FH JOANNEUM
UNIVERSITY OF APPLIED SCIENCES

DATENSCHUTZHANDBUCH DER FH JOANNEUM GESELLSCHAFT MBH V1.01

Herausgegeben vom

Datenschutzausschuss der FH JOANNEUM Gesellschaft mbH

Beschluss vom

2. Oktober 2012

Vorwort

Die FH JOANNEUM setzt zur Durchführung ihrer Aufgaben im Bereich der Lehre und Forschung moderne IT-Infrastruktur ein und ist zu einem großen Teil davon abhängig. Der effiziente und sichere Betrieb, sowie die vertrauensvolle Verarbeitung der anfallenden Daten setzt voraus, dass alle Mitwirkenden innerhalb der FH JOANNEUM verantwortungsvoll mit den ihnen anvertrauten Daten und dem eingeräumten Handlungsspielraum umgehen.

Durch die Vernetzung von Arbeitsplätzen können absichtliche oder auch unabsichtliche Handlungen Einzelner sehr schnell zu großen Auswirkungen für andere im selben Netzwerk führen. Vor allem wenn dadurch Daten von natürlichen aber auch juristischen Personen berührt werden, kann sehr schnell das Vertrauen in die ganze Institution in Mitleidenschaft gezogen werden.

Dieses Datenschutzhandbuch (DS-Handbuch) soll deshalb ein Leitfaden sein, wie das Miteinander in einer Hochschule gestaltet sein muss, damit der Kreativität und dem freien Geist möglichst wenig technische Schranken auferlegt werden müssen. Es gibt außerdem im Kapitel 3 eine grundlegende Einführung in das österreichische Datenschutzgesetz in der die darin auftretenden Begriffe und prinzipiellen Ver- und Gebote erklärt werden.

Im DS-Handbuch finden sich bewusst keine technischen Spezifikationen von Hard- oder Software. Konkrete Umsetzungen, detaillierte Regelungen oder Anforderungen an Geräte oder Programme werden in aktuellen Beschreibungen von der zentralen IT (ZIT) der FH JOANNEUM erstellt und auf deren Inter- oder Intranetseite publiziert.

Die Grundsätze zur Gewährleistung des vertrauensvollen und verantwortungsbewussten Umgangs mit den der FH JOANNEUM anvertrauten Daten finden sich in der Datenschutzerklärung der FH JOANNEUM. Dieses Dokument beinhaltet weiters die Erklärung zur Erfüllung der Informationspflicht von Auftraggeberinnen und Auftraggebern von Datenanwendungen gemäß § 24 DSG 2000 und kann in seiner jeweils gültigen Fassung über die Website der FH JOANNEUM abgerufen werden.

Das vorliegende Datenschutzhandbuch ist auch als Information und Belehrung zum Thema Datenschutz nach § 14 Abs 2 Z 3 DSG 2000, die die FH JOANNEUM ihren Mitarbeitern und Mitarbeiterinnen zur Verfügung stellt, zu verstehen. Die bzw. der Datenschutzbeauftragte (DSB, datenschutz@fh-joanneum.at) steht darüber hinaus allen Personen an der FH JOANNEUM gerne für Auskünfte und Erklärungen zum Thema Datenschutz oder dem vorliegenden DS-Handbuch zur Verfügung.

Harald Burgsteiner
Datenschutzbeauftragter der FH JOANNEUM

Inhaltsverzeichnis

Kapitel 1

Allgemeines

Die FH JOANNEUM zählt zu den führenden Fachhochschulen Österreichs. Neben der Lehre stellen auch die Bereiche Forschung und Entwicklung wesentliche Bestandteile der Hochschulausbildung dar.

In den verschiedenen Bereichen des Fachhochschulbetriebs werden große Mengen von Daten automatisiert verarbeitet und gespeichert. Diese Daten (unter anderem personenbezogene Daten und Forschungsergebnisse) müssen sorgfältig geschützt werden, um Datendiebstahl, Datenmissbrauch, Datenverlust und andere Gefährdungen abzuwenden. Die Einhaltung der Datenschutzbestimmungen wird an der FH JOANNEUM gewährleistet, indem die mit der Verarbeitung von Daten betrauten Personen entsprechend aufgeklärt bzw. geschult werden und die Einhaltung der Bestimmungen durch die bzw. den Datenschutzbeauftragten (DSB) kontrolliert wird.

Mit Hilfe dieses DS-Handbuches, das auf dem Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) basiert, soll die große Bedeutung des Datenschutzes an der FH JOANNEUM betont werden. Gleichzeitig hat diese Richtlinie das Ziel, eine Überregulierung zu vermeiden und durch den Grundsatz der Verhältnismäßigkeit lebbar und kontrollierbar zu sein.

Aus Gründen der einfacheren Lesbarkeit und der Textökonomie werden alle an der FH JOANNEUM mit der Verarbeitung von Daten betrauten Personen (Studentinnen und Studenten, Mitarbeiterinnen und Mitarbeiter, Administratorinnen und Administratoren etc.) im Folgenden als »Datenverarbeitende« bezeichnet.

Im vorliegenden DS-Handbuch werden Anleitungen und Empfehlungen für Datenverarbeitende, bzw. kurze Zusammenfassungen davon, mit diesem Symbol gekennzeichnet

Dieses DS-Handbuch gilt uneingeschränkt für alle Standorte der FH JOANNEUM.

Kapitel 2

Verantwortlichkeiten

Alle Datenverarbeitenden an der FH JOANNEUM sind verpflichtet, die im vorliegenden DS-Handbuch sowie die im DSG 2000 definierten Bestimmungen in ihrer jeweils gültigen Fassung einzuhalten und die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten der FH JOANNEUM bei jedem Vorfall durch den die Sicherheit der verarbeiteten Daten gefährdet ist (auch bei Verdacht), unverzüglich zu kontaktieren. Dies ist insofern wichtig, als dass der Mißbrauch, aber auch der Verlust von Daten für die FH JOANNEUM nach geltendem Recht teilweise schwerwiegende Konsequenzen nach sich ziehen kann.

Vorfälle, durch die die Sicherheit verarbeiteter Daten gefährdet werden kann, sind (demonstrativ):

- Virenbefall von Geräten, die im EDV-Netzwerk der FH JOANNEUM zur Datenverarbeitung verwendet werden (PCs, mobile Endgeräte und ähnliches, auch im privaten Eigentum).
- Verlust oder Diebstahl von Rechnern, Datenträgern, Passwörtern oder Schlüsseln (insbesondere auch Zugangscodes, Chip- oder Magnetkarten).
- Sonstige Sicherheitsvorfälle (z.B. Einbruch in Räumlichkeiten der FH JOANNEUM).

Alle Datenverarbeitenden der FH JOANNEUM haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer Tätigkeit an der FH JOANNEUM anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis, § 15 Abs 1 DSG 2000). Diese Verpflichtung behält auch nach Beendigung des Dienstverhältnisses ihre Gültigkeit.

Weiters sind alle Datenverarbeitenden der FH JOANNEUM verpflichtet, die im Intranet der FH JOANNEUM veröffentlichten Organisations-, IT-, EDV- und Passwortrichtlinien zu befolgen.

Wichtige Links zu Richtlinien der FH JOANNEUM finden sich in Kapitel 5.1 dieses Handbuches

2.1 Leiterinnen und Leiter von Organisationseinheiten

Als Leiterinnen und Leiter im Sinne dieses DS-Handbuches gelten alle Personen, die eine Organisationseinheit der FH JOANNEUM mit Verantwortung für andere Personen (Studentinnen und Studenten, Mitarbeiterinnen und Mitarbeiter bzw. Lehrende) leiten.

Alle Leiter und Leiterinnen tragen die Verantwortung für den Datenschutz in ihrem Zuständigkeitsbereich. Dies umfasst die Verantwortung für die in ihrem Verantwortungsbereich tätigen Personen aber auch für sämtliche zur Verarbeitung von Daten eingesetzte Anwendungen, Dateien und Systeme.

Jede Leiterin und jeder Leiter muss die bzw. den DSB der FH JOANNEUM über die Vorgänge in ihrem bzw. seinem Bereich informieren, in denen personenbezogene Daten ermittelt, verarbeitet oder gespeichert werden, sofern diese nicht unter die Verwendung für wissenschaftliche Forschung und Statistik (wie in Abschnitt 3.3 beschrieben) fallen. Dies ist nötig, damit der oder die DSB die rechtmäßige Verwendung überprüfen kann.

