme Straße 11
**01662 Meißen**

**Ausfüllhinweise**
- Zutreffendes bitte ankreuzen bzw. ausfüllen!
- Diese Felder müssen ausgefüllt werden.
- Weitere Informationen und Hinweise.

## Bewerbung um die Zulassung zum schriftlichen Auswahlverfahren

für Studiengänge in der
1. Einstiegsebene der höheren Laufbahn

**Persönliche Angaben**

| | | | |
|---|---|---|---|
| Name | Nachname | Vorname | Vorname |
| Geburtsname | Geburtsname | | |
| Strasse / Hausnummer | Straße | | |
| PLZ und Ort | PLZ | Wohnort | |
| Adresszusatz (z. B. Ortsteil: OT ...) | Ortsteil/Adresszusatz | | |
| Geburtsdatum und -ort | DD.MM.JJJJ | Geburtsort | |
| Geburtsstaat | Geburtsstaat | | |
| Staatsangehörigkeit | | andere Staatsangehörigkeit | |
| Telefonnummer | Telefonnummer | Geschlecht | ○ weiblich ○ männlich |
| E-Mail-Adresse | E-Mail-Adresse | | |

**1. Ich habe die Fachhochschulreife bzw. die allgemeine Hochschulreife bereits erworben. Wenn nicht zutreffend, bitte weiter mit Punkt 2.**

| | | |
|---|---|---|
| ○ Allgemeine Hochschulreife | Abschlussjahr | JJJJ |
| ○ Fachhochschulreife | Abschlussnote (z. B. 1,9) | |
| | Abschlussnote wiederholen | |
| Art der Bildungseinrichtung | | |
| Name der Bildungseinrichtung | | |

eGovernment

**2. Ich habe die Fachhochschulreife bzw. die allgemeine Hochschulreife noch nicht erworben.**

Ich besuche folgenden Bildungsgang ▼

Name der Bildungseinrichtung

○ Allgemeine Hochschulreife — Abschlussjahr voraussichtlich JJJJ

Mein aktuelles Zwischenzeugnis (11/2 oder 12/2) weist einen Punkte-Durchschnitt aller von mir belegten Unterrichtsfächer von (z. B. 10,85) Punkten aus. — Abschlussnote (z. B. 10,85)

Abschlussnote wiederholen

○ Fachhochschulreife — Abschlussjahr voraussichtlich JJJJ

Mein aktuelles Zwischenzeugnis weist einen Noten-Durchschnitt aller von mir belegten Unterrichtsfächer von (z. B. 2,3) aus: — Abschlussnote (z. B. 1,9)

Abschlussnote wiederholen

☐ Kein Zwischenzeugnis vorhanden (z. B. einjährige Fachoberschule)

Ich habe noch kein aktuelles Zwischenzeugnis. Dieses erhalte ich erst am TT.MM.JJJJ

**3. Ich habe keine ausgewiesene Fachhochschulreife oder allgemeine Hochschulreife. Nur auszufüllen, wenn Punkt 1 oder 2 nicht zutreffend.**

☐ Ich möchte Zugang zum Studium mit folgendem Abschluss erlangen: *noch 254 Zeichen*

Bezeichnung des Abschlusses

**4. Ich bewerbe mich für nachstehende Studiengänge** Mehrfachbewerbungen sind möglich!

☐ Allgemeine Verwaltung (Bachelor of Laws)

☐ Rechtspflege (Diplom-Rechtspfleger (FH))

☐ Sozialverwaltung (Bachelor of Laws)

☐ Steuerverwaltung (Diplom-Finanzwirt/in (FH))

☐ Sozialversicherung (Bachelor of Laws)

**5. Ich habe zu Punkt 1 oder 2 bereits folgende Abschlüsse erworben.**

**Laufbahnausbildung**

○ mittlerer Dienst — Bezeichnung: Bezeichnung des Abschlusses — Abschlussjahr: JJJJ

○ gehobener Dienst — Bundesland: Bundesland

**Berufsausbildung**

☐ Berufsausbildung — Berufsbezeichnung: Bezeichnung des Abschlusses — Abschlussjahr: JJJJ

**Studium**

☐ Studium — erworbener Abschluss: Bezeichnung des Abschlusses — Abschlussjahr: JJJJ

