Technische Hochschule Wildau
Technical University of Applied Sciences

TH Wildau Hochschulring 1 15745 Wildau

Herrn
Marcel Langner
[redacted]

[redacted]

Wildau, 29. Juli 2021
Ihr Zeichen #225443 | *Unser Zeichen* #225443

Antrag nach dem Akteneinsichts- und Informationszugangsgesetz (AIG), BbgUIG, VIG
Antrag vom 23. Juli 2021

Sehr geehrter Herr Langner,

Ihr oben genannter Antrag auf Akteneinsicht nach dem Brandenburgischen Akteneinsichts- und Informationszugangsgesetz (AIG) ist am 23. Juli 2021 eingegangen.

Mit oben genannter Anfrage bitten Sie um Übersendung folgender Informationen:

Aus meiner Anfrage hier https://fragdenstaat.de/a/209324 kommt heraus, dass Schriftverkehr mit dem vor Ort ansässigen Datenschutzbeauftragten stattfand. Ich erbitte diesen Schriftverkehr. Diese Anfrage geht auch direkt dem Datenschutzbeauftragten zu.
Leider konnten Sie die Verpflichtungserklärungen aus dem Wiki aus dieser Anfrage https://fragdenstaat.de/a/221305 nicht mehr auffinden. Sollte diese im Rahmen Ihrer jetzigen Recherchen doch noch auftauchen, so erbitte ich diese und benötige dann den Schriftverkehr mit dem Datenschutzbeauftragten nicht mehr.

Da dieser Schriftverkehr mit dem Datenschutzbeauftragten der TH Wildau von mehreren Organisationseinheiten hätte stattfinden können, wurde Ihre Anfrage an die möglichen Adressaten und Absender weitergeleitet. Dazu liegen zwei Rückmeldungen vor:
1. Der Datenschutzbeauftrage hat die ihm vorliegenden Dokumente an mich gesendet. Es handelt sich hierbei um eine vierseitige Verpflichtungserklärung und um eine dreiseitige Anlage dazu.

Technische Hochschule Wildau
Technical University of Applied Sciences

2. Eine Person der Verwaltung hat die vorliegenden Dokumente entsprechend des Zeitraumes, also Ende 11'2018 bis 12'2018 durchgearbeitet. An einer Position ist eine vierseitige Verpflichtungserklärung gefunden worden.

In der Anlage übersende ich Ihnen die mir nun vorliegenden Dokumente.

Gemäß § 6 Abs. 1 a.E. AIG weise ich Sie darauf hin, dass jede Person gemäß § 11 Abs. 2 Satz 1 AIG das Recht hat, die Landesbeauftragte für Datenschutz und das Recht auf Akteneinsicht anzurufen.

Mit freundlichen Grüßen

[redacted]

Technische Hochschule Wildau
Technical University of Applied Sciences

Alex Personal

1. Verpflichtungserklärung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung (DS-GVO) im Sinne des § 53 BDSG Datengeheimnis

Frau/Herr_____

verpflichtet sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen:

a. auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");
b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung");
c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");
d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit");
e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung");
f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Personenbezogene Daten dürfen daher **nur nach Weisung** des Verantwortlichen verarbeitet werden, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor. Neben Einzelweisungen der Vorgesetzten gelten als Weisung: Prozessbeschreibungen, Ablaufpläne, Betriebsvereinbarungen, allgemeine Dienstanweisungen sowie betriebliche Dokumentationen und Handbücher. Bestehende Vorschriften über den Umgang bzw. die Sicherung personenbezogener Daten (z.B. im Hinblick auf den Passwortschutz) sowie die Regelungen zur Unterstützung der Informationssicherheit sind zu beachten. Zum Schutze personenbezogener Daten ist die **notwendige Sorgfalt** anzuwenden und sind festgestellte **Mängel dem Datenschutzbeauftragten zu melden**.

Technische Hochschule Wildau
Technical University of Applied Sciences

Derzeitiger Datenschutzbeauftragter:

Prof. Dr. Martin Richartz,
Tel.: +49 3375 508 551,
Mail: martin.richartz(at)th-wildau.de

Die Verpflichtung umfasst insbesondere folgende Anweisungen:

- Alle Daten und Programme dürfen nur in der Art und Weise verwahrt, verarbeitet oder ausgegeben werden, wie es von entscheidungsberechtigten Stellen angeordnet wird.
- Daten, Programme und andere Informationen dürfen nicht zu einem anderen als dem Zweck der Erfüllung der Dienstaufgaben vervielfältigt werden.
- Es ist untersagt, Daten oder Programme zu verfälschen, unechte Daten oder Programme herzustellen sowie unechte oder verfälschte Daten und Programme vorsätzlich zu gebrauchen.
- Es dürfen nur die für die konkrete Aufgabenerfüllung notwendigen Daten abgerufen werden. Eine Weitergabe personenbezogener Daten an Dritte (Externe) ist nur zulässig, wenn dem Empfänger ein Recht auf Kenntnisnahme auf Grund einer Rechtsvorschrift zusteht bzw. die Zustimmung des Vorgesetzten erteilt wird.
- Unterlagen mit personenbezogenen Daten sind sicher vor dem Zugriff Dritter aufzubewahren.
- Zur Löschung oder zur Vernichtung vorgesehene Ausdrucke sind ordnungsgemäß zu vernichten (Datentonne oder Schredder).

Verstöße gegen diese Verpflichtung können mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen. Die sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebenden Vertraulichkeitsverpflichtungen werden durch diese Erklärung nicht berührt. Die Verpflichtung gilt auch nach Beendigung der Tätigkeit an der Technischen Hochschule Wildau fort.

Hiermit bestätige ich, dass ich über meine Verpflichtungen bezüglich der o.g. Anweisungen zur Wahrung des Datengeheimnisses unterrichtet worden bin und diese einhalten werde.

Ein Exemplar der Verpflichtung und der Regelungen zur Unterstützung der Informationssicherheit sowie die Anlage zur Verpflichtungserklärung habe ich erhalten.

Ort, Datum	Unterschrift der/des Verpflichteten	Unterschrift der/des Verantwortlichen

2. Regelungen zur Unterstützung der Informationssicherheit

Auf allen Endgeräten der TH Wildau und besonders auf allen Servern, Computern und Laptops dürfen nur Softwareprodukte installiert und genutzt werden, die von dem zuständigen Administrator genehmigt und die rechtmäßig lizenziert wurden.

- Die Installation von Software darf ausschließlich durch den zuständigen Administrator erfolgen. Insbesondere gelten folgende Regelungen:
  - Mitarbeiter dürfen ohne Befugnis keine fremde Software aus dem Internet herunterladen oder auf anderem Weg auf Computern der Hochschule installieren. Dazu gehören auch Bildschirmschoner, Demoprogramme, Computerspiele oder Utilities.
  - Ohne besondere Genehmigung dürfen keine fremden Programme direkt aus dem Internet oder aus E-Mail-Anhängen gestartet werden.
- Unbefugte Personen dürfen weder von zugekaufter noch von der Hochschule selbst erstellter Software Kopien erstellen. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.
- Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder als Notiz in den Büros der Mitarbeiter noch als Datei auf Computern oder Datenträgern. Wichtige administrative Passwörter müssen hinterlegt werden. Hierbei ist auf einen geeigneten Schutz zu achten (z.B. Passwortdatenbank KeePass). Passwörter dürfen unter keinen Umständen an Dritte weitergegeben werden.
- Der Mitarbeiter sichert zu, dass er alle ihm im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten der Hochschule, seiner Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich behandelt und geheim hält. Er versichert, dass er derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben wird, außer in Erfüllung seiner vertraglichen Pflichten. Zieht der Mitarbeiter im Auftrage der Hochschule Dritte zur Mitarbeit hinzu, ist er verpflichtet, diesen die gleiche Verschwiegenheitspflicht aufzuerlegen.
- Mitarbeiter dürfen nicht versuchen, auf Bereiche des LANs oder WANs vorzudringen, die nicht für den Mitarbeiter und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte und das Informationssicherheitsteam der TH Wildau ohne Verzug zu informieren. Der Einsatz von Netzwerkanalyse-Tools ist generell untersagt.
- Bei Verdacht auf Schadsoftware, Datenspionage oder anderer Umstände die einen Sicherheitsvorfall darstellen könnten und die die Sicherheit der Informationen der Hochschule betreffen, ist unverzüglich der Vorgesetzte und das Informationssicherheitsteam der TH Wildau zu informieren.
- Störungen und Defekte bei informationstechnischen Einrichtungen und auftretende Fehler in der Software sind unverzüglich den dafür verantwortlichen Personen zu berichten.
- Jeder Mitarbeiter ist angehalten, die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchmaterialien, wie Druckerpapier, Druckfolien, Druckerpatronen usw.
- Hochschulinformationen müssen generell so gespeichert werden, dass bei Ausfall eines Mitarbeiters dessen Vertretung oder der Vorgesetzte auf diese Informationen zugreifen kann. Für die Speicherung von Hochschulinformationen ist das persönliche Verzeichnis, auf das nur der einzelne Mitarbeiter über sein Passwort zugreifen kann, nicht geeignet. Hochschulinformationen wie Word oder Excel Dateien sollten vielmehr in Gruppenverzeichnissen abgelegt werden. Damit bei Ausfall eines Mitarbeiters diese Informationen von anderen Mitarbeitern gefunden werden, muss die Ordnerstruktur im

Gruppenverzeichnis auf dem/den Servern ständig mit den zuständigen Kollegen abgesprochen werden. Namen für Ordner oder Dokumente sollen eindeutig gewählt werden, damit Dokumente auch von Kollegen schnell geortet werden können.

- Jeder Mitarbeiter ist angehalten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen und damit dazu beizutragen, dass die Datenbestände und deren Strukturen überschaubar bleiben und die Kosten der Datenhaltung und Datensicherung in vertretbaren Grenzen bleiben.
- Verlässt ein Mitarbeiter befristet (Mutterschaftsurlaub, Kur) oder unbefristet (Kündigung, Rente) die Hochschule, so ist er angehalten, nicht mehr benötigte Datenbestände und E-Mails zu löschen und die verbleibenden Datenbestände an einen Kollegen/eine Kollegin zu übergeben. Vorgesetzte sind angehalten, die ordnungsgemäße Übergabe von Datenbeständen sicherzustellen.
- Der Zugriff auf pornografische oder politisch radikale Internetinhalte ist generell verboten. Prinzipiell darf nur auf Internetinhalte zugegriffen werden, die zur Erledigung der Aufgaben nützlich sind.

Hiermit bestätige ich, dass ich über die Regelungen zur Unterstützung der Informationssicherheit unterrichtet worden bin.

_____

Ort, Datum

_____

Unterschrift des/der Verpflichteten

Original: - Personalakte
Abschrift/Kopie: - Betrieblicher Datenschutzbeauftragte/r
- Mitarbeiter/in

Technische Hochschule Wildau
Technical University of Applied Sciences

DSB

1. Verpflichtungserklärung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung (DS-GVO) im Sinne des § 53 BDSG Datengeheimnis

Frau/Herr_____

verpflichtet sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen:

a. auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");
b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung");
c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");
d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit");
e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung");
f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Personenbezogene Daten dürfen daher **nur nach Weisung** des Verantwortlichen verarbeitet werden, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor. Neben Einzelweisungen der Vorgesetzten gelten als Weisung: Prozessbeschreibungen, Ablaufpläne, Betriebsvereinbarungen, allgemeine Dienstanweisungen sowie betriebliche Dokumentationen und Handbücher. Bestehende Vorschriften über den Umgang bzw. die Sicherung personenbezogener Daten (z.B. im Hinblick auf den Passwortschutz) sowie die Regelungen zur Unterstützung der Informationssicherheit sind zu beachten. Zum Schutze personenbezogener Daten ist die **notwendige Sorgfalt** anzuwenden und sind festgestellte **Mängel dem Datenschutzbeauftragten zu melden**.

Technische Hochschule Wildau
Technical University of Applied Sciences

Derzeitiger Datenschutzbeauftragter:

Prof. Dr. Martin Richartz,
Tel.: +49 3375 508 551,
Mail: martin.richartz(at)th-wildau.de

Die Verpflichtung umfasst insbesondere folgende Anweisungen:

- Alle Daten und Programme dürfen nur in der Art und Weise verwahrt, verarbeitet oder ausgegeben werden, wie es von entscheidungsberechtigten Stellen angeordnet wird.
- Daten, Programme und andere Informationen dürfen nicht zu einem anderen als dem Zweck der Erfüllung der Dienstaufgaben vervielfältigt werden.
- Es ist untersagt, Daten oder Programme zu verfälschen, unechte Daten oder Programme herzustellen sowie unechte oder verfälschte Daten und Programme vorsätzlich zu gebrauchen.
- Es dürfen nur die für die konkrete Aufgabenerfüllung notwendigen Daten abgerufen werden. Eine Weitergabe personenbezogener Daten an Dritte (Externe) ist nur zulässig, wenn dem Empfänger ein Recht auf Kenntnisnahme auf Grund einer Rechtsvorschrift zusteht bzw. die Zustimmung des Vorgesetzten erteilt wird.
- Unterlagen mit personenbezogenen Daten sind sicher vor dem Zugriff Dritter aufzubewahren.
- Zur Löschung oder zur Vernichtung vorgesehene Ausdrucke sind ordnungsgemäß zu vernichten (Datentonne oder Schredder).

Verstöße gegen diese Verpflichtung können mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen. Die sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebenden Vertraulichkeitsverpflichtungen werden durch diese Erklärung nicht berührt. Die Verpflichtung gilt auch nach Beendigung der Tätigkeit an der Technischen Hochschule Wildau fort.

Hiermit bestätige ich, dass ich über meine Verpflichtungen bezüglich der o.g. Anweisungen zur Wahrung des Datengeheimnisses unterrichtet worden bin und diese einhalten werde.

Ein Exemplar der Verpflichtung und der Regelungen zur Unterstützung der Informationssicherheit sowie die Anlage zur Verpflichtungserklärung habe ich erhalten.

Ort, Datum	Unterschrift der/des Verpflichteten	Unterschrift der/des Verantwortlichen

2. Regelungen zur Unterstützung der Informationssicherheit

Auf allen Endgeräten der TH Wildau und besonders auf allen Servern, Computern und Laptops dürfen nur Softwareprodukte installiert und genutzt werden, die von dem zuständigen Administrator genehmigt und die rechtmäßig lizenziert wurden.

- Die Installation von Software darf ausschließlich durch den zuständigen Administrator erfolgen. Insbesondere gelten folgende Regelungen:
  - Mitarbeiter dürfen ohne Befugnis keine fremde Software aus dem Internet herunterladen oder auf anderem Weg auf Computern der Hochschule installieren. Dazu gehören auch Bildschirmschoner, Demoprogramme, Computerspiele oder Utilities.
  - Ohne besondere Genehmigung dürfen keine fremden Programme direkt aus dem Internet oder aus E-Mail-Anhängen gestartet werden.
- Unbefugte Personen dürfen weder von zugekaufter noch von der Hochschule selbst erstellter Software Kopien erstellen. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.
- Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder als Notiz in den Büros der Mitarbeiter noch als Datei auf Computern oder Datenträgern. Wichtige administrative Passwörter müssen hinterlegt werden. Hierbei ist auf einen geeigneten Schutz zu achten (z.B. Passwortdatenbank KeePass). Passwörter dürfen unter keinen Umständen an Dritte weitergegeben werden.
- Der Mitarbeiter sichert zu, dass er alle ihm im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten der Hochschule, seiner Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich behandelt und geheim hält. Er versichert, dass er derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben wird, außer in Erfüllung seiner vertraglichen Pflichten. Zieht der Mitarbeiter im Auftrage der Hochschule Dritte zur Mitarbeit hinzu, ist er verpflichtet, diesen die gleiche Verschwiegenheitspflicht aufzuerlegen.
- Mitarbeiter dürfen nicht versuchen, auf Bereiche des LANs oder WANs vorzudringen, die nicht für den Mitarbeiter und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte und das Informationssicherheitsteam der TH Wildau ohne Verzug zu informieren. Der Einsatz von Netzwerkanalyse-Tools ist generell untersagt.
- Bei Verdacht auf Schadsoftware, Datenspionage oder anderer Umstände die einen Sicherheitsvorfall darstellen könnten und die die Sicherheit der Informationen der Hochschule betreffen, ist unverzüglich der Vorgesetzte und das Informationssicherheitsteam der TH Wildau zu informieren.
- Störungen und Defekte bei informationstechnischen Einrichtungen und auftretende Fehler in der Software sind unverzüglich den dafür verantwortlichen Personen zu berichten.
- Jeder Mitarbeiter ist angehalten, die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchmaterialien, wie Druckerpapier, Druckfolien, Druckerpatronen usw.
- Hochschulinformationen müssen generell so gespeichert werden, dass bei Ausfall eines Mitarbeiters dessen Vertretung oder der Vorgesetzte auf diese Informationen zugreifen kann. Für die Speicherung von Hochschulinformationen ist das persönliche Verzeichnis, auf das nur der einzelne Mitarbeiter über sein Passwort zugreifen kann, nicht geeignet. Hochschulinformationen wie Word oder Excel Dateien sollten vielmehr in Gruppenverzeichnissen abgelegt werden. Damit bei Ausfall eines Mitarbeiters diese Informationen von anderen Mitarbeitern gefunden werden, muss die Ordnerstruktur im

Gruppenverzeichnis auf dem/den Servern ständig mit den zuständigen Kollegen abgesprochen werden. Namen für Ordner oder Dokumente sollen eindeutig gewählt werden, damit Dokumente auch von Kollegen schnell geortet werden können.

- Jeder Mitarbeiter ist angehalten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen und damit dazu beizutragen, dass die Datenbestände und deren Strukturen überschaubar bleiben und die Kosten der Datenhaltung und Datensicherung in vertretbaren Grenzen bleiben.
- Verlässt ein Mitarbeiter befristet (Mutterschaftsurlaub, Kur) oder unbefristet (Kündigung, Rente) die Hochschule, so ist er angehalten, nicht mehr benötigte Datenbestände und E-Mails zu löschen und die verbleibenden Datenbestände an einen Kollegen/eine Kollegin zu übergeben. Vorgesetzte sind angehalten, die ordnungsgemäße Übergabe von Datenbeständen sicherzustellen.
- Der Zugriff auf pornografische oder politisch radikale Internetinhalte ist generell verboten. Prinzipiell darf nur auf Internetinhalte zugegriffen werden, die zur Erledigung der Aufgaben nützlich sind.

Hiermit bestätige ich, dass ich über die Regelungen zur Unterstützung der Informationssicherheit unterrichtet worden bin.

_____

Ort, Datum

_____

Unterschrift des/der Verpflichteten

Original: - Personalakte
Abschrift/Kopie: - Betrieblicher Datenschutzbeauftragte/r
- Mitarbeiter/in

Technische Hochschule Wildau
Technical University of Applied Sciences

DSB

Anlage zur Verpflichtungserklärung

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „**Personenbezogene Daten**" [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**" [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz").

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger** Verarbeitung und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer **Verletzung** des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG
(1) Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1) einem Dritten übermittelt oder
2) auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1) ohne hierzu berechtigt zu sein, verarbeitet oder
2) durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a StGB Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden

§ 202b StGB Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder

sonst zugänglich macht, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 303a StGB Datenveränderung:

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303b StGB Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe **Freiheitsstrafe** bis zu fünf Jahren oder **Geldstrafe**.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe **Freiheitsstrafe** von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.