Editorial - Grußwort des Forschungsprojektleiters »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur vierten Ausgabe des BayWiDI-Newsletters. Kurz vor dem Ende der diesjährigen Fastenzeit möchten wir auf aktuelle Entwicklungen im Bereich der IT-Sicherheit aufmerksam machen und Sie herzlich zu dem bevorstehenden 12. Internationalen For..Net-Symposium zum Thema »IT-Fitness – Urheberschutz. Datenschutz. Blockchain.« einladen. Ausführliche Informationen zum Inhalt und Ablauf des Symposiums können Sie diesem Newsletter entnehmen. Neben hochkarätigen Vorträgen von IT-Rechtsexperten aus Wissenschaft und Praxis erwartet Sie ein besonderes Veranstaltungshighlight. Das Thema IT-Fitness wird sowohl aus der Perspektive »Fit für IT« als auch »Fit trotz IT« betrachtet. Zu diesem Zweck konnte ich SHENTI*SPORTS*, einen der größten deutschen Anbieter für Personal Training und Firmenfitness, für die Veranstaltung gewinnen. Mit Blick auf die fortschreitende Digitalisierung der Arbeitswelt gilt es, dem Bewegungsmangel der Beschäftigten mit Mitteln der IT entgegenzuwirken. SHENTI*SPORTS* ist dies durch eine Online-Fitnessplattform gelungen, die das BayWiDI-Team derzeit testen darf. Nähere Informationen hält dieser Newsletter für Sie bereit.

Inhalt

Aus aktuellem Anlass möchte ich an dieser Stelle auf das eIDAS-Durchführungsgesetz vom 29. März 2017 hinweisen. Im Mittelpunkt des Artikelgesetzes steht das Vertrauensdienstegesetz (VDG). Mit dem Gesetz soll die Nutzung elektronischer Vertrauensdienste erleichtert werden. Neben der bereits bekannten »digitalen Unterschrift« werden zukünftig das elektronische Siegel, der elektronische Zeitstempel, elektronische Zustellungsdienste sowie Webseitenzertifikate gesetzlich geregelt.

Wie bereits auf dem 1. BayWiDI-Workshop am 11. Oktober 2016 thematisiert, ist die Stellung des IT-Sicherheitsbeauftragten im Unternehmen nicht zu unterschätzen. Um die Relevanz erneut zu unterstreichen, befindet sich in diesem Newsletter ein Überblick über die wichtigsten Fakten. Auch der Einfluss der IT-Sicherheit auf Fertigungsprozesse wirft in Zeiten von »Industrie 4.0« neue Fragestellungen auf. Hierzu möchte ich umfassend auf den Artikel in diesem Newsletter verweisen. IT-sicherheitsrechtliche Fragestellungen betreffen aber nicht nur die Fertigungsprozesse großer Hersteller, sondern unter Umständen auch Kleinstanbieter internetbasierter Dienstleistungen. Abschließend informiert der Newsletter über die einzuhaltenden Vorgaben in diesem Bereich.

Das BayWiDI-Projekt befindet sich derzeit in der Konzeptionierungsphase zur Einführung eines internen Bereichs (BayWiDI Intern). Ein Überblick über die aktuellen Fortschritte der Arbeit wird voraussichtlich auf dem ersten BayWiDI-Kongress im Rahmen des 12. Internationalen For..Net Symposiums stattfinden.

Mit diesen einleitenden Worten wünsche ich Ihnen eine unterhaltsame Lektüre bei unserem vierten Newsletter sowie ein frohes Osterfest.

Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

12. Internationales For..Net Symposium »IT-Fitness: Urheberschutz. Datenschutz. Blockchain.« am 27. und 28. April 2017

Zum mittlerweile 12. Mal lädt Prof. Dr. Dirk Heckmann, Leiter der Forschungsstelle For..Net, zum internationalen For..Net Symposium in die Universitätsstadt Passau ein. Bei dem For..Net Symposium handelt es sich um eine hochkarätige zweitägige Fachveranstaltung für IT-Rechtsexperten aus Wissenschaft, Wirtschaft und Praxis in den Passauer Redoutensälen, die von einem besonderen kulturellen Abendprogramm umrahmt wird. Die Schirmherrschaft übernimmt erneut Frau Dorothee Bär, Parlamentarische Staatssekretärin im Bundesministerium für Verkehr und Digitale Infrastruktur. Die diesjährige 12. Veranstaltung findet am 27. und 28. April 2017 statt und wird sich dem Thema »IT-Fitness« widmen. Unter diesem Generalthema geht es um verschiedene Einzelaspekte, die sich jeweils der Frage zuwenden, ob Staat, Wirtschaft und Gesellschaft, insbesondere der Bürger, »fit« für die IT-Nutzung sind. »Fit« bedeutet in diesem Kontext in der Lage zu sein, rechtskonform und interessengerecht zu agieren.

Es erwartet Sie unter anderem ein Vortrag des Leiters der Forschungsstelle Prof. Dr. Dirk Heckmann zusammen mit Dr. Frank Rahmstorf zu neuen Wertschöpfungen durch die Digitalisierung. Das interessante Tagungsprogramm besticht zudem durch weitere hochkarätige Referenten wie Prof. Dr. Dr. Walter Blocher, Universität Kassel, Prof. Dr. Jochen Schneider, Rechtsanwalt aus München, Prof. Dr. Louisa Specht, Universität Passau sowie den Datenschutzaktivisten Max Schrems aus Wien.

Der zweite Veranstaltungstag wird mit der Keynote zu »Nudging für eine bessere IT-Sicherheit« von Dr. Ulf Buermeyer eröffnet. Das vollständige Veranstaltungsprogramm entnehmen Sie bitte unserem Flyer, abrufbar unter:

https://www.for-net.info/wp-content/uploads/2017/02/Symposium2017-Flyer.pdf

Wie bereits durch den 3. BayWiDI-Newsletter angekündigt, wird während des Symposiums auch der 1. BayWiDI-Kongress stattfinden. In diesem Rahmen stellen wir den Projektbeirat und ein kontinuierliches Leistungspaket für die Zukunft vor. Darüber hinaus wird das Projekt mit einem eigenen Stand vertreten sein, der den Teilnehmern der Veranstaltung die Möglichkeit gibt, sich über das Projekt zu informieren.

Auch dieses Jahr bieten wir Ihnen ein besonderes Veranstaltungshighlight. Wir werden das Thema »IT-Fitness« nicht nur aus der Perspektive »fit **für** IT« betrachten, sondern auch der Frage nachgehen, wie man »fit **trotz** IT« bleibt. Hierfür dürfen wir SHENTI*SPORTS*, einen der größten deutschen Anbieter für Personal Training und Firmenfitness, in der Drei-Flüsse-Stadt begrüßen. Lassen Sie sich überraschen! Während des traditionellen Galaabends auf der Veste Oberhaus wird bereits zum 4. Mal der For..Net-Award, ein Preis für datenschutzkonforme IT-Innovationen, verliehen.

Wir hoffen mit diesem Kurzüberblick Ihr Interesse geweckt zu haben und freuen uns über Ihre Anmeldung. Die Veranstaltung ist kostenfrei, aber anmeldepflichtig.

Online Anmeldungen werden erbeten über

https://www.for-net.info/symposien/symposium-2017/anmeldung/.

Sie sind herzlich eingeladen uns unter @ForNet_Passau auf Twitter zu folgen. Dort werden Sie mit aktuellen Nachrichten vor und während der Veranstaltung versorgt. Darüber hinaus können Sie unter dem #fornet17 aktiv an Diskussionen teilhaben.

for..net
Forschungsstelle für IT-Recht und Netzpolitik

IT-Fitness?! - Fit **trotz** IT? Fit **durch** IT!

Die digitalisierte Berufswelt stellt Arbeitnehmerinnen und Arbeitnehmer regelmäßig auf die Probe. Die fortschreitende Entwicklung ermöglicht effizientere Produktionsabläufe, schafft neue Tätigkeitsbereiche und sorgt für die zunehmende Vernetzung der beteiligten Komponenten.