Studiengang: Studiengang

**6. Behinderung**

schwerbehindert (nach § 2 Abs. 2 Sozialgesetzbuch IX) Grad der Behinderung (GdB ab 50)

gleichgestellt (nach § 2 Abs. 3 Sozialgesetzbuch IX) Grad der Behinderung (GdB unter 50)

Gleichstellungsbescheid ausstellende Behörde Datum TT.MM.JJJJ

behindert ohne Gleichstellung Grad der Behinderung (GdB unter 30)

Antrag gestellt - Bescheid liegt noch nicht vor Antrag gestellt am TT.MM.JJJJ

Antrag auf Gleichstellung bei zuständiger Behörde gestellt

Antrag auf erstmalige Feststellung einer Behinderung gestellt

Antrag auf Arbeitszeitverlängerung beim schriftlichen Auswahlverfahren

Bitte "Fragebogen für Menschen mit Behinderung oder chronischen Krankheiten" per E-Mail an die Geschäftsstelle des Auswahlausschusses senden. Er dient lediglich dazu, für Sie möglichst optimale Bedingungen bei der Bearbeitung des Eignungstests sowie ggf. für die Studienaufnahme zu gewährleisten.

**Mir ist bekannt, dass ein Anspruch auf Übernahme in ein Beamten- oder Angestelltenverhältnis nach bestandener Laufbahnprüfung nicht besteht.**

**Datenschutzerklärung**

**Ich willige ein, dass meine in diesem Zulassungsantrag (einschließlich ggf. eingereichter Nachweise) gemachten Angaben an der Hochschule für öffentliche Verwaltung und Rechtspflege (FH), Fortbildungszentrum des Freistaates Sachsen (HSF Meißen) elektronisch zur Durchführung des Zulassungsverfahrens verarbeitet werden.**

**Zudem beinhaltet meine Einwilligung im Auswahlverfahren für die grundständigen Studiengänge und für die Ausbildung für die Laufbahngruppe 1.2 die Übermittlung der Daten an die mögliche(n) künftige(n) Einstellungsbehörde(n). Ebenso wird mein Testergebnis der/den Einstellungsbehörde(n) bekanntgegeben.**

Ich willige ferner darin ein, dass meine personenbezogenen Daten und mein Testergebnis für die nächsten beiden Einstellungstermine verarbeitet und ich von der HSF Meißen über das jeweilige Verfahren informiert werde. Ich habe das Recht, dieser Datenverarbeitung jederzeit zu widersprechen.

**Nähere Informationen über die Verarbeitung meiner personenbezogenen Daten kann ich auf der Internetseite der Hochschule unter https://www.hsf.sachsen.de/datenschutz/auswahlverfahren einsehen.** Dies gilt auch für die weitere Verarbeitung meiner Daten an der HSF Meißen für den Fall der Aufnahme des Studiums bzw. der Ausbildung.

Ich widerspreche der Verarbeitung meiner Daten.

Zwar bin ich nicht verpflichtet, die erhobenen Angaben zu machen, mir ist jedoch bewusst, dass mein Zulassungsantrag ohne meine Einwilligung in die Verarbeitung der Daten nicht bearbeitet werden kann.

**Wir weisen Sie darauf hin, dass fehlerhafte Angaben zum Ausschluss aus dem Verfahren führen können.**

Bewerbung einreichen | leeres Formular drucken | Formular leeren

## Anhang 2: Stammdatenblatt aus der Studentenakte der HSF Meißen (FH)

HOCHSCHULE MEISSEN (FH)
UND FORTBILDUNGSZENTRUM | Freistaat SACHSEN

**P**

**Stammdatenblatt für die Personalnebenakte der Studentin / des Studenten**

(Diese Daten dienen nur zur fachhochschulinternen Nutzung)

**Angaben zur Person:**

| | |
|---|---|
| *Familienname:* | xxxx.xxxxxxxx |
| *Geburtsname:* | |
| *Vorname:* | xxxxxxxxxxx |
| *Geburtsdatum:* | xx.xx.xxxx |
| *Geburtsort:* | xxxxxxxxxxxxxxx |
| *Fachbereich / Fachrichtung:* | FS / Sozialversicherung |
| *Matrikelnummer:* | 00000014xxxx |
| *Einstellungsbehörde:* | Deutsche Rentenversicherung Mitteldeutschland |

| | |
|---|---|
| **Datum der Immatrikulation:** | **01.09.2014** |
| **Bestehen der Abschlussprüfung am:** | **31.08.2017** |
| **Studium vorzeitig beendet:** | |