Informationen zu den Informationspflichten der Leiter und Leiterinnen finden sich in diesem Dokument. Außerdem werden in unregelmäßigen Abständen Informationsveranstaltungen abgehalten. Des weiteren kann bei Unklarheiten bezüglich des Datenschutzes jederzeit der oder die Datenschutzbeauftragte bzw. die Personal- und Rechtsabteilung kontaktiert werden.

2.2 Administratorinnen und Administratoren

Administratorinnen und Administratoren der FH JOANNEUM sind verpflichtet, dafür Sorge zu tragen, dass der Zugriff auf Systeme in ihrem Verantwortungsbereich mit denen per-

sonenbezogene Daten verarbeitet oder gespeichert werden, nur dazu berechtigten Datenverarbeitenden und nur im Umfang der persönlichen Rechte dieser Datenverarbeitenden möglich ist. Diese Systeme (Software, Hardware, Räume etc.) sind dazu mit Identifikations- und Authentifizierungsmaßnahmen sowie bei Bedarf (unterschiedliche Rechte auf Daten) mit Rollenkonzepten zu versehen und in jedem Fall mit technisch aktuellen Mitteln gegen Angriffe zu schützen (z.B. durch die Installation von Virenschutzprogrammen und Firewalls). Änderungen an den zentralen, datenverarbeitenden Systemen müssen der jeweiligen Systemversion zuordenbar dokumentiert werden.

Vor dem produktiven Einsatz neuer Komponenten an der FH JOANNEUM, ist auf deren Tauglichkeit in Bezug auf den Schutz personenbezogener Daten zu achten. Dabei ist auch darauf zu achten, ob eine aktuelle, vollständige und auch für fachkundiges Vertretungspersonal verständliche Dokumentation der Komponente verfügbar ist und die Komponente die erforderlichen Protokollierungsmechanismen (siehe Abschnitt 3.5.7 dieses Handbuches) zur Verfügung stellt.

Weiters liegt es im Verantwortungsbereich der Administratorinnen und Administratoren, für sämtliche in ihrem Verantwortungsbereich eingesetzten Komponenten regelmäßig zu überprüfen, ob neue Sicherheitsupdates verfügbar sind, und deren Beschaffung und Installation zu veranlassen.

Die Administratorinnen und Administratoren der FH JOANNEUM sind aufgrund ihrer Tätigkeit notwendigerweise mit großzügigen Rechten ausgestattet. Sie sind deshalb verpflichtet, mit den ihnen zur Verfügung stehenden Administratorrechten besonders sorgfältig umzugehen und für Systeme gezielt, d.h. nur in Fällen, die dies auch erfordern, zu verwenden. Generell gilt der Grundsatz, dass mit der geringsten benötigten Berechtigungsstufe gearbeitet werden soll.

Vor dem Zugriff auf Sitzungen von angemeldeten Benutzern auf Systemen im Netzwerk der FH JOANNEUM (z.B. mittels »Remote Desktop«, KVM-Switches oder Konsolen von Virtualisierungssoftware) bzw. auf Geräte die nicht im Eigentum der FH JOANNEUM stehen, muss die Zustimmung der respektive des Datenverarbeitenden bzw. der Eigentümerin respektive des Eigentümers eingeholt werden.

2.3 Betriebsrätinnen und Betriebsräte

Einige Maßnahmen im Bereich der Datenverarbeitung bedürfen vor ihrer Einführung der Zustimmung in Form einer Betriebsvereinbarung des Betriebsrates (Kollegialorgans) der FH JOANNEUM:

- Die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmerinnen und Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren (§ 96 Abs 1 Z 3 ArbVG).
- Die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der Arbeitnehmerinnen und Arbeitnehmer, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen (§ 96a Abs 1 Z 1 ArbVG).
- Die Einführung von Systemen zur Beurteilung von Arbeitnehmerinnen bzw. Arbeitnehmern der FH JOANNEUM, sofern mit diesen Systemen Daten erhoben werden, die nicht durch die betriebliche Verwendung gerechtfertigt sind (§ 96a Abs 1 Z 2 ArbVG).

Keine der oben genannten Maßnahmen kann an der FH JOANNEUM eingeführt werden, ohne dass der Betriebsrat der FH JOANNEUM vorab darüber informiert wurde und dieser Maßnahme auch aktiv zugestimmt hat. Der Betriebsrat ist verpflichtet, die geplanten Maßnahmen sorgfältig zu prüfen und über die Einführung zu entscheiden.

2.4 Datenschutzausschuss

Um die Sicherheit der Daten von Angestellten, Lehrbeauftragten, Studierenden und Forschungspartnern zu gewährleisten, wurde an der FH JOANNEUM ein Datenschutzausschuss (DSA) eingerichtet.

Dieser Datenschutzausschuss ist eine Vertrauensinstanz für die Verwendung von personenbezogenen und sonstigen schutzbedürftigen Daten an der FH JOANNEUM, sowohl Studierenden- als auch MitarbeiterInnendaten betreffend.

Er legt allenfalls notwendige Reglementierungen für die Datenanwendungen von Studierenden- und MitarbeiterInnendaten fest. Insbesondere obliegt es dem Datenschutzausschuss zu

bestimmen, welche Sammlungen und Auswertungen von MitarbeiterInnendaten und Studierendendaten vorgenommen bzw. welche Einsichtnahmen vorgenommen werden dürfen, unter Berücksichtigung der gesetzlichen Bestimmungen.

Außerdem zählt zu seinen Aufgaben, Richtlinien für die Verwendung von personenbezogenen und sonstigen schutzwürdigen Daten (wie z.B. aus dem Bereich F&E) an der FH JOANNEUM herauszugeben, sich mit Problemstellungen mit Datenschutzrelevanz zu befassen und eine Bewusstseinsbildung für den Bereich Datenschutz und -sicherheit zu erreichen. Die Initiierung geeigneter Maßnahmen zur Durchsetzung obiger Regelungen, um die IT-Sicherheit zu erhöhen und Verstöße gegen den Datenschutz zu unterbinden, liegt ebenfalls im Aufgabenbereich des DSA.

Der Ausschuss setzt sich derzeit aus den folgenden Mitgliedern aufgrund ihres Amtes und den entsendeten Mitgliedern folgender Gremien zusammen:

- RektorIn / wissenschaftlicheR GeschäftsführerIn
- KaufmännischeR GeschäftsführerIn
- Vize-RektorIn
- DatenschutzbeauftragteR
- ein ständiger Vertreter oder eine ständige Vertreterin des Betriebsrates
- ein ständiger Vertreter oder eine ständige Vertreterin der Personal- und Rechtsabteilung
- ein ständiger Vertreter oder eine ständige Vertreterin der zentralen IT
- je eine Person aus den im Kollegium vertretenen Gruppen (StudiengangsleiterInnen, Lehrende, Studierende)

Die Gremien haben auch jeweils ein Ersatzmitglied nominiert. Alle Mitglieder des Datenschutzausschusses verfügen über ein gleich gewichtetes Stimmrecht. Bei Bedarf können weitere Personen (Experten und Expertinnen) hinzugezogen werden. Nähere Aufgaben und Regelungen des Datenschutzausschusses finden sich in dessen Geschäftsordnung (siehe Organisationshandbuch).

Es ist jedoch zu beachten, dass der Datenschutzausschuss keine rechtliche Entscheidungskompetenz hat, sondern als beratendes Organ der Geschäftsführung dient.

2.5 Datenschutzbeauftragte

Formell gesehen, ist der/die Datenschutzbeauftragte die Geschäftsstelle des Datenschutzausschusses der FH JOANNEUM und ist damit dessen Kontaktstelle innerhalb der FH. Das bedeutet, MitarbeiterInnen und Studierende können sich mit allen Fragen und Angelegenheiten des Datenschutzes jederzeit an den/die DSB wenden. Er/Sie ist nicht berechtigt, verbindliche rechtliche Auskünfte zu geben, wird aber Anfragen dementsprechend weiterleiten und sich dafür einsetzen, anstehende Fragen – in Zusammenarbeit mit z.B. der Geschäftsführung, der Personal- und Rechtsabteilung oder Dritten – zu klären. Die bzw. der Datenschutzbeauftragte berät die Geschäftsführung der FH JOANNEUM bei Entscheidungen im Bereich des Datenschutzes.