Insbesondere bei der Tätigkeit am Bildschirmarbeitsplatz ist damit die Herausforderung verbunden, einerseits mit den technischen Innovationen Schritt zu halten, andererseits aber auch körperlich fit zu bleiben. Der Gesetzgeber hat dieses Problem erkannt und verpflichtet den Arbeitgeber in § 4 der Bildschirmarbeitsverordnung (BildScharbV), geeignete Maßnahmen zur Ergonomie am Arbeitsplatz zu treffen. Weiterhin ist die Tätigkeit der Beschäftigten so zu organisieren, dass die tägliche Arbeit an Bildschirmgeräten regelmäßig durch andere Tätigkeiten oder durch Pausen unterbrochen wird (vgl. § 5 BildScharbV).

Die praktische Umsetzung bleibt jedoch oftmals hinter den Erwartungen des Gesetzgebers zurück. Dabei ist es im Interesse des Arbeitgebers, die mit der sitzenden Tätigkeit einhergehenden Bewegungsmängel zu vermeiden. Die Beschwerden reichen dabei von Kopf- und Rückenschmerzen über Seh- und Konzentrationsstörungen, Ohrengeräusche, Muskelschwund bis hin zu Herz-/Kreislaufstörungen.

Fit trotz IT?

Ursächlich ist meist der Trainings- und Bewegungsmangel der Beschäftigten, der sich insbesondere durch Defizite der Muskulatur im Bereich des Halte- und Bewegungsapparates auswirkt. Die richtige Ausgestaltung des Arbeitsplatzes sowie ein angepasstes Sitzverhalten im Sinne eines dynamischen Wechsels zwischen Stehen und Sitzen während der Arbeitszeit können lediglich teilweise dazu beitragen diese Gesundheitsrisiken zu minimieren. Entscheidend ist die Integration von Bewegung und Entspannung in den Arbeitsalltag.

IT-Fitnessprogramme mit persönlichen Fitnesscoaches, wie sie SHENTI*SPORTS* mit einer Online-Trainingsplattform betreibt, können die Belastung durch die Arbeit an Bildschirmarbeitsplätzen nachhaltig verringern. Das individuelle Trainingsprogramm kann jederzeit mit den bereitstehenden Mitteln am Arbeitsplatz durchgeführt werden. Die Trainingsprogramme sind dabei auf die individuellen Beschwerden und persönlichen Vorlieben des einzelnen Beschäftigten angepasst. Durch die Möglichkeit einer *Challenge* unter Arbeitskollegen kann die Motivation zusätzlich gesteigert werden.

Fit durch IT!

Auf Anregung des Projektleiters Prof. Dr. Dirk Heckmann stellt sich das BayWiDI-Team bis zum 12. Internationalen For..Net-Symposium in zwei konkurrierenden Gruppen den Herausforderungen des SHENTI*SPORTS*-Programms »***FIT***MIT***5***«.

Die jeweils fünfminütigen Videoeinheiten können jederzeit online abgerufen werden und lassen sich aufgrund ihrer kurzen Dauer problemlos in den Arbeitsalltag integrieren. Im Rahmen des For..Net Symposiums 2017 werden die Ergebnisse der Challenge und die individuellen Erfolge der Teilnehmerinnen und Teilnehmer des BayWiDI-Teams eingehend diskutiert werden.

Weitere Informationen zum Fitnessprogramm von SHENTI*SPORTS* können Sie unter https://www.fitmit5.de/ abrufen.

SHENTI*SPORTS* steht für:

- Effektivität
- Alltagstauglichkeit
- Nachhaltigkeit
- Ehrlichkeit

Der IT-Sicherheitsbeauftrage im Unternehmen - Pflicht oder Kür?

Der IT-Sicherheitsbeauftragte ist im Unternehmen für alle Fragen in Bezug auf die Informationssicherheit zuständig. Daher sollte er organisatorisch unabhängig sein und im direkten Kontakt zur Unternehmensleitung stehen. Der IT-Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) empfiehlt, diese Funktion als Stabsstelle in die Organisationsleitung einzugliedern.

Auch nach Einführung des IT-Sicherheitsgesetzes ist die Bestellung eines IT-Sicherheitsbeauftragten grundsätzlich **nicht unmittelbar** gesetzlich verpflichtend vorgeschrieben. Lediglich § 109 Abs. 4 TKG normiert eine Pflicht zur Bestellung für Telekommunikationsunternehmen, wobei sich der Vorschrift keine Angaben zur erforderlichen Qualifikation oder zu den Aufgaben des *Telekommunikationssicherheitsbeauftragten* entnehmen lassen.