**Letzte Wohnanschrift:**

| | |
|---|---|
| *Straße:* | xxxxxxxxxxxx |
| *PLZ Wohnort:* | xxxxxxxxxxxx |
| *Telefonnummer:* | xxxxxxxxxxxxxx |
| *E-Mail-Adresse:* | xxxxxxxxxxx |

Mit der Unterschrift wird bestätigt, dass

- alle Originalunterlagen, die an die Personalgrundakte führende Einstellungsbehörde geschickt und
- alle in der Personalnebenakte der FHSV Meißen befindlichen Kopien datenschutzgerecht vernichtet wurden.

Datum: .....11.03.2017.....

Unterschrift: .....

Dieses Stammdatenblatt ist der Prüfungsakte der Studentin/des Studenten für einen Zeitraum von drei Jahren nach Nr. P 4 beizuheften und vor der endgültigen Archivierung der Prüfungsakte zu vernichten!

## Anhang 4: Gefahren und Maßnahmen nach BSI-Katalog

| Mögliche Gefahren | Maßnahmen gegen die Gefahren |
|---|---|
| Feuer | 5, 6, 19 |
| Wasser | 8, 10 |
| Staub/Verschmutzung | 22, 25 |
| Naturkatastrophen | 4, 10, |
| Stromausfall | 1, 3, 17 |
| Ausfall der Netzwerkstrukturen | 3, 4, 10, 17 |
| Spionage | 11, 12, 18, 27 |
| Abhören | 7, 11, 20 |
| Diebstahl von Geräten und Dokumenten | 7, 11, 18 |
| Verlust von Geräten und Dokumenten | 14 |
| Manipulation von Hard- und Software | 15, 16, 24, 27 |
| Manipulation von Informationen | 2, 11, 28 |
| Unbefugtes Eindringen in IT-Systeme | 7, 11, 27 |
| Zerstörung von Geräten und Dokumenten | 10, 11, 27, 28 |
| Ausfall von Geräten oder Systemen | 3, 4, 17 |
| Fehlfunktionen von Geräten und Systemen | 17, 22, 24 |
| Software-Schwachstellen | 25 |
| Verstoß gegen Gesetze und Regelungen | 1, 26 |
| Unberechtigte Nutzung von Geräten und Systemen | 2, 28 |
| Fehlerhafte Nutzung von Geräten und Systemen | 26 |
| Missbrauch von Berechtigungen | 20, 28 |
| Personalausfall | 26, 28 |
| Anschlag | 7, 12, 27 |
| Nötigung/Erpressung/Korruption | 27 |
| Identitätsdiebstahl | 1, 9 |
| Missbrauch personenbezogener Daten | 1, 20 |

| | |
|---|---|
| Schadprogramme (Viren/Trojaner/etc.) | 17, 23, 27 |
| Sabotage | 2, 9, 25 |
| Social Engineering | 26 |
| Unbefugtes Eindringen in Räumlichkeiten | 2, 7, 11 |
| Datenverlust | 9, 16, 18 |
| Integritätsverlust schützenswerter Daten | 1, 15, 24 |
| Unzureichende Regelungen | 1, 27 |
| Unzureichenden Kenntnisse über Regelungen | 2, 9, 28 |
| Unzureichende Kontrolle | 9, 20 |
| Fehlende Wartung | 15, 17, 22, 23 |
| Unbefugter Zutritt zu Räumen | 2, 7, 9, 10, 11, 20, 27 |
| Unerlaubtes Ausüben von Rechten | 1, 2, 28 |
| Mangelnde Anpassung des IT-Systems | 22 |
| Verfügbarkeit von Daten | 15, 21, 24 |
| Vertraulichkeitsverlust | 2, 11, 27 |
| Unzureichende Test- und Produktivumgebung | 23 |
| Unzureichende Dokumentation | 1, 26 |
| Unzureichende Leistungskapazitäten | 15, 21, 25 |
| Unkontrollierter Aufbau von Kommunikationsverbindungen | 10, 14, 15 |
| Datenbank-Sicherheitsmechanismen | 11, 25, 28 |
| Konzeptionelle Schwäche des Netzwerkes | 1, 2, 15, 23, 24, 28 |
| Ungesicherte Akten- und Datentransporte | 14 |
| Ungeeignete Entsorgung von Dokumenten und Datenträgern | 27 |
| Unzureichende Schulungen (Telearbeiten) | 1, 27 |