Die bzw. der DSB wird bei ihrer bzw. seiner Tätigkeit vom Datenschutzausschuss der FH JOANNEUM unterstützt und arbeitet zur Informationsbeschaffung intensiv mit den zuständigen zentralen Services, wie z.B. der ZIT bei Fragen zur Umsetzung von Projekten die die IT-Infrastruktur an der FH JOANNEUM betreffen oder der Abteilung für Personal und Recht bei rechtlichen Fragen zum Thema Datenschutz zusammen und publiziert die geltenden Grundsätze des Datenschutzes der FH JOANNEUM im Datenschutzhandbuch sowie der Datenschutzerklärung.

Die Mitwirkungsbereiche der bzw. des Datenschutzbeauftragten umfassen im Wesentlichen:

- Erstellung, Wartung und Publikation der Datenschutzerklärung und des Datenschutzhandbuches
- Schulung und Kontrolle von Datenverarbeitenden
- Beratung in Datenschutzangelegenheiten
- Bearbeitung von Auskunftsanfragen
- Prüfung von datenschutzrelevanten Vorgängen an der FH JOANNEUM
- Prüfung und Genehmigung von Ausnahmeregelungen
- Mitgestaltung datenschutzrelevanter Prozesse
- Einhaltung gesetzlicher Pflichten (Meldungen/Genehmigungen).

Der bzw. die Datenschutzbeauftragte hat in seiner bzw. ihrer Funktion keine anderen Zugriffsrechte auf Daten als andere MitarbeiterInnen oder Studierende und er/sie kann und darf weder Personalakten, Dateien oder andere personenbezogene Informationen anderer einsehen.

Die meisten Verstöße gegen den Datenschutz werden aus Unwissenheit und fehlenden oder falschen Informationen begangen. Es geht daher darum, durch präventive Maßnahmen, wie Regelungen und die Zurverfügungstellung von Informationen, den Datenschutz und die Datensicherheit zu gewährleisten. Der bzw. die Datenschutzbeauftragte arbeitet daher gemeinsam mit allen am Datenschutz Interessierten miteinander daran, innerhalb der FH JOANNEUM einen gesetzeskonformen Umgang mit personenbezogenen Daten zu bewahren und soll als Unterstützung in Hinblick auf Datenschutzrelevanz gesehen werden.

Kapitel 3

Umgang mit personenbezogenen Daten

Zur Wahrung des Grundrechtes auf Geheimhaltung von personenbezogenen Daten (§ 1 Abs 1 DSG 2000) wurden an der FH JOANNEUM Grundsätze für die Ermittlung, Verarbeitung und Nutzung dieser Daten definiert. Das wichtigste Prinzip dabei ist, dass personenbezogene Daten – sofern sie nicht aus anderen öffentlichen Datenquellen stammen – nur aus gesetzlichen Bestimmungen heraus, oder mit Zustimmung der Betroffenen für einen bestimmten Zweck verwendet werden dürfen und danach umgehend wieder gelöscht werden müssen.

3.1 Verwendung von Daten

§ 4 Z1 DSG 2000 definiert Daten bzw. personenbezogene Daten als »Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist«. Voraussetzung für die Zulässigkeit der Verwendung von Daten ist gemäß § 7 DSG 2000, dass Zweck und Inhalt der Datenanwendung von den rechtlichen Befugnissen der FH JOANNEUM gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der bzw. des Betroffenen nicht verletzt werden.

Als Kontaktperson für Fragen in Bezug auf die Rechtmäßigkeit der Verwendung von Daten steht Ihnen die bzw. der DSB der FH JOANNEUM (datenschutz@fh-joanneum.at) gerne zur Verfügung.

3.1.1 Sensible Daten

Sensible Daten, also Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben dürfen an der FH JOANNEUM nur dann verwendet werden, wenn zumindest eines der in § 9 DSG 2000 taxativ aufgezählten Tatbestandsmerkmale erfüllt ist.

Die Verwendung von Daten an der FH JOANNEUM ist unter folgenden Voraussetzungen zulässig:

- Die bzw. der Betroffene hat die Daten offenkundig selbst öffentlich gemacht.
- Die Daten werden in nur indirekt personenbezogener Form verwendet.
- Die bzw. der Betroffene hat seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt.
- Die Daten werden für wissenschaftliche Forschung oder Statistik gemäß § 46 DSG 2000 verwendet.
- Die Verwendung ist erforderlich, um Rechten und Pflichten auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen.

3.1.2 Nicht-sensible Daten

Nicht-sensible Daten dürfen gemäß § 8 DSG 2000 an der FH JOANNEUM unter anderem dann verwendet werden, wenn eine der folgenden Bedingungen erfüllt ist:

- Es wurde eine Zustimmung der bzw. des Betroffenen in Kenntnis der Sachlage für den konkreten Fall erteilt und nicht widerrufen.
- Es handelt sich um zulässigerweise veröffentlichte Daten oder um nur indirekt personenbezogene Daten, bei denen die Identität der bzw. des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann.
- Die Verwendung der Daten ist zur Erfüllung einer vertraglichen Verpflichtung zwischen der FH JOANNEUM und der Betroffenen bzw. dem Betroffenen erforderlich.

3.1.3 Andere kritische Daten

An der FH JOANNEUM werden darüber hinaus noch weitere wichtige Daten verarbeitet, die für den Betrieb der Hochschule von großer Bedeutung sind. Dies sind insbesondere Daten über den Inhalt von Forschungsprojekten, aber auch nicht personenbezogene vertrauliche Daten (wie z.B. Finanz- oder Strategiedaten), sowie Daten die der FH JOANNEUM von Dritten zur Verarbeitung anvertraut wurden. Solche Daten fallen teilweise nicht unter das österreichische Datenschutzgesetz, da ein direkter oder indirekter Personenbezug fehlt. Trotzdem sind die in den nachfolgenden Kapiteln beschriebenen Verhaltensweisen auch auf diese Art von Daten – egal ob personenbezogen oder nicht – anzuwenden.

3.2 Überwiegend berechtigte Interessen

Der § 1 des DSG regelt das Grundrecht auf Geheimnisschutz für alle personenbezogenen Daten. In dieses Grundrecht darf nur aus drei Gründen eingegriffen werden: lebenswichtige Interessen des bzw. der Betroffenen (was in unserem Fall i.d.R. nicht zutrifft), Zustimmung der bzw. des Betroffenen und überwiegend berechtigte Interessen eines bzw. einer Anderen. Die Zustimmung der Betroffenen wird für die meisten personenbezogenen Daten im Rahmen von Interessenserklärung, Bewerbung und Aufnahme eines Studiums eingeholt bzw. ergibt sich durch rechtliche Pflichten der FH JOANNEUM.

Des weiteren ist es möglich personenbezogene Daten auch mit dem Argument des »überwiegend berechtigten Interesses« zu verarbeiten. Hierzu gibt der Gesetzgeber allerdings keine klaren Regelungen, daher ist die Verarbeitung unter dieser Begründung mit Vorsicht und nur nach Rückfrage bei der Personal- und Rechtsabteilung oder dem DSB anzuwenden.

- Beispiel: Die Zugriffe von Studierenden in einer Online-Learning-Applikation werden gespeichert, ohne dass diese dem explizit zugestimmt haben. Es ist das überwiegend berechtigte Interesse eines Lehrenden oder einer Lehrenden zu wissen, welche Dokumente sich Studierende angesehen haben.
- Beispiel: Ein Lehrender oder eine Lehrende möchte Zugriff auf die privaten eMail-Adressen der Studierenden bekommen um mit ihnen im Rahmen der Lehrveranstaltung kommunizieren zu können. Hier gibt es kein überwiegend berechtigtes Interesse, da allen Studierenden offizielle FH-eMail-Adressen zur Verfügung gestellt werden.