Diese Pflicht kann sich allerdings **mittelbar** aus gesetzlichen Vorschriften ergeben. Unternehmen sind gesellschaftsrechtlich mit der Sorgfalt eines ordentlichen Geschäftsmannes zu führen (§§ 43 Abs. 1 GmbHG, 93 Abs. 1 S. 1 AktG). Andernfalls sind der Geschäftsführer und/oder die Vorstandsmitglieder für Schäden haftbar (§§ 43 Abs. 2 GmbHG, 93 Abs. 2 S. 1 AktG). Insbesondere muss die IT-Sicherheit in digitalisierten Arbeitsumgebungen als Teil der Sorgfaltspflicht zur Vermeidung von Haftungsrisiken stets beachtet werden. Die Bestellung eines IT-Sicherheitsbeauftragten trägt somit im Rahmen eines umfassenden IT-Sicherheitskonzepts zur Minimierung von Haftungsrisiken bei.

Das BSI empfiehlt darüber hinaus jedem Unternehmen, welches Informationstechnik verwendet, die Bestellung eines IT-Sicherheitsbeauftragten. Die Bestellung verfolgt dabei keinen Selbstzweck. Vielmehr sind die Aufgaben und Tätigkeitsbereiche des IT-Sicherheitsbeauftragten klar zu benennen.

Nach Empfehlung des BSI fallen insbesondere die folgenden Aufgaben in das Tätigkeitsfeld des IT-Sicherheitsbeauftragten:

- **Koordination der IT-Sicherheit insgesamt**
- **Unterstützung der Geschäftsleitung in allen IT-sicherheitsrelevanten Themen**
- **Erstellung, Betreuung und Aktualisierung der IT-sicherheits- sowie entsprechender Notfallkonzepte**
- **Untersuchung, Aufklärung und Berichterstattung über alle IT-sicherheitsrelevanten Vorfälle**
- **Schulungen und Sensibilisierung der Beschäftigten**

Unternehmen, die sich für die Bestellung eines IT-Sicherheitsbeauftragten entscheiden, sollten bereits bei der Stellenausschreibung und den Anforderungen an das Tätigkeitsprofil folgende Eigenschaften des Kandidaten berücksichtigen:

- **Wissen und Erfahrung in den Gebieten Informationssicherheit und Informationstechnik**
- **Überblick über Aufgaben und Ziele der Institution**
- **Identifikation mit den Zielsetzungen der Informationssicherheit**
- **Kooperations- und Teamfähigkeit**
- **Fähigkeit zum selbstständigen Arbeiten**
- **Durchsetzungsvermögen**
- **Erfahrung im Projektmanagement**

Keinesfalls sollte das Amt des IT-Sicherheitsbeauftragten mit dem Amt des gesetzlich vorgeschriebenen Datenschutzbeauftragten in einer Person zusammenfallen. Mitunter kann es zu Interessenkonflikten zwischen den beiden Ressorts kommen. Beispielsweise kann das Erfassen von Daten aus Sicht der IT-Sicherheit wünschenswert sein, um die Effizienz und Kontrolle zu steigern, während der Datenschutz eine solche Datensammlung in der Regel vermeiden will. Die besondere Stellung des Datenschutzbeauftragten wird zukünftig auch nach den Vorgaben der Datenschutz-Grundverordnung geregelt. Art. 38 Abs. 6 Satz 2 DSGVO legt fest, dass dieser keine Aufgaben und Pflichten wahrnehmen darf, die zu einem Interessenkonflikt führen.

Im Ergebnis erfolgt die Bestellung des IT-Sicherheitsbeauftragten letztlich im eigenen unternehmerischen Interesse. Mit Blick auf die fortschreitende Digitalisierung, die zunehmende Vernetzung der Arbeitsbereiche sowie die damit verbundenen (Haftungs-)Risiken ist die Bestellung eines IT-Sicherheitsbeauftragten in der Praxis keine Frage des »OB«, sondern des »WIE«.

Vertiefende Hinweise finden Sie unter:

https://www.baywidi.de/wiki/organisatorische-grundlagen/

IT & OT: IT-Sicherheit und Operational Technology

Informationstechnik (IT) und Produktionsumgebungen (Operational Technology - OT) waren in der Vergangenheit zwei getrennte Bereiche. Sie existierten nebeneinander und verrichteten ihre jeweiligen Aufgaben. Anknüpfungspunkte oder Überschneidungen gab es fast nicht. Zwar unterstützte die IT den Fertigungsprozess, sie dominierte ihn allerdings zu keinem Zeitpunkt. Mit der zunehmenden Verbreitung der »Industrie 4.0« verschmelzen diese Bereiche. So kommen mehrfach sog. industrielle Steuerungssysteme zum Einsatz. Hierzu zählen beispielsweise die Automatisierungstechnik in der Fertigungsindustrie, die Verfahrens- und Prozessleittechnik in den Bereichen der Chemie und Petrochemie sowie in der Lebensmittelindustrie als auch die Netzleittechnik der Versorgungsnetze bei Strom, Wasser und Gas.

Diese industriellen Steuerungssysteme sind durch die zunehmende Vernetzung und den fortschreitenden Einzug von IT-Systemen in industrielle Umgebungen vermehrt IT-sicherheitsrechtlichen Gefahren ausgesetzt. Dies wird durch die Top 10-Bedrohungen und Gegenmaßnahmen 2016 für Industrial Control System Security des Bundesamts für Sicherheit in der Informationstechnik (BSI) belegt (https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile). Der Studie zufolge zählen Social Engineering und Phishing im Jahr 2016 zu den größten technischen Kompromittierungen im Produktionsumfeld. Schwachstellen für die IT-Sicherheit können aufgrund der Komplexität der Produktionsumgebungen in vielen Bereichen auftreten. Einfallstor sind dabei sowohl die verwendete Systemarchitektur als auch einzelne Komponenten.

Die Bedrohungslage hat der Gesetzgeber bereits erkannt und versucht mit dem 2015 in Kraft getretenen IT-Sicherheitsgesetz (vgl. https://www.baywidi.de/wiki/gesetzliche-grundlagen/) und der 2016 in Kraft getretenen NIS-Richtlinie (vgl. https://www.baywidi.de/wiki/gesetzliche-grundlagen/gesetzliche-grundlagen-fuer-betreiber-kritischer-infrastrukturen/nis-richtlinie/) eine Antwort zu geben. Die neuen Vorschriften richten sich jedoch vorrangig an Betreiber kritischer Infrastrukturen. Industriekomponentenhersteller sind hiervon in den meisten Fällen nicht erfasst. Sie haften für Schwachstellen in der IT-Sicherheit nur nach den allgemeinen Grundsätzen. Hierzu gehören unter anderem die vertragliche Haftung nach dem kaufrechtlichen Gewährleistungsrecht, die deliktische verschuldensunabhängige Produzentenhaftung, die Haftung für die Produktsicherheit sowie die verschuldensabhängige Produkthaftung aus dem Produkthaftungsgesetz (ProdHaftG).

Im Rahmen der vertraglichen Gewährleistungsrechte wird dem Hersteller empfohlen, die IT-sicherheitsrelevanten Eigenschaften seiner Komponenten möglichst genau zu beschreiben. Hierzu gehört auch eine klare Beschreibung dessen, was nicht vom Leistungsumfang umfasst ist. Bei der Produzentenhaftung müssen Verkehrssicherungspflichten beachtet werden. Welcher Sicherheitsstandard im Einzelfall erforderlich ist, hängt von den Sicherheitserwartungen des betroffenen Benutzerkreises ab. Zudem muss das Sicherheitsniveau eingehalten werden, das nach dem »Stand von Wissenschaft und Technik« möglich und zumutbar ist. Dies ergibt sich unter anderem aus technischen Standards wie der Normenreihe IEC 62443. Letztlich muss immer haftungsbegrenzend berücksichtigt werden, dass eine Software niemals fehlerfrei programmiert werden kann, die Bedrohungslagen ständig variieren und ein hinreichendes Maß an IT-Sicherheit nur durch Zusammenwirken aller Akteure erreicht werden kann. IT-Sicherheit ist niemals absolut, sondern immer nur relativ. Ein Anspruch auf Aufrechterhaltung der IT-Sicherheit im Rahmen von Software-Updates besteht nur während der Gewährleistungsrechte und folgt nicht aus der Produzentenhaftung. Den Hersteller treffen nach Verjährung der Gewährleistungsrechte Produktbeobachtungs- und Warnpflichten.

Vertiefungshinweise:

- *Rockstroh/Kunkel*, **IT-Sicherheit in Produktionsumgebungen, Verantwortlichkeit von Herstellern für Schwachstellen in ihren Industriekomponenten, MMR 2017, 77.**
- *Rockstroh*, **Die Verantwortlichkeit der Hersteller für Schwachstellen in Industriekomponenten, DSRITB 2016, 279.**

IT-Sicherheit bei internetbasierten Dienstleistungen wie Online-Shops

Trotz des IT-Sicherheitsgesetzes und der NIS-Richtlinie ist die IT-Sicherheit nicht nur für kritische Infrastrukturen von Relevanz. Durch den neu eingeführten § 13 Abs. 7 TMG werden auch Telemedien-Diensteanbieter mit erhöhten Anforderungen an die IT-Sicherheit konfrontiert.

Der Anwendungsbereich der Norm erfasst solche Diensteanbieter, die *geschäftsmäßig* Telemedien anbieten. Nach dem Willen des Gesetzgebers liegt diese vor, sobald die Tätigkeit *nachhaltig*, *planmäßig* und *dauerhaft* erbracht wird. Auf die Entgeltlichkeit des Dienstes kommt es demnach nicht an. Betroffen sind mithin Online-Shops, internetbasierte Dienstleistungen und unter Umständen auch schlichte Webseiten ohne weitergehende Funktionen. Die dem Telemedium zugrunde liegenden technischen Einrichtungen wie beispielsweise Serveranlagen müssen durch technische und organisatorische Vorkehrungen gesichert werden. Dabei ist der Stand der Technik zu berücksichtigen. Diese Sicherungspflicht umfasst unter anderem die Vermeidung interner und externer Angriffe sowie den allgemeinen Schutz personenbezogener Daten.

Bei der Umsetzung dieser Vorgaben sind insbesondere die folgenden Maßnahmen zu beachten:

- **Verwendung entsprechender Sicherheitssoftware**
- **Verwendete Software ist stets aktuell zu halten**
- **Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten**
- **Verschlüsselung der Daten**
- **Authentifizierung der Nutzer**
- **Entsprechende Notfallszenarien**

Um eine übermäßige Belastung der Diensteanbieter zu vermeiden, müssen Sicherungsmaßnahmen allerdings nur ergriffen werden, soweit sie *wirtschaftlich zumutbar* sind. Entscheidend ist hierbei die individuelle Leistungsfähigkeit des Anbieters. Dieser soll zu keinen Maßnahmen verpflichtet werden, die ihn in eine ernsthafte wirtschaftliche Bedrängnis bringen. Auf das Merkmal der Kostenpflicht des Dienstes kommt es nicht an.

Sofern die Sicherung der technischen Einrichtungen beziehungsweise der Schutz der personenbezogenen Daten nicht hinreichend gewährleistet wird, droht gem. § 16 Abs. 2 Nr. 3 TMG ein Bußgeld in Höhe von maximal 50.000 €. Das TMG benennt keine zuständige Behörde, so dass diese letztlich durch das Landesrecht bestimmt wird. In Bayern ist beispielsweise das Landesamt für Datenschutzaufsicht zuständig.

Eine ausführliche Darstellung der Problematik sowie weitergehende Handlungsempfehlungen können in unserem WiKI nachgelesen werden.

https://www.baywidi.de/wiki/gesetzliche-grundlagen/

Der nächste Newsletter erscheint am 15. Juli 2017.

Sie finden den Newsletter und die Möglichkeit, sich an-, bzw. abzumelden auch unter https://www.baywidi.de/

Hinweise, Anregungen, Lob und Kritik sind herzlich Willkommen. Schreiben Sie einfach an baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation
Gemäß Art. 4 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung:
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.