**Maßnahmen gegen die oben genannten Gefahren mit Nummerierung**

| | |
|---|---|
| 1 | Einhaltung einschlägiger Normen und Vorschriften |
| 2 | Regelungen für Zutritt |
| 3 | Stromversorgung absichern |
| 4 | Blitzschutzvorrichtungen |
| 5 | Brandschutzvorschriften einhalten |
| 6 | Feuerlöscher |
| 7 | Sichere Türen und Fenster |
| 8 | Selbstständige Entwässerung |
| 9 | Pförtnerdienst |
| 10 | Gefahrmeldeanlagen |
| 11 | Einbruchsschutz |
| 12 | Abgeschlossene Türen |
| 13 | Klimatisierung der Technik |
| 14 | Aufbewahrung mobiler Geräte |
| 15 | Aufbewahrung stationärer Geräte |
| 16 | Schutzschränke |
| 17 | Schutz der Netzwerkkomponenten |
| 18 | Diebstahl-Sicherung |
| 19 | Brandmeldeanlage |
| 20 | Videoüberwachung |
| 21 | Geeignete Lagerung von Archivmedien |
| 22 | Erneuerung der IT-Verkabelung |
| 23 | Fachgerechte Installationen |
| 24 | Schutz des Rechenzentrums gegen Unbefugte |
| 25 | Funktionstest |
| 26 | Klimatisierung für Menschen |
| 27 | Sicherheitskonzept |
| 28 | Zutrittskontrollsystem und Berechtigungsmanagement |

# Literaturverzeichnis

**Bentz**, Volker: Personenbezogene Daten – Unterschied zwischen DSGVO und BDSG. Brandmauer IT Security Blog, Artikel vom 19.12.2017. URL: https://www.brandmauer.de/blog/it-security/personenbezogene-daten-unterschied-zwischen-dsgvo-und-bdsg
zuletzt aufgerufen am 22. August 2018; 14:07 Uhr

**Bieker**, Felix ; Friedewald, Michael ; Nebel, Maxi ; Obersteller, Hannah ; Rost, Martin : White Paper: Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Eggenstein: Sober GmbH Druck und Verlag, 2016; URL: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf
zuletzt aufgerufen am 22. August 2018; 13:34 Uhr

**Boegelein**, Linda: Datenschutz-Folgenabschätzung: Kennen Sie Ihr Risiko?. IT-Service.network, Artikel vom 03. Januar 2018; URL: https://it-service.network/blog/2018/01/03/datenschutz-folgenabschaetzung-risikobewertung/
zuletzt aufgerufen am 22. August 2018; 17:24 Uhr

**Brünen**, Bea ; Lexow, Lev ; Siebert, Sören: Die Datenschutz-Grundverordnung: Was sich 2018 im Datenschutz ändert und warum das für sie wichtig ist. Letzte Aktualisierung am 05. Juli 2018; URL: https://www.e-recht24.de/datenschutzgrundverordnung.html
zuletzt aufgerufen am 22. August 2018; 13:47 Uhr

**Czernik**, Agnieszka: Datenschutz-Grundverordnung und Datensicherheit. Fachbeitrag vom 08. Juli 2016; URL: https://www.datenschutzbeauftragter-info.de/datenschutz-grundverordnung-datensicherheit/
zuletzt aufgerufen am 23. August 2018; 15:40 Uhr

**Czernik**, Agnieszka: Definition und Unterscheidung der Begriffe Daten, Informationen & Wissen. Fachbeitrag vom 05. August 2016; URL: https://www.datenschutzbeauftragter-info.de/definition-und-unterscheidung-der-begriffe-daten-informationen-wissen/
zuletzt aufgerufen am 22. August 2018; 16:55 Uhr

**Datenschutz, Dr.** (Pseudonym): Datenschutz-Folgenabschätzung: Was ist das überhaupt? Fachbeitrag vom 06. April 2016; URL: https://www.datenschutzbeauftragter-info.de/datenschutz-folgenabschaetzung/
zuletzt aufgerufen am 22. August 2018; 16:30 Uhr

**Datenschutz, Dr.** (Pseudonym): DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten. Fachbeitrag vom 29. Mai 2017; URL: https://www.datenschutzbeauftragter-info.de/dsgvo-grundsaetze-fuer-die-verarbeitung-personenbezogener-daten/
zuletzt aufgerufen am 22. August 2018; 13:23 Uhr

**Härting**, Niko: Datenschutz-Grundverordnung : Das neue Datenschutzrecht in der betrieblichen Praxis über 100 Fragen und Antworten. Köln: Verlag Dr. Otto Schmidt KG, 2016

**Rassek**, Anja: Integrität: Unverzichtbar fürs Vertrauen. Artikel vom 10. August 2017; URL: https://karrierebibel.de/integritaet/
zuletzt aufgerufen am 22. August 2018; 15:35 Uhr

**Reinis**, Mathias: Privacy Impact Assessment : Datenschutz-Folgenabschätzung nach ISO/IEC 29134 und ihre Anwendung im Rahmen der EU-DSGVO mit Schlagwortverzeichnis : Band 2 unserer GRC Reihe „Fit für die EU Datenschutzgrundverordnung“. 2. Auflage, Concept Factory Inh. Mathias Reinis, Bonn: Books on Demand, Norderstedt, 2018

**Stalla**, Mirco: Backup-Strategie: Vollsicherung, inkrementelle und differenzielle Datensicherung erklärt: Methoden zur Datensicherung im Überblick. Artikel vom 13. Juni 2016; URL: https://www.netzwelt.de/system/backup-ultimative-guide-datensicherung/158793_2-backup-strategie-vollsicherung-inkrementelle-

differentielle-datensicherung-erklaert.html
zuletzt aufgerufen am 22. August 2018; 15:31 Uhr

**Ohne Verfasser**: Das Abstract in der wissenschaftlichen Arbeit. Datum unbekannt; URL:
https://www.studium-und-pc.de/abstract-in-der-wissenschaftlichen-arbeit.htm
zuletzt aufgerufen am 22. August 2018; 17:13 Uhr

**Ohne Verfasser**: Datenschutzerklärungen. Information der Hochschule Meißen (FH) und Fortbildungszentrum, Datum unbekannt; URL: https://www.hsf.sachsen.de/datenschutz/
zuletzt aufgerufen am 23. August 2018; 14:34 Uhr

**Ohne Verfasser**: Datenschutz-Folgenabschätzung : Durchführung einer DSFA am Beispiel Videoüberwachung. Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacy officers. Stand Januar 2018; URL:
https://www.privacyofficers.at/Privacyofficers_DSFA-Umsetzung_DSGVO_v1.0.pdf
zuletzt aufgerufen am 22. August 2018; 14:43 Uhr

**Ohne Verfasser**: Kompakte Checkliste zur Umsetzung der Datenschutz-Grundverordnung : (VO [EU] 2016/679). Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacy officers. Stand September 2017; URL:
https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v2.0.pdf
zuletzt aufgerufen am 23. August 2018; 18:35 Uhr

**Ohne Verfasser**: Definition: vertrauliche Daten. Artikel von der Informationstechnologie Technische Universität München, Datum unbekannt; URL: https://www.it.tum.de/it-sicherheit/fuer-mitarbeiterinnen/vertrauliche-daten/definition-vertrauliche-daten/
zuletzt aufgerufen am 22. August 2018; 15:40 Uhr

**Ohne Verfasser**: Europäische Datenschutz-Grundverordnung : Internationale Digitalpolitik. Bereitgestellt vom Bundesministerium für Wirtschaft und Energie, Datum unbekannt. URL:

https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html
zuletzt aufgerufen am 22. August 2018; 13:44 Uhr

**Ohne Verfasser**: GDD-Praxishilfe DS-GVO X: Voraussetzungen der Datenschutz-Folgenabschätzung. Bereitgestellt von der Gesellschaft für Datenschutz und Datensicherheit e.V., erstellt vom Arbeitskreis „DS-GVO Praxis“. Stand vom November 2017; URL: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf
zuletzt aufgerufen am 22. August 2018; 17:18 Uhr

**Ohne Verfasser**: IT-Grundschutz-Kataloge. Bereitgestellt vom Bundesamt für Sicherheit in der Informationstechnik, insbesondere Gefährdungs- und Maßnahmenkataloge, Datum unbekannt. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
zuletzt aufgerufen am 22. August 2018; 15:18 Uhr

**Ohne Verfasser**: Kurzpapier Nr. 1: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO. Datenschutzkonferenz, Stand Januar 2018. URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_Verzeichnis%20von%20Verarbeitungstaetigkeiten.pdf?__blob=publicationFile&v=3
zuletzt aufgerufen am 22. August 2018; 19:16 Uhr

**Ohne Verfasser**: Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. Datenschutzkonferenz, Stand Januar 2018. URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_DatenschutzFolgeabschaetzung.pdf?__blob=publicationFile&v=2
zuletzt aufgerufen am 22. August 2018; 19:17 Uhr

**Ohne Verfasser**: Verfügbarkeit. IT-Wissen.info, Artikel vom 03. Oktober 2017; URL:
https://www.itwissen.info/Verfuegbarkeit-availability.html
zuletzt aufgerufen am 22. August 2018; 15:24 Uhr

**Vetter**, Anita: Datenschutz, Datensicherheit und Arten von Daten. Artikel vom 09. Februar 2016; URL: https://www.polyas.de/blog/de/online-wahlen/sicherheit/datenschutz-datensicherheit-und-arten-von-daten zuletzt aufgerufen am 22. August 2018; 16:57 Uhr

# Rechtsquellenverzeichnis

**Bundesdatenschutzgesetz** i. d. F. der Bekanntmachung vom 30. Juni 2017 (BGBl. I S. 2097)

**Gesetz über die Freiheit der Hochschulen im Freistaat Sachsen** (Sächsisches Hochschulfreiheitsgesetz) i. d. F. der Bekanntmachung vom 15. Januar 2013 (SächsGVBl. 2013 Nr.1, S. 3), zuletzt geändert durch Art. 44 des Gesetzes vom 26. April 2018 (SächsGVBl. S. 198)

**Gesetz über die Hochschule für öffentliche Verwaltung und Rechtspflege (FH), Fortbildungszentrum des Freistaates Sachsen** (Fachhochschule-Meißen-Gesetz) i. d. F. der Bekanntmachung vom 22. Oktober 2016 (SächsGVBl. 2016 Nr. 12, S. 498)

**Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen** (Sächsisches Datenschutzgesetz) i. d. F. der Bekanntmachung vom 25. August 2003 (SächsGVBl. 2003 Nr. 12, S. 330), zuletzt geändert durch Art. 46 des Gesetzes vom 26. April 2018 (SächsGVBl. S. 198)

**Gesetz zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG** (Sächsisches Datenschutzdurchführungsgesetz) i. d. F. der Bekanntmachung vom 26. April 2018 (SächsGVBl. 2018 Nr. 7, S 198, 199)

**Verordnung des Sächsischen Staatsministeriums des Innern und des Sächsischen Staatsministeriums für Soziales und Verbraucherschutz über die Ausbildung und Prüfung im Vorbereitungsdienst für die erste Einstiegsebene der Laufbahngruppe 2 der Fachrichtung Allgemeine Verwaltung mit dem fachlichen Schwerpunkt allgemeiner Verwaltungsdienst und der Fachrichtung Gesundheit und Soziales mit dem fachlichen Schwerpunkt sozialwissenschaftlicher Dienst im Freistaat Sachsen** (Sächsische Ausbildungs- und Prüfungsordnung allgemeiner Verwaltungsdienst und sozialwissenschaftlicher

Dienst) i. d. F. der Bekanntmachung vom 19. Januar 2017 (SächsGVBl. 2017 Nr. 2, S. 20)

**Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst über die Verarbeitung personenbezogener Daten der Mitglieder, Angehörigen, Studienbewerber, Prüfungskandidaten, Gasthörer und ehemaligen Mitglieder der staatlichen Hochschulen** (Sächsische Hochschulpersonendatenverordnung) i. d. F. der Bekanntmachung vom 20. Oktober 2017 (SächsGVBl. 2017 Nr. 15, S. 568)

**Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG** (Datenschutz-Grundverordnung) i. d. F. der Bekanntmachung vom 27. April 2016

## Eidesstattliche Versicherung

Ich versichere hiermit an Eides Statt, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die gedruckte und digitalisierte Version der Arbeit sind identisch.

Die Arbeit oder Teile daraus wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Meißen, 27.08.2018

Unterschrift
Tom Rajko Hauwetter