UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

AMTLICHE MITTEILUNGEN

VERKÜNDUNGSBLATT DER UNIVERSITÄT PADERBORN AM.UNI.PB

AUSGABE 21.24 VOM 24. APRIL 2024

RICHTLINIE ZUR EINORDNUNG DES SCHUTZBEDARFS VON INFORMATIONEN UNTER BERÜCKSICHTIGUNG DES SCHUTZES PERSONENBEZOGENER DATEN DER UNIVERSITÄT PADERBORN (MIT ENGLISCHER ÜBERSETZUNG)

VOM 24. APRIL 2024

HERAUSGEBER: PRÄSIDIUM DER UNIVERSITÄT PADERBORN

Richtlinie zur Einordnung des Schutzbedarfs von Informationen unter Berücksichtigung des Schutzes personenbezogener Daten der Universität Paderborn
vom 24. April 2024

Dokumenteneigenschaften

Verantwortung	CIO / Informationssicherheitsbeauftragter
Klassifizierung	S1 Öffentlich
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	März 2025
Ablageort / Dateiname	Sharepoint Informationssicherheit RL016

Dokumentenstatus und Freigabe

Status	Version	Datum	Name / Abteilung / Firma
Erstellung	0.1	2022-06-21	Kampmeyer / IST
Freigabe	1.0	2023-09-06	Präsidium

Dokumentenhistorie

Ver-sion	Änderung	Datum	Autor*in der Änderung
0.1	Zusammenfassung der Einzeldokumente • RL001 2020 Definition Schutzbedarfskatego-rien • RL002 2020 Klassen von Informationen und ihr üblicher Schutzbedarf • RL003 2020 Richtlinie zur Einordnung des Schutzbedarfs von Informationen • Versionsverfolgung hinzugefügt	2022-06-21	Kampmeyer / IST
0.2	Link und Rechtschreibung korrigiert	2022-07-04	Kampmeyer / IST
1.1	Redaktionelle Änderungen	2024-02-20	Porombka / IST
1.2	Formatierung der Kopf- und Fußzeilen Dokumenten-Klassifizierung ist jetzt S1 Öffentlich	2024-04-24	Kampmeyer / IST

Inhaltsverzeichnis / Table of contents

1) EINLEITUNG ... 4

2) GELTUNGSBEREICH ... 4

3) ZIELSETZUNG ... 4

4) BEGRIFFSDEFINITIONEN ... 5

5) FESTLEGUNG SCHUTZBEDARFSKATEGORIEN AN DER UNIVERSITÄT PADERBORN ... 8

6) ORIENTIERUNGSHILFE ZUR EINORDNUNG DES SCHUTZBEDARFS VON INFORMATIONEN ... 10

ANHANG 1: VORGEHEN ZUR ERMITTLUNG EINES SCHUTZBEDARFES ... 12

SCHADENSSZENARIO "VERSTOß GEGEN GESETZE/VORSCHRIFTEN/VERTRÄGE" ... 12
SCHADENSSZENARIO „BEEINTRÄCHTIGUNG DES INFORMATIONELLEN SELBSTBESTIMMUNGSRECHTS“ ... 12
SCHADENSSZENARIO „BEEINTRÄCHTIGUNG DER AUFGABENERFÜLLUNG“ ... 14
SCHADENSSZENARIO "NEGATIVE INNEN- ODER AUßENWIRKUNG" ... 14
SCHADENSSZENARIO "FINANZIELLE AUSWIRKUNGEN" ... 15

ANHANG 2: KLASSEN VON INFORMATIONEN UND IHR ÜBLICHER SCHUTZBEDARF ... 17

EINLEITUNG ... 17
VERWALTUNGSDATEN ... 18
STUDIERENDENDATEN ... 19
WISSENSCHAFTLICHE DATEN ... 20
GESUNDHEITSDATEN ... 20
ARBEITSSCHUTZ ... 21