3.3 Verwendung von Daten für die wissenschaftliche Forschung und Statistik

Im Rahmen der Lehre und Forschung wird an der FH JOANNEUM häufig mit personenbezogenen Daten wie in Abschnitt 3.1 definiert, gearbeitet. Darunter fallen auch z.B. alle Bakkalaureats- und Diplomarbeiten in denen Studierende personenbezogene Daten durch Umfragen erheben. Der Gesetzgeber sieht für die Verwendung in der wissenschaftlichen Forschung Ausnahmen gegenüber der z.B. kommerziellen Verwertung vor. Dies bedeutet aber nicht, dass man im Namen der Wissenschaft keinen Beschränkungen mehr unterworfen wäre.

Der § 46 DSG 2000 regelt diesen Bereich der Datenverarbeitung genau. Es gilt nach wie vor eine klare Beschränkung über die Erhebung von Daten, selbst dann wenn die Ergebnisse anonymisiert dargestellt werden. Daten, die nicht über besondere gesetzliche Vorschriften oder mit spezieller Genehmigung der Datenschutzkommission erhoben werden bzw. öffentlich zugänglich sind, dürfen weiterhin nur mit vorliegender Zustimmung der Betroffenen gesammelt werden.

Ausnahmen für die Forschung und Statistik sehen aber vor, dass Daten auch verwendet werden dürfen, wenn diese für den Forscher oder die Forscherin nur indirekt personenbezogen

vorliegen, auch wenn diese zuvor bereits für andere Untersuchungen legal erhoben wurden. Damit wird ermöglicht, dass umfangreiche, erhobene Daten relativ einfach für mehrere Auswertungen und statistische oder wissenschaftliche Fragestellungen herangezogen werden können, ohne dass dafür eine erneute Genehmigung der betroffenen Personen eingeholt werden müsste.

Im Absatz 5 des § 46 DSG 2000 findet sich noch ein wichtiger Hinweis für die wissenschaftliche Praxis: Selbst wenn die Daten rechtmäßig erhoben wurden, »*ist der direkte Personenbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anders vorgesehen, ist der Personenbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.*«

- Achten Sie bei dem Fragebogendesign bereits darauf, dass möglichst kein Personenbezug hergestellt werden kann.
- Stellen Sie – wenn möglich – nicht vollständige Rohdaten von Umfragen für weitere Auswertungen z.B. für Studierende zur Verfügung, wenn aus diesen Daten ein Personenbezug ableitbar ist.
- Stellen Sie bei Zustimmungserklärungen für Interviews oder andere Datenerhebungen sicher, dass die jeweilige Person auch ihr schriftliches Einverständnis für die weitere Verarbeitung der Daten gibt.
- Achten Sie darauf, dass auch bei wissenschaftlichen Erhebungen für jede einzelne Studie in denen tatsächlich Daten personenbezogen gespeichert werden, eine Meldung beim Datenschutzregister durchzuführen ist. »Pauschalmeldungen« sind nicht zulässig.

3.4 Verbot von automatisierten Einzelentscheidungen

Gemäß § 49 Abs 1 DSG 2000 darf niemand einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte seiner Person ergeht.

Dieses Verbot bezieht sich insbesondere auf die Bewertung und Auswahl von Bewerberinnen und Bewerbern, sowohl im Bereich der Studierenden als auch des Personals. Die letzte Entscheidung muss in solchen Fällen immer von Menschen getroffen werden.

3.5 Gewährleistung der Datensicherheit

Die in § 14 DSG 2000 geforderte Gewährleistung der Datensicherheit wird an der FH JOANNEUM durch die nachfolgend beschriebenen Maßnahmen sichergestellt. Die Maßnahmen sind unter dem Aspekt der wirtschaftlichen Vertretbarkeit und der Bedingung, dass damit dem Stand der technischen Möglichkeiten Rechnung getragen wird, gewählt und werden laufend dahingehend überprüft.

3.5.1 Festlegung der Aufgabenverteilung

Die Aufgabenverteilung bei der Datenverwendung zwischen Organisationseinheiten sowie zwischen Mitarbeiterinnen und Mitarbeitern der FH JOANNEUM wird durch die für die jeweiligen Organisationseinheiten verantwortlichen Leiter und Leiterinnen ausdrücklich (mündlich oder schriftlich) festgelegt.

Bei Unklarheiten in Bezug auf die Aufgabenverteilung wenden Sie sich bitte an Ihre Vorgesetzte bzw. Ihren Vorgesetzten.

3.5.2 Auftrag für Datenverwendung

Personenbezogene Daten werden an der FH JOANNEUM nur dann verwendet, wenn dazu gültige Aufträge der jeweils anordnungsbefugten Organisationseinheiten bzw. Mitarbei-

terinnen oder Mitarbeiter vorliegen. Die Auftragserteilung kann mündlich, schriftlich oder konkludent erfolgen.

Bei Unklarheiten in Bezug auf den Auftrag für die Datenverwendung wenden Sie sich bitte an Ihre Vorgesetzte bzw. Ihren Vorgesetzten.

3.5.3 Belehrung über Datensicherheitsvorschriften

Dieses Handbuch dient auch zur Belehrung von Mitarbeiterinnen und Mitarbeitern im Sinne des § 14 Abs 2 Z 3 DSG 2000. Datenverarbeitende an der FH JOANNEUM verpflichten sich durch die Unterzeichnung ihres Dienstvertrags, die nach dem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten einzuhalten.

Bei Fragen betreffend die an der FH JOANNEUM geltenden Datensicherheitsvorschriften wenden Sie sich bitte an Ihre Vorgesetzte bzw. Ihren Vorgesetzten oder kontaktieren Sie die bzw. den DSB der FH JOANNEUM (datenschutz@fh-joanneum.at).

3.5.4 Zutrittsregelungen

Durch ein auf persönlichen Berechtigungen basierendes Raumzutrittskonzept mittels elektronischer Ausweise und Schlüssel wird an der FH JOANNEUM sichergestellt, dass Unbefugten der Zutritt zu Anlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt bleibt. Gleichzeitig miteintretende Personen müssen – sofern diese nicht selbst zutrittsberechtigt sind – von der Person, durch die der Zutritt gewährt wurde, überprüft und verantwortet werden. Die Weitergabe von Schlüsseln und Zutrittsausweisen an Dritte ist nicht zulässig. Räume in denen personenbezogene oder andere kritische Daten gelagert werden oder von denen aus Zugang zu solchen möglich ist, müssen von der letzten Person, die den Raum verlässt, versperrt werden.

- Nehmen Sie Personen nur mit in Räume bzw. geben Sie Personen nur dann Schlüssel weiter, wenn Ihnen bekannt ist, dass diese Personen über die dazu erforderlichen Berechtigungen verfügen.
- Versperren Sie Räume, wenn Sie sie als Letzte oder Letzter verlassen.

3.5.5 Zugriffsregelungen

An der FH JOANNEUM wird sichergestellt, dass der Zugriff auf Daten und Programme, mit denen personenbezogene Daten verarbeitet werden, nur mit entsprechender Berechtigung möglich ist und Datenträger, auf denen personenbezogene Daten gespeichert werden, vor der Einsicht und Verwendung durch Unbefugte gesichert sind.

Dies wird realisiert, indem die entsprechenden Systeme (Software, Hardware, etc.) mit Identifikations- und Authentifizierungsmaßnahmen, sowie bei Bedarf mit Rollenkonzepten versehen sind und gegen Angriffe geschützt werden (Virenschutzprogramme, Firewalls etc.).

Geben Sie sensible oder kritische Daten nur an Personen weiter, von denen Ihnen ausdrücklich bekannt ist, dass diese über die dazu erforderlichen Berechtigungen verfügen. Kennzeichnen Sie die Sensibilität der Daten unter Umständen entsprechend bzw. weisen Sie den Empfänger oder die Empfängerin darauf hin.

3.5.6 Betrieb von Datenverarbeitungsgeräten

Mittels auf Identifikations- und Authentifizierungsmaßnahmen basierenden Zugriffsberechtigungen wird sichergestellt, dass die Datenverarbeitungsgeräte der FH JOANNEUM vor Einsicht und Betrieb durch Unbefugte geschützt sind.

Personen mit speziellen Administrationsrechten (zentrale oder auch lokale Administrationsrechte, spezielle Berechtigungsadministrationsrechte auf Studiengangsebene, etc.) sind verantwortlich für Auswirkungen der von ihnen vergebenen Rechte.

3.5.7 Protokollierung von Verwendungsvorgängen

Verwendungsvorgänge wie Änderungen, Abfragen und Übermittlungen von personenbezogenen Daten müssen an der FH JOANNEUM aus Datensicherheitsgründen (§ 14 Abs 2 Z 7 DSG 2000) protokolliert werden. Die Protokollierung erfolgt nur dann manuell, wenn eine automatisierte Protokollierung nicht möglich ist. Auch datenschutzrelevante Aktionen auf Systemen mit denen Daten verarbeitet werden, wie beispielsweise das An- oder Abmelden von Benutzerinnen und Benutzern, werden damit automatisch protokolliert.

3.5.8 Dokumentation der Datensicherheitsmaßnahmen

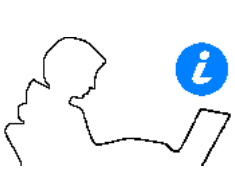
Um die Kontrolle und Beweissicherung zu erleichtern, werden die Details zu sämtlichen oben beschriebenen Maßnahmen zur Gewährleistung der Datensicherheit von der jeweils verantwortlichen Person bzw. vom DSB der FH JOANNEUM dokumentiert.

3.6 Aufbewahrung personenbezogener Daten

Daten werden an der FH JOANNEUM in personenbezogener Form nur solange aufbewahrt, als dies für den Zweck, für den die Daten erhoben wurden, oder aufgrund von gesetzlichen Verpflichtungen (Archivierung), erforderlich ist.

3.7 Recht auf Auskunft, Richtigstellung, Löschung und Widerruf

Jede bzw. jeder hat das Recht auf Auskunft darüber, welche Daten an der FH JOANNEUM über sie bzw. ihn verarbeitet werden, woher diese Daten stammen, wozu sie verwendet werden und an wen sie gegebenenfalls übermittelt werden. Weiters hat jede bzw. jeder das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten (§ 1 Abs 3 DSG 2000). Ebenso besteht das Recht, eine bereits erteilte Zustimmung zur Verarbeitung von Daten zu widerrufen (§ 8 - 9 DSG 2000).



Die bzw. der DSB der FH JOANNEUM (datenschutz@fh-joanneum.at) steht Ihnen als Kontaktperson für sämtliche diesbezüglichen Anliegen zur Verfügung.

3.8 Schutz der Daten von MitarbeiterInnen, Studierenden und BewerberInnen

Bewerbungsunterlagen und Daten von potentiellen MitarbeiterInnen und Studierenden, die nicht im Unternehmen tätig werden bzw. nicht zu studieren beginnen, sind nach Ablauf der Evidenz und wenn kein Einverständnis über das längere Aufbewahren vorliegt zu löschen.

Persönliche Daten werden auch nach einer Tätigkeit oder nach der Beendigung des Studiums nur solange aufbewahrt, wie es für den Verwendungszweck erforderlich ist. Ausgenommen davon sind lediglich diejenigen Daten, die aufgrund einer gesetzlichen Vorschrift aufzubewahren sind. Diese Ausnahme gilt jedoch nur für den jeweils gesetzlich vorgeschriebenen Zeitraum.

MitarbeiterInnen und Studierende haben Einsichtsrecht über die zur Person gespeicherten Daten und das Recht auf Richtigstellung nicht korrekt erfasster Daten. Die Daten von MitarbeiterInnen und Studierenden sind nur in den jeweils zuständigen Studiengängen und zentralen Einrichtungen gespeichert bzw. gesichert aufbewahrt. Außerdem ist sichergestellt, dass nur berechtigte Personen für einen bestimmten und notwendigen Zweck darauf Zugriff haben.

3.8.1 Ausscheiden einer Mitarbeiterin bzw. eines Mitarbeiters

Von der ausscheidenden Mitarbeiterin bzw. dem ausscheidenden Mitarbeiter sind sämtliche Unterlagen, ausgehändigte Schlüssel, MitarbeiterInnenausweis und zur Verfügung gestellte IT-Geräte (Speichermedien, Laptops etc.) zurückzugeben.

Es ist sicherzustellen, dass auf den von der FH JOANNEUM zur Arbeit zur Verfügung gestellten Geräten zur Datenverarbeitung, unternehmenswichtige Informationen nicht mehr lokal gespeichert sind. Alle notwendigen Daten für die Weiterführung der Arbeit durch eine andere Person müssen dem/der Vorgesetzten bzw. NachfolgerIn übergeben werden bzw.

sich geordnet auf einem zentralen Netzlaufwerk befinden, zu dem diese Personen Zugang haben. Die Daten auf dem bzw. den persönlichen Arbeitsgerät(en) können danach jederzeit gelöscht bzw. zur Sicherung und Durchsicht anderen Mitarbeitern und Mitarbeiterinnen der FH JOANNEUM zur Verfügung gestellt werden.

Außerdem sind alle eingerichteten Zugriffsberechtigungen zu entziehen bzw. zu löschen. Auch entsprechende Gruppenmitgliedschaften und damit verbundene Gemeinschaftsrechte sind zu entziehen.

Die ausscheidende Mitarbeiterin bzw. der ausscheidende Mitarbeiter ist nochmals darauf hinzuweisen, dass die eventuell zu Dienstbeginn oder im Laufe von Projekten unterschriebenen Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine im Rahmen der Tätigkeiten erhaltenen geheimen Informationen weitergegeben werden dürfen.

Im Falle einer Änderung des Beschäftigungsverhältnisses (z.B. andere Abteilung, andere Funktion, etc.) sind sofort mit dem Übertrittsdatum die Berechtigungen entsprechend zu ändern.

3.9 Schutz der Daten der FH JOANNEUM GmbH

An die FH JOANNEUM werden vielfach Anfragen um Überlassung von Daten (statistische Daten zu Lehre, Forschung und Finanzen) gerichtet. Beispielhaft können sich solche Anfragen beziehen auf

- Unternehmenskennzahlen (Umsatz, Betriebsaufwand, Anzahl der MitarbeiterInnen, Investitionen etc.)
- Statistische Daten zum Lehrbetrieb an der FHJ oder an einzelnen Studiengängen (Quantitative und qualitative Angaben über Lehrende, Lehrveranstaltungen, Studierende, Drop-Out-Zahlen, Entwicklungsprojekte für Lehrangebote etc.)
- Statistische Daten zu Forschung und Entwicklung an der FHJ (Auftragslage, Auftragseingang, Projektdaten, Informationen über FördergeberInnen und Fördervolumina u.ä.).

Manche der angefragten Daten sind öffentlich einsehbar (z.B. Jahresabschlussdaten im Firmenbuch), andere Daten sind Gegenstand von Veröffentlichungen der FH JOANNEUM (z.B.

Daten im jährlich erscheinenden Geschäftsbericht und der Wissensbilanz sowie Veröffentlichungen auf der Webseite der FHJ), bestimmte Daten sind nur zur Kenntnisnahme für einen bestimmten, eingeschränkten Personenkreis (z.B. Aufsichtsrat, Gesellschafter) bestimmt, viele Daten sind gar nicht zur Veröffentlichung bestimmt und daher geheim zu halten.

Um sicherzustellen, dass keine geheimhaltungsbedürftigen Daten an Externe weitergegeben werden, muss die Beantwortung derartiger Anfragen von der Geschäftsführung autorisiert werden. Die Entscheidung, welche Daten an den jeweiligen Anfragesteller (z.B. Statistik Austria, FHR, andere Hochschulen und F&E-Betriebe) weiter gegeben werden können, fällt in die ausschließliche Zuständigkeit der Geschäftsführung der FH JOANNEUM und daher sind Anfragen an die GEF weiter zu leiten.

Die Anfrage sowie ein Vorschlag zur Beantwortung ist daher möglichst rasch an die Geschäftsführung — via eMail oder als Hardcopy — weiter zu leiten. Die Geschäftsführung entscheidet darüber, ob weitere Stellen (z.B. PER, PRM, Stabstellen) mit der Beurteilung der Anfragebeantwortung befasst werden, oder ob die Anfragebeantwortung direkt frei gegeben wird. Die Freigabe eines Antwortvorschlages erfolgt formlos durch die GEF.

Kapitel 4

IT-Sicherheit

Die aktuellen Regeln und Richtlinien zur Nutzung der IT-Infrastruktur der FH JOANNEUM können im Intranet über die Seiten der ZIT (Zentrale IT-Services), insbesondere in der EDV-Ordnung, in ihrer jeweils gültigen Version abgerufen werden und sind zu befolgen. Im Folgenden werden daher nur die wichtigsten Grundsätze hinsichtlich der Gewährleistung einer sicheren Nutzung der IT-Infrastruktur in Bezug auf die Sicherheit von personenbezogenen Daten beschrieben.

Die nachfolgenden Abschnitte beziehen sich auf alle datenverarbeitenden Geräte, die im Netzwerk der FH JOANNEUM betrieben werden. Geräte im Bereich der Administration der ZIT stehen unter deren Verantwortung. Mitarbeiter und Mitarbeiterinnen die Geräte mit eigenen lokalen Administrationsrechten verwalten, sind für die entsprechende IT-Sicherheit wie sie in den nachfolgenden Abschnitten beschrieben wird selbst verantwortlich und haben für eine äquivalente Sicherheit wie die ZIT zu sorgen.

Wichtige Links zu Regeln und Richtlinien der FH JOANNEUM finden sich in Kapitel 5.1 dieses Handbuches.

4.1 Arbeitsplatz- und Datensicherung

4.1.1 Ablage von Daten

Allen Benutzerinnen und Benutzern im Netzwerk der FH JOANNEUM steht ein persönliches Laufwerk zur Ablage eigener Dokumente und Dateien zur Verfügung (Homeverzeichnis). Das persönliche Laufwerk wird an Werktagen täglich gesichert (Backup). Gespeicherte Dokumente und Dateien können eine begrenzte Anzahl von Tagen in die Vergangenheit reichend wiederhergestellt werden. Weitere Details dazu sind vom Helpdesk der ZIT erhältlich.

Wichtige Dokumente und Dateien sollten nicht auf lokalen Laufwerken (z.B. C: oder D:) der Rechner der FH JOANNEUM gespeichert werden, da diese nicht gesichert werden und außerdem für sämtliche Benutzerinnen und Benutzer ohne großen technischen Aufwand einsehbar sind.

Bei Betriebssystemen, bei denen die Dateinamenserweiterung eine wichtige Rolle spielt, ist die Anzeige so einzustellen, dass der Typ einer Datei (ausführbares Programm, Textdatei, etc.) sofort anhand der Namenserweiterung erkannt werden kann. Damit kann ein versehentliches Ausführen von z.B. als Textdatei getarnten, bösartigen Programmen leichter vermieden werden.

- Nutzen Sie Ihr persönliches Laufwerk (Z:) zur Ablage Ihrer persönlichen Dokumente und Dateien. Durch die automatische Sicherung können diese Dokumente auch im Fehlerfall (z.B. Virenbefall ihres Rechners) wieder hergestellt werden.
- Um die Dateinamenserweiterung in Windows anzuzeigen, deaktivieren Sie die Checkbox »Erweiterungen bei bekannten Dateitypen ausblenden« in den Ordneroptionen (unter Windows 7: Explorer – Organisieren – Ordner- und Suchoptionen – Ansicht).

4.1.2 Benutzerinnen- bzw. Benutzerkennung und Passwort

Die von der ZIT der FH JOANNEUM vergebene Benutzerinnen- bzw. Benutzerkennung sowie das von der jeweiligen Benutzerin bzw. dem jeweiligen Benutzer selbst gewählte Passwort sind geheim zu halten und dürfen keinesfalls weitergegeben werden. Ebenso darf die Funktion »Kennwort speichern« für das FH-Kennwort auf Rechnern der FH JOANNEUM sowie in installierten Programmen nicht verwendet werden, wenn dies vermeidbar ist. Das ist erforderlich, um zu verhindern, dass unbefugte Personen auf personenbezogene Daten oder andere vertrauliche Daten zugreifen können, da in vielen Fällen damit das Passwort im Klartext auf dem lokalen Rechner gespeichert werden würde.

Das Passwort ist entsprechend der in der von der ZIT veröffentlichten Passwortrichtlinie definierten Passwort-Konventionen zu wählen und in den dort vorgeschriebenen Abständen zu erneuern. Das an der FH JOANNEUM verwendete Passwort und auch die Benutzerkennung dürfen – soweit auswählbar – auf Systemen außerhalb der FH JOANNEUM nicht verwendet werden (z.B. für Dienste im WWW, private Computer, Webplattformen, etc.), um auch Angriffe von außen zu erschweren.

Auch die eMail-Adressen von Benutzerinnen und Benutzern der FH JOANNEUM dürfen nur für dienst- oder studienbezogene Tätigkeiten verwendet werden, da ansonsten auch damit das Spam- und Angriffsaufkommen erhöht wird.

- Verwenden Sie nach Möglichkeit auch bei externen Webanwendungen überall verschiedene und komplexe Passwörter. Es ist besser, schwierige Passwörter zu notieren oder zu speichern, als überall einfach das gleiche zu verwenden.
- Stellen Sie sicher, dass diese Passwörter – aber auch Inhalte anderer Möglichkeiten der BenutzerInnenauthentifizierung wie bei Public-Key-Verfahren o.ä. – gesichert (versperrt) und für andere unzugänglich verwahrt werden.
- Bei der Verwendung eines Passwort- oder Key-Managers muss das Master-Passworts mindestens den Passwort-Konventionen der FH JOANNEUM genügen.
- Für Fragen und Anliegen zu diesem Thema steht der Helpdesk der ZIT der FH JOANNEUM jederzeit gerne zur Verfügung.

4.1.3 Arbeitsplatzsicherung

Alle Benutzerinnen und Benutzer haben sich auf Systemen der FH JOANNEUM mit ihrer persönlichen Kombination aus Benutzerinnen- bzw. Benutzerkennung und Passwort anzumelden. Beim Verlassen des Arbeitsplatzes ist dieser zu sperren, beim Verlassen der FH JOANNEUM sollte sich die jeweilige Benutzerin bzw. der jeweilige Benutzer auch abmelden (bzw. aus ökologischen und ökonomischen Gründen auch den Rechner herunterfahren).

In Bereichen mit Publikumsverkehr (z.B. Sekretariate, Infostellen) sind Monitore, Drucker, Faxgeräte, aber auch Dokumentenablagen so aufzustellen, dass das Risiko der Einsichtnahme Unbefugter möglichst ausgeschlossen ist.

- Mit Hilfe von Tastenkombinationen (Windows: »Windowstaste+L«, Linux: z.B. »STRG+ALT+L«) können Rechner schnell und einfach gesperrt werden.
- Wenn nicht bereits von der ZIT installiert, verwenden Sie zusätzlich Bildschirmschoner, die nach einer fix definierten Wartezeit automatisch aktiviert werden und die nur mittels Passworteingabe wieder deaktiviert werden können.

4.1.4 Versehentliche Dateneinsicht

Benutzerinnen oder Benutzer, die aufgrund einer Störung oder Fehlbedienung Zugang zu Daten oder Mitteilungen erhalten, die nicht für sie bestimmt sind, dürfen diese nicht einsehen, kopieren, manipulieren oder weiterleiten.

Sollten Sie versehentlich Einsicht in nicht für Sie bestimmte Daten erlangen, informieren Sie bitte umgehend die ZIT der FH JOANNEUM sowie ggf. die Absenderin bzw. den Absender der Daten über das Versehen.

4.2 Internet und eMail

Die Benutzerinnen und Benutzer sind berechtigt, das eMail System sowie den Internet-Zugang der FH JOANNEUM zu verwenden, solange dabei nicht gegen geltendes Österreichisches Recht verstoßen und zusätzlich die EDV-Ordnung der FH JOANNEUM eingehalten wird.

Die Arbeitsplätze, über die auf das Internet zugegriffen wird, müssen mit einem aktuellen, aktiven Virenscanner ausgestattet sein. Der verwendete Browser muss so konfiguriert sein, dass ein möglichst hohes Maß an Sicherheit gewährleistet ist. Dies gilt insbesonders für Viren- und Malware-gefährdete Systeme wie Windows.

Bei der Übermittlung von personenbezogenen oder vertraulichen Daten per eMail oder über das Internet müssen entsprechende Sicherheitsvorkehrungen getroffen werden (z.B. sichere, verschlüsselte Datenübertragung).

Auch ist dabei zu beachten, dass eine automatisierte Weiterleitung von eMails an externe Anbieter dazu führen kann, dass das DSG verletzt wird, indem z.B. personenbezogene Daten, die unverschlüsselt und vermeintlich intern versendet werden, dadurch an einen Anbieter in Übersee weitergeleitet und dort gespeichert werden.

Die ZIT der FH JOANNEUM behält sich das Recht vor, Details zum eMail Verkehr (Absender, Empfänger, Zeitstempel und Größe, keinesfalls jedoch die Nachrichten selbst), sowie die Adressen besuchter Websites (ohne deren Inhalt und ohne einen direkten Personenbezug) zu Statistikzwecken und um mögliche Angriffe zu detektieren zu protokollieren.

- Archivieren bzw. löschen Sie Ihre eMails regelmäßig.
- Führen Sie regelmäßig die von den Betriebssystemherstellern veröffentlichten Sicherheitsupdates durch.
- Deaktivieren Sie nach Möglichkeit aktive Inhalte (z.B. ActiveX) und Skriptsprachen (z.B. Visual Basic Script) in Ihrem Browser und nutzen Sie dessen Sicherheitsfunktionen.
- Bei Problemen mit dem Zertifikat einer vermeintlich sicheren Website (Information durch den Browser) stoppen Sie im Zweifelsfall bitte die geplante Transaktion und wenden Sie sich an den Helpdesk der ZIT der FH JOANNEUM.
- Klicken Sie nur auf Links in eMails und öffnen Sie nur dann eMail Attachments, wenn Ihnen die wahre Absenderin bzw. der wahre Absender bekannt ist oder Sie die eMail bzw. das Attachment erwarten.
- Um Adressdatenmissbrauch zu vermeiden, verwenden Sie das Feld »BCC« anstelle des Feldes »An«, wenn Sie ein eMail an mehrere, einander unbekannte Empfängerinnen bzw. Empfänger verschicken. Die Empfängerinnen bzw. Empfänger erhalten dadurch keine Information über weitere Empfängerinnen bzw. Empfänger derselben Nachricht.

4.3 Software

Allen Benutzerinnen und Benutzern ist es ausdrücklich untersagt, Software ohne Berechtigung oder von zweifelhaften Quellen zu installieren oder zu kopieren, sowie Software ohne gültige Lizenz auf Geräten der FH JOANNEUM zu verwenden. Software aus zweifelhaften Quellen ist sehr oft mit Viren oder Spyware versehen, die heutzutage eine der größten Gefahren im Internet darstellen.

- Nutzen Sie die vom jeweiligen Softwareprodukt angebotenen Sicherheitsfunktionen (z.B. Vergabe von Passwörtern für den Zugriff, automatische Speicherung von Zwischenergebnissen oder Verschlüsselungsmechanismen).
- Lassen Sie veröffentlichte Sicherheitsupdates für die eingesetzten Softwareprodukte – wenn möglich automatisch – installieren.

4.4 Virenschutz

Zum Schutz vor Viren sind alle Arbeitsplätze der FH JOANNEUM mit Windows als Betriebssystem mit Virenscannern ausgestattet, die bei jedem Startvorgang automatisch mit gestartet werden und nicht deaktiviert werden dürfen. Alle Benutzerinnen und Benutzer sind dafür verantwortlich, Vireninfektionen zu verhindern.

Von Viren befallene Wechselmedien dürfen an Arbeitsplätzen der FH JOANNEUM nicht verwendet werden (Prüfung vor Verwendung). Ebenso sind Dateien beim Download aus dem Internet, sowie per eMail erhaltene Dateien, besonders zu prüfen. Bitte wenden Sie sich im Zweifelsfall an den ZIT Helpdesk.

- Führen Sie regelmäßig die von den Anbietern von Virenscannern veröffentlichten Sicherheitsupdates durch bzw. aktivieren Sie nach Möglichkeit ein automatisches Update.
- Überprüfen Sie sämtliche nicht selbst erstellte Dateien bzw. Datenträger vor der Verwendung mit Hilfe eines Virenscanners, wenn dies nicht der Virenscanner schon selbständig durchführt (»On-Access-Scanning«).
- Bei Problemen mit der Beseitigung von Viren mittels Virenscanner oder bei Verdacht einer Vireninfektion kontaktieren Sie bitte den Helpdesk der ZIT der FH JOANNEUM.

4.5 Remote Access

Die FH JOANNEUM stellt den Benutzerinnen und Benutzern einen externen Zugang zum Netzwerk der FH JOANNEUM zur Verfügung. Die Benutzerinnen und Benutzer sind verpflichtet, bei der bzw. durch die Nutzung dieses Zugangs nicht gegen geltendes Österreichisches Recht zu verstoßen und den Zugang keinesfalls betriebsfremden Personen zugänglich zu machen. Der verwendete PC muss mit einem aktuellen, aktiven Virenscanner – insbesondere bei Windows-Computern – entsprechend der Vorgaben der ZIT der FH JOANNEUM, sowie allen aktuellen Sicherheitsaktualisierungen ausgestattet sein.

Wichtige Links zu Richtlinien der FH JOANNEUM finden sich in Kapitel 5.1 dieses Handbuches.

4.6 Mobile Datenträger

Mobile Datenträger wie z.B. USB-Sticks, Mobiltelefone, externe Festplatten und Laptops stellen eine besondere Herausforderung für den Datenschutz dar, da das Risiko des Verlustes oder Diebstahls relativ hoch ist. Nachdem man im Laufe des Datenträgerlebens nie davon

ausgehen kann, dass immer nur »unwichtige« Daten darauf gespeichert werden, sind – soweit technisch möglich – alle mobilen Datenträger zur Gänze (und nicht nur einzelne Verzeichnisse) mit starken kryptografischen Methoden zu verschlüsseln.

- Stellen Sie sicher, dass mobile Datenträger stets zugriffs- und diebstahlsgeschützt aufbewahrt werden (sperren bzw. versperren Sie diese).
- Für Fragen in Bezug auf Verschlüsselungsmethoden und -möglichkeiten wenden Sie sich bitte an den Helpdesk der ZIT der FH JOANNEUM.
- Bei Diebstahl oder Verlust von mobilen Datenträgern mit personenbezogenen Daten bzw. bei einem diesbezüglichen Verdacht ist unverzüglich bei der Polizei Meldung bzw. Anzeige zu erstatten. Kontaktieren Sie bitte danach die bzw. den DSB der FH JOANNEUM (datenschutz@fh-joanneum.at).

4.7 Öffentliche Cloud-Services

Viele Firmen bieten im Internet sogenannte Cloud-Services an. Zu den Anbietern gehören Firmen wie Google, Ubuntu, Dropbox, Microsoft, etc. Die angebotenen Dienste können – bei kleineren Datenmengen in den meisten Fällen sogar kostenlos – unter anderem zum Speichern von Office-Dokumenten, Dateien, persönlichen Kontaktdaten usw. verwendet werden. Mit der Möglichkeit der Freigabe dieser Dokumente für andere ergeben sich sehr einfache Möglichkeiten der Kooperation.

Probleme ergeben sich dadurch, dass hierbei die Daten an Dritte (in den meisten Fällen im Ausland, größtenteils in den USA) weitergegeben werden. Personenbezogene Daten (z.B. Daten von Studierenden, PatientInnen, AuftragsgeberInnen, ...) dürfen jedoch laut DSG – vereinfacht gesagt – nicht, oder nur mit Zustimmung der Betroffenen weitergegeben werden.

Teilweise unterscheiden sich die Anbieter hier in der technischen Ausführung essentiell voneinander, was die Verschlüsselung, aber auch die Server-seitigen Entschlüsselungsmöglichkeiten betrifft. Einige verschlüsseln Daten überhaupt nicht, manche übertragen sie über eine verschlüsselte Verbindung, speichern diese am Server jedoch so, dass eine Möglichkeit die Daten zu lesen für den Anbieter erhalten bleibt. Nur ganz wenige verschlüsseln die Daten bereits lokal und auch so, dass der Anbieter selbst diese nicht entschlüsseln kann. Will man dennoch Daten in der Cloud speichern, so sollte man sie selbst durch Zusatzsoftware lokal sicher verschlüsseln.

Sie sollten daher dienstliche, personenbezogene Daten keinesfalls in einer öffentlichen Cloud speichern. Seien Sie auch mit privaten Daten vorsichtig, insbesondere wenn es sich um sensible Daten wie Verträge, Fotos und ähnliches handelt.

- Achten Sie bei der Wahl des Anbieters auf Angaben zur Verschlüsselung von Daten bei der Übertragung und am Server und auf Angaben zur Möglichkeit der Entschlüsselung durch den Anbieter selbst.
- Stellen Sie sicher, dass allgemeine Daten die sie bei Cloud-Services speichern zumindest verschlüsselt übertragen werden.
- Verschlüsseln Sie die Daten nach Möglichkeit selbst lokal bevor sie in der Cloud gespeichert werden (unter Windows z.B. mit TrueCrypt, unter Linux oder MacOS z.B. mit *encfs*)

4.8 Videoaufzeichnungen

An der FH JOANNEUM wird zur Gebäude- und Diebstahlssicherung (»Eigentumsschutz«) ein automatisches Videoaufzeichnungssystem verwendet. Gebäude und Plätze die überwacht werden, sind durch spezielle, gesetzlich vorgeschriebene Warnaufkleber gekennzeichnet, welche die Möglichkeit eröffnen sollen, der Überwachung zu entgehen.

Die Vidoeüberwachung wird explizit *nicht* an Orten verwendet, die zum höchstpersönlichen Lebensbereich der Betroffenen gehören (z.B. Toiletten, Sozialräume, Umkleiden, etc.). Es erfolgt keine Überwachung von Mitarbeiterinnen und Mitarbeitern am Arbeitsplatz, auch nicht um das zeitgerechte Kommen und Gehen zu kontrollieren.

Bei der Aufzeichnung der Videos wird darauf geachtet, dass nur die relevanten Bereiche der Gebäude überwacht werden und nicht im Hintergrund zufällig Passanten mitgefilmt werden. Die Aufzeichnungen werden nach spätestens 72 Stunden gelöscht, wenn in der Zwischenzeit nicht z.B. ein eventueller Strafbestand gemeldet wird und damit die Aufzeichnungen zu Beweiszwecken weiterhin benötigt werden. Jeder Verwendungsvorgang von Videoaufzeichnungen wird protokolliert, d.h. dass jeder Zugriff auf die Aufzeichnungen schriftlich festzuhalten ist. Zugriffe sind außerdem nur bei einem konkreten Verdacht auf eine Straftat z.B. nach einer Diebstahlsmeldung erlaubt.

Melden Sie den Verdacht von Diebstählen oder ähnlichem unverzüglich, damit eventuell noch auf die Videoaufzeichnungen zurückgegriffen werden kann bevor diese gelöscht werden müssen.

4.9 Datenentsorgung

Alle Datenträger (z.B. Festplatten, USB-Sticks, aber auch Röntgenaufnahmen, Papier etc.) die personenbezogene oder andere kritische Daten enthalten, dürfen nicht ohne vorherige Unkenntlichmachung der darauf befindlichen Daten entsorgt werden. Für Großgeräte, die von der FH JOANNEUM verwaltet werden, geschieht dies durch die ZIT. Für kleine und mobile Datenträger (USB-Sticks, externe Festplatten) ist die Betreiberin bzw. der Betreiber selbst für die ordnungsgemäße und sichere Zerstörung der Daten verantwortlich. Für diesbezügliche Fragen steht der Helpdesk der ZIT der FH JOANNEUM jederzeit zur Verfügung.

Größere Papiermengen können in speziell dafür bereitgestellten, versperrten Containern entsorgt werden (werden von den Altpapiersammelstellen angeboten), kleinere Mengen sind mittels Dokumentenvernichter zu entsorgen.

Austauschbare Datenträger (CDs, DVDs etc.) sind deutlich zu beschriften um einen eventuell kritischen Inhalt leichter erkennen zu können.

- Entsorgen Sie Datenträger mit Daten, die falsch sind (z.B. fehlerhafte Ausdrucke) oder Daten, die nicht mehr benötigt werden.
- Zerstören Sie Datenträger und Papierdokumente mit personenbezogenen oder anderen kritischen Daten physisch, bevor Sie diese wegwerfen (z.B. zerschneiden, shreddern).
- Stellen Sie sicher, dass keine Datenträger mit personenbezogenen oder kritischen Daten (Notizzettel, Flipcharts, Whiteboards, CDs etc.) frei zugänglich sind (Ablagen bzw. Räume versperren).

Kapitel 5

Änderungen des DS-Handbuches und mitgeltende Dokumente

Die Erstellung, Wartung und Publizierung dieses DS-Handbuches liegt im Verantwortungsbereich der bzw. des Datenschutzbeauftragten (DSB) der FH JOANNEUM. Änderungswünsche sollen der bzw. dem DSB mitgeteilt werden (datenschutz@fh-joanneum.at). Sie werden von der bzw. dem DSB geprüft und gegebenenfalls eingearbeitet. Die jeweils gültige Fassung der Datenschutzrichtlinie wird von der bzw. dem DSB im Intranet der FH JOANNEUM veröffentlicht.

Weiterführende Informationen zu den an der FH JOANNEUM geltenden Grundsätzen in Bezug auf IT-Sicherheit und den Umgang mit personenbezogenen Daten finden sich in den nachfolgend gelisteten Dokumenten. Die Dokumente können in ihrer jeweils geltenden Fassung über das Intranet der FH JOANNEUM bzw. das Internet bezogen werden.

5.1 Regelungen und Richtlinien der FH JOANNEUM

Datenschutzerklärung der FH JOANNEUM:

http://www.fh-joanneum.at/global/show_document.asp?id=aaaaaaaaaaggnqx

EDV-Ordnung der FH JOANNEUM:

http://www.fh-joanneum.at/global/show_document.asp?id=aaaaaaaaaacxnnv

Änderung des FH Passworts und Passwort-Richtlinien an der FH JOANNEUM:

http://www.fh-joanneum.at/global/show_document.asp?id=aaaaaaaaaabvpqj

Allgemeine IT Infrastrukturinformationen:

https://hlpdsk.fh-joanneum.at/zitdoku/IT-Info-Allgemein.pdf

IT Infrastrukturinformationen für Studierende:

https://hlpdsk.fh-joanneum.at/zitdoku/IT-Info-Studenten.pdf

IT Infrastrukturinformationen für Mitarbeiterinnen und Mitarbeiter:

https://hlpdsk.fh-joanneum.at/zitdoku/IT-Info-Mitarbeiter.pdf

Sonstige Anleitungen, Regelungen und Richtlinien:

http://www.fh-joanneum.at/aw/home/Die_FH/Zentrale_Services/ZIT/Dokumentation/~fad/ZIT-Anleitungen/?lan=de

5.2 Bundesgesetze

Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000):

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

Bundesgesetz betreffend die Arbeitsverfassung:

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008329

Anhang A

Literaturangabe

Weiterführende Informationen zu den Themen Datenschutz und IT-Sicherheit finden sich in folgenden Quellen:

- Wirtschaftskammer Österreich (Bundessparte Information und Consulting), IT-Sicherheitshandbuch für Mitarbeiter (2009).
- Informationssicherheitsbüro des Bundeskanzleramtes (in Zusammenarbeit mit A-SIT und der OCG, Österreichisches Informationssicherheitshandbuch (2007).

Versionsverfolgung

Version	Datum	Autorin bzw. Autor	Änderungen
0.1	29.04.10	Birgit Reinhofer-Mitterer	Ersterstellung
0.2	21.05.10	Harald Burgsteiner	Konzept für 3. DSA-Sitzung
0.3	12.08.10	Birgit Reinhofer-Mitterer	Trennung in externe DS-Erklärung und DS-Handbuch mit User-Empfehlungen
0.4	18.11.11	Harald Burgsteiner	Überarbeitung der Inhalte und User-Empfehlungen
0.5	10.6.12	Harald Burgsteiner	Überarbeitung nach Hinweisen der Abteilungen PER und ZIT
1.0	13.9.12	Harald Burgsteiner	Korrektur und Einarbeitung letzter neuer Inhalte
1.01	19.9.12	Harald Burgsteiner & Peter Gritsch	Korrektur und Finalisierung für die Veröffentlichung der ersten Version