1) INTRODUCTION ... 23

2) SCOPE OF APPLICATION ... 23

3) OBJECTIVE ... 23

4) DEFINITIONS OF TERMS ... 24

5) DEFINITION OF PROTECTION REQUIREMENT CATEGORIES AT PADERBORN UNIVERSITY ... 27

6) GUIDANCE ON CLASSIFYING THE NEED FOR PROTECTION OF INFORMATION ... 29

APPENDIX 1: PROCEDURE FOR DETERMINING A PROTECTION REQUIREMENT ... 30

DAMAGE SCENARIO "VIOLATION OF LAWS/REGULATIONS/CONTRACTS" ... 30
DAMAGE SCENARIO "IMPAIRMENT OF THE RIGHT TO INFORMATIONAL SELF-DETERMINATION" ... 31
DAMAGE SCENARIO "IMPAIRMENT OF TASK FULFILLMENT" ... 32
DAMAGE SCENARIO "NEGATIVE INTERNAL OR EXTERNAL IMPACT" ... 33
DAMAGE SCENARIO "FINANCIAL IMPACT" ... 33

APPENDIX 2: CLASSES OF INFORMATION AND THEIR USUAL PROTECTION REQUIREMENTS ... 35

INTRODUCTION ... 35
ADMINISTRATIVE DATA ... 36
PERSONNEL DATA ... 37
STUDENT DATA ... 38
SCIENTIFIC DATA ... 38
HEALTH DATA ... 39
OCCUPATIONAL SAFETY ... 39

1) Einleitung

Im Arbeitsalltag kommen Angehörige der Universität Paderborn (UPB) regelmäßig mit verschiedensten Informationen in Kontakt. Die Veröffentlichung, Veränderung oder der Verlust einiger dieser Informationen können schwerwiegende Konsequenzen für die UPB aber auch für die Personen, deren Daten verarbeitet werden, haben.

Gegenstand von Informationen sind regelmäßig auch personenbezogene Daten. 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. 1 der EU-Datenschutzgrundverordnung (DS-GVO)). Insofern besteht ein Grundrecht auf informationelle Selbstbestimmung, welches sich aus dem Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetztes (GG)) herleitet. Darüber hinaus ist der Schutz personenbezogener Daten ausdrücklich in Art. 8 der EU-Grundrechtecharta (GRCh) verankert, auf die sich sämtliche Unionsbürger*innen berufen können. Umgesetzt werden diese grundrechtlichen Garantien durch europäische wie nationale gesetzliche Vorgaben. Danach sind, insb. auf Basis der in Art. 5 DS-GVO geregelten Grundprinzipien (Rechtmäßigkeit, Zweckbindung, …), Risiken für natürliche Personen hinsichtlich eine sie betreffenden Datenverarbeitung zu verhindern, wobei es mittelbar auch um Konsequenzen für die UPB gehen kann.

Diese Richtlinie behandelt die Feststellung des Schutzbedarfs von Informationen und den Schutzbedarf Betroffener der sie betreffenden Daten. Ist der Schutzbedarf festgestellt, so können aufbauend darauf Regeln zum Umgang mit der Information und/oder personenbezogenen Daten festgelegt und umgesetzt werden.

2) Geltungsbereich

Diese Richtlinie hat verbindliche Gültigkeit für alle Mitarbeiter*innen der UPB. Sie legt fest, wie Mitarbeiter*innen der UPB den Schutzbedarf von Informationen einschließlich personenbezogener Daten einordnen müssen.

3) Zielsetzung

Ziel dieses Dokuments ist es, verbindliche Regeln für die Feststellung des Schutzbedarfs von Informationen und personenbezogenen Daten an der UPB festzulegen. Der Schutzbedarf gibt dabei an wie schwerwiegend die Konsequenzen einer Verletzung der weiter unten definierten Sicherheits- und Gewährleistungsziele für die UPB und ggf. für die Betroffene sind. Andere Richtlinien oder Empfehlungen können dann diese Festlegung des Schutzbedarfs verwenden, um Regeln für den Umgang mit den Informationen und personenbezogenen Daten zu definieren.

Schutzbedarfsfeststellungen müssen jedoch nicht von den Beschäftigten für jede Information im Einzelfall durchgeführt werden, sondern finden in der Regel für einzelne Verarbeitungen (Studierendenverwaltung, Bewerbungsverfahren, Prüfungsverwaltung, …) zentral im Rahmen der Erstellung des für jede Verarbeitungstätigkeit personenbezogener Daten erforderlichen Verzeichnisses von Verarbeitungstätigkeiten statt. Die Schutzbedarfsfeststellung wird von den Datenschutzkoordinator*innen, der Datenschutzbeauftragten und den Sicherheitsbeauftragten unterstützt.

Von der UPB werden damit für bestimmte Datenkategorien (Anmeldungen zu Lehrveranstaltungen, Personalakten, Beihilfedaten, …) grundsätzliche Schutzbedarfsfeststellungen durchgeführt und den Beschäftigten zur Verfügung gestellt, sodass eine Schutzbedarfsfeststellung in der Regel nur bei neuen noch nicht dokumentierten Verarbeitungstätigkeiten durchzuführen ist.

4) Begriffsdefinitionen

In folgender Tabelle werden für das Verständnis des Dokuments wichtige Begriffe definiert und an Beispielen erläutert.

Sicherheitsziele und Gewährleistungsziele	*Definition:* Ein Sicherheitsziel ist eine Eigenschaft von Informationen, dessen Verletzung negative Konsequenzen haben kann. Der Schutz personenbezogener Daten wird durch rechtlich verankerte Anforderungen abgebildet. Maßgeblich sind dafür insbesondere die DS-GVO sowie landesspezifische nationale Regelungen, wie das DSG NRW zzgl. konkretisierender Regelungen. Die sich daraus ergebenden rechtlichen Anforderungen lassen sich durch sog. Gewährleistungsziele bündeln und strukturieren, mit dem Ziel, die mit einer Datenverarbeitung zusammenhängenden Risiken für die Rechte und Freiheiten natürlicher Personen durch technische und organisatorische Maßnahmen zu mindern. Konkret betrachtet werden in der weiteren Tabelle die drei Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit, sowie zusätzlich die für personenbezogene Daten zusätzlich relevanten Gewährleistungsziele Datenminimierung, Nichtverkettung, Transparenz sowie Intervenierbarkeit.
Vertraulichkeit	*Definition: Vertraulichkeit* bezeichnet die Anforderung, dass Informationen und personenbezogene Daten, nur einem eingeschränkten Kreis von befugten Personen zugänglich sein dürfen. Unbefugt sind i. d. R. alle Personen, die keinerlei inhaltlichen Bezug zu einer Datenverarbeitung oder zu der jeweiligen betroffenen Person haben.
	Beispiele: Ein typisches Beispiel mit einem hohen Bedarf an Vertraulichkeit sind Personalakten(daten).
Integrität	*Definition: Integrität* bezeichnet die Anforderung, dass Informationen und personenbezogene Daten, seit der letzten autorisierten Veränderung unverändert sind. Sie haben vollständig, richtig und aktuell zu sein. Es sind jegliche Veränderungen an gespeicherten Informationen durch unberechtigte Dritte auszuschließen oder zumindest so erkennbar zu machen, dass sie korrigiert werden können.
	Beispiele: Werden Klausurergebnisse gespeichert, so ist für die Speicherung Integrität nötig, da sonst Klausurergebnisse von unbefugten Dritten verändert werden könnten.
Verfügbarkeit	*Definition: Verfügbarkeit* bezeichnet die Anforderung, dass Informationen und personenbezogene Daten, abrufbar sein müssen. Personenbezogene Daten müssen und dürfen (nur) solange verarbeitet werden, wie ein Zweck zur Datenverarbeitung gegeben ist.
	Beispiel: Informationen für Gehaltsabrechnungen haben beispielweise einen hohen Schutzbedarf der Verfügbarkeit, da ohne diese nicht mehr die korrekten Gehälter gezahlt werden können.

Zusätzliche Anforderungen in Bezug auf personenbezogene Daten[1]:

Datenminimierung	*Definition:* Datenminimierung bezeichnet die Anforderung, dass, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken sind. Dies betrifft gleichermaßen die Menge und den Umfang der verarbeiteten personenbezogenen Daten sowie ihre Speicherfrist und ihre Zugänglichkeit.
	Beispiel: Im Rahmen einer Studie werden personenbezogene Daten im Vorfeld ihrer Auswertung pseudonymisiert,
Nichtverkettung	*Definition:* Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt werden. Sie ist insbesondere dann maßgeblich, wenn personenbezogen Daten für unterschiedliche Zwecke erhoben wurden.
	Beispiel: Der Personalbereich verarbeitet Kontodaten zwecks Überweisung von monatlichen Gehaltszahlungen. Darüber hinaus werden Kontodaten in Zusammenhang mit einer Spendenaktion an anderer Stelle verarbeitet. Die jeweils erhobenen personenbezogenen Daten müssen getrennt verarbeitet werden. Die mit den Verarbeitungsprozessen betrauten Mitarbeiter*innen dürfen ausschließlich Zugriff auf den von ihnen zu verarbeitenden Datenverarbeitungsvorgang haben.
Transparenz	*Definition:* Transparenz bezeichnet die Anforderung, dass alle an einer Verarbeitung personenbezogener Daten beteiligten Akteure (Betroffene, Betreiber von Systemen, Kontrollinstanzen) von ihrer Entstehung bis zum Ende erkennen und nachvollziehen können, ob, wann, von wem, zu welchem Zweck, durch welche Systeme und auf welche Art und Weise personenbezogene Daten verarbeitet werden.
	Beispiel: Die Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten gewährleistet die Transparenz.
Intervenierbarkeit	*Definition:* Intervenierbarkeit bezeichnet die Anforderung, dass jede von einer Datenverarbeitung betroffene Person, zu jeder Zeit, die ihnen dabei zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen gelten machen können und die verarbeitende Stelle diese Rechte wirksam umzusetzen hat mitsamt der erforderlichen Maßnahmen.
	Beispiel: Jede von einer Datenverarbeitung betroffene Person, hat zu jeder Zeit ein Recht darauf, Auskunft darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über ihre personenbezogenen Daten. Zeigt sich dabei bspw., dass diese Daten nicht mehr verarbeitet werden dürfen, hat die Person, sofern die gesetzlichen Voraussetzungen erfüllt sind, ein Recht darauf, dass die sie betreffenden personenbezogenen Daten gelöscht werden.

[1] Aus Gründen der Lesbarkeit wurde auf die zu den einzelnen Gewährleistungszielen zugehörige Nennung konkreter datenschutzrechtlicher Vorschriften verzichtet.

Schadenswirkung	*Definition:* Werden die Sicherheits- und Gewährleistungsziele nicht erfüllt, so kann dies auf verschiedene Arten und Weisen zu Schaden führen. Eine spezielle Art und Weise in der Schaden entsteht, nennt man *Schadenswirkung.*
	Beispiele: Im Rahmen einer Forschungskooperation mit der Wirtschaft erhält ein Lehrstuhl Geschäftsgeheimnisse eines Unternehmens. Der Lehrstuhl ist daher vertraglich verpflichtet die Informationen geheim zu halten. Nun werden die Informationen aus Versehen vom Lehrstuhl veröffentlicht. Daher muss er nun eine Vertragsstrafe zahlen. Die *Schadenswirkung* ist in diesem Fall finanzieller Natur. Selbstverständlich können sich in diesem Fall noch weitere Schadenswirkungen, wie zum Beispiel der Verlust von öffentlichem Ansehen ergeben. Ein Arbeitgeber hat über einen seiner Beschäftigten die Information erhalten, dass sich dieser erst kürzlich zu einer bestimmten Religion bekannt hat. Die Information wird auf einem Betriebsausflug zum Thema, wodurch der betroffene Beschäftigte durch verachtende Aussagen einiger Kolleg*innen angeprangert wird und dadurch einen hohen immateriellen Schaden erleidet (Diskriminierung).
Schutzbedarf und Risiko	*Definition:* Der *Schutzbedarf* von Informationen in Bezug auf eine der oben genannten Sicherheitsziele ergibt sich aus den Konsequenzen, die sich aus der Verletzung der Eigenschaft ergeben können. Dabei werden bereits getroffene Vorkehrungen *nicht* berücksichtigt. Im Gegensatz zur Risikoanalyse spielt die Eintrittswahrscheinlichkeit somit keine Rolle, bewertet wird der Schaden der sich aus einer Verletzung ergeben kann. Der Schutzbedarf betroffener Personen ergibt sich aus dem für die Personen bestehenden grundsätzlichen Risiko. Ein Risiko im Sinne der DS-GVO ist dabei das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das einen Schaden für die Rechte und Freiheiten natürlicher Personen darstellt oder zu einem Schaden für eine oder mehrere natürliche Personen führen kann. Relevant sein können physische, materielle und immaterielle Schäden. Der Schutzbedarf einer Person entsteht aus den Risiken, die eine Verarbeitungstätigkeit mit Personenbezug ohne technische und organisatorische Maßnahmen erzeugen würde. Zusätzlich zur Schutzbedarfsfeststellung wird für die einzelnen Verarbeitungen personenbezogener Daten das Risiko für die Betroffenen im Rahmen einer so genannten Schwellwertanalyse abgeschätzt, um ggf. eine datenschutzrechtlich erforderliche Datenschutzfolgenabschätzung durchzuführen. Im Einzelfall ist eine individuelle Beratung notwendig.
	Beispiel: Es wird der Schutzbedarf der Vertraulichkeit von Patientendaten betrachtet, die bei einem Arzt gespeichert sind. Sollten diese ohne das Bestehen einer wirksamen gesetzlichen Grundlage veröffentlicht werden, die Vertraulichkeit also verletzt werden, so hätte dies schwere Konsequenzen sowohl für den Arzt als auch für den Patienten. Diese Konsequenzen haben dabei die Form von Schadenswirkungen, können also zum Beispiel finanzieller Art sein, das Ansehen des Arztes oder die gesellschaftliche Stellung des Patienten betreffen. Aufgrund dieser sehr hohen potentiellen Schäden wird der Arzt daher den Schutzbedarf der Vertraulichkeit seiner Patientendaten als sehr hoch einstufen und entsprechende Maßnahmen zum Schutz ergreifen. Die getroffenen Maßnahmen sind dabei Konsequenz des Schutzbedarfs, beeinflussen diesen aber nicht.

5) Festlegung Schutzbedarfskategorien an der Universität Paderborn

Zweck der folgenden Festlegungen ist es ein verbindliches Rahmenwerk zur Einordnung von Schutzbedarfen festzulegen.

Schadenwirkung	**Normal**	**Hoch**	**Sehr hoch**
Verstoß gegen Gesetze, Vorschriften und Verträge im Allgemeinen	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen. Strafen sind ohne finanzielle Einschnitte bestreitbar.	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen. Strafen sind nicht ohne finanzielle Einschnitte bestreitbar.	Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind.
Beeinträchtigung des informationellen Selbstbestimmungsrechts / des Schutzes personenbezogener Daten im Besonderen	Ein Missbrauch personenbezogener Daten hätte höchstens geringfügige Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse betroffener Personen. Beispiele für solche Daten sind Teilnahmelisten von Lehrveranstaltungen, Verträge, Bauakten oder Angebote mit Angaben zu den bearbeitenden Personen.	Ein Missbrauch personenbezogener Daten hätte erhebliche Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse betroffener Personen. Beispiele für solche Daten sind Gesundheitsdaten, Gewerkschaftszugehörig-keit, religiöse oder politische Anschauungen, oder Ordnungswidrigkeiten.	Ein Missbrauch personenbezogener Daten könnte für betroffene Personen den gesellschaftlichen und/oder wirtschaftlichen Ruin oder eine Gefahr für Leib und Leben bedeuten. Beispiele für solche Daten sind Adressen von potentiellen V-Leuten oder Personen, die dem Zeugenschutzprogramm unterliegen.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Es besteht Gefahr für Leib und Leben.

Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den betroffenen Personen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt bei mehr als 24 Stunden.	Die Beeinträchtigung würde von einzelnen betroffenen Personen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt zwischen vier Stunden und einem Tag.	Die Beeinträchtigung würde von allen betroffenen Personen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als vier Stunden.
Negative Innen- oder Außenwirkung	Ein Missbrauch von Daten führt höchstens zu geringem Ansehens- und/oder Vertrauensverlust eines Teilbereichs der Universität bei einer eingeschränkten Öffentlichkeit.	Ein Missbrauch von Daten führt zu einem Ansehens- und/oder Vertrauensverlust der Universität bei einer eingeschränkten Öffentlichkeit oder zu einem hohen Ansehens- und/oder Vertrauensverlusts eines Teilbereichs der Universität.	Ein Missbrauch von Daten führt zu einem landesweiten Ansehens- und/oder Vertrauensverlust der Universität in der breiten Öffentlichkeit. Sogar eine Gefährdung der Existenz der Universität ist denkbar.
Finanzielle Auswirkungen	Die Summe der finanziellen Auswirkungen ist tolerabel, beträgt weniger als 150.000 Euro.	Die Summe der finanziellen Auswirkungen ist beachtlich aber nicht existenzbedrohend, d.h. weniger als 5.000.000 Euro.	Die Summe der finanziellen Auswirkungen ist existenzbedrohend, beträgt also mehr als 5.000.000 Euro.

6) Orientierungshilfe zur Einordnung des Schutzbedarfs von Informationen

Der Schutzbedarf von Informationen und ggf. betroffenen Personen ist mit Hilfe der obigen Tabelle der für die Universität Paderborn definierten Schutzbedarfskategorien zu bestimmen. Darin sind verschiedene Schadenswirkungen aufgeführt.

Für jede verarbeitete Information sind alle Sicherheits- bzw. Gewährleistungsziele gesondert zu betrachten. Für jedes Sicherheits- bzw. Gewährleistungsziel ist zu bewerten, welches Ausmaß die verschiedenen Schadenswirkungen annehmen, wenn das Sicherheitsziel nicht erreicht wird. So wird der Schutzbedarf bei jeder Information in Bezug auf jedes Sicherheits- bzw. Gewährleistungsziel beurteilt. Konkret geht man dabei wie folgt vor:

1. Es wird jede Kombination aus Sicherheits- bzw. Gewährleistungsziel und Schadenswirkung aus der Tabelle mit den Schutzbedarfskategorien betrachtet.
2. Entsprechend der angegebenen Stufen wird der Schutzbedarf der Information in Bezug auf Sicherheitsziel und Schadenswirkung als „normal“, „hoch“ oder „sehr hoch“ eingeordnet.
3. Der Schutzbedarf eines Sicherheitsziels in dem Bezug auf eine Information, ergibt sich als die höchste Einstufung, die über alle Schadenswirkungen für das Sicherheitsziel ermittelt wurde.
4. Sofern personenbezogene Daten Gegenstand einer Information sind, sind stets die weiteren datenschutzrechtlichen Anforderungen zu beachten, namentlich die Datenminimierung (Datenverarbeitung auf das notwendige Maß beschränken), die Gewährleistung der Nichtverkettung (Daten, die zu unterschiedlichen Zwecken verarbeitet werden, dürfen nicht zusammengeführt werden), die Transparenz (Erkennbarkeit, wer Daten von wem zu welchem Zweck, durch welche Systeme und auf welche Art und Weise verarbeitet) sowie die Intervenierbarkeit (Sicherstellung der Betroffenenrechte (z. B. Auskunft gemäß Art. 15 DS-GVO und ggf. Umsetzung von erforderlichen Maßnahmen)).

Beispiel: Auf einer Liste mit Klausurergebnissen sind Namen, Matrikelnummern und Noten von Studierenden eingetragen. Dazu muss der Schutzbedarf der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit dieser Information bewertet werden.

1. Es wird mit der Einordnung des Schutzbedarfs der Vertraulichkeit der Information begonnen. Um diese Einstufung durchzuführen, nimmt man an, dass die Vertraulichkeit der Information verletzt wird, die Liste also an die Öffentlichkeit gelangt und Unbefugte Kenntnis der Informationen erlangen Nun muss für jede der sechs Schadenswirkungen eingeordnet werden, wie stark diese ausgeprägt ist.
2. Betrachtet wird in diesem Beispiel exemplarisch die Beeinträchtigung des informationellen Selbstbestimmungsrechts als Schadenswirkung.
3. Betrachtet man die Schutzbedarfskategorien, so scheint es plausibel, dass einzelnen Betroffenen ein nicht unerheblicher gesellschaftlicher Ansehensverlust droht, wenn die Vertraulichkeit verletzt wird, indem Noten an die Öffentlichkeit gelangen. Daraus wird geschlossen, dass die Vertraulichkeit dieser Information mindestens als hoch eingeordnet werden muss.
4. Nimmt man für dieses Beispiel an, dass sich für andere Schadenswirkungen kein höherer Schutzbedarf der Vertraulichkeit der Information ergibt, so kann man den Schutzbedarf der Vertraulichkeit der Information als *hoch* einstufen.

Dieses Vorgehen muss nun für alle weiteren Kombinationen aus Sicherheitsziel und Schadenswirkung durchgeführt werden. Als Hilfestellung können die im Anhang befindlichen Fragestellungen verwendet werden. Diese sind an den BSI Grundschutz sowie – in Bezug auf personenbezogene Daten – an das Standard-Datenschutzmodell der unabhängigen Datenschutzbehörden des Bundes und der Länder angelehnt. Darüber hinaus können aus der Tabelle mit Informationsklassen und ihrem üblichen Schutzbedarf der Schutzbedarf für viele Klassen von Informationen bereits entnommen werden.

7) Inkrafttreten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Mitteilungen der Universität Paderborn in Kraft.

Ausgefertigt aufgrund der Einführung eines Informationssicherheitsmanagementsystems an der Universität Paderborn sowie nach Genehmigung durch das Präsidium der Universität Paderborn vom 6. September 2023.

Paderborn, den 24. April 2024

Die Präsidentin
der Universität Paderborn

Professorin Dr. Birgitt Riegraf

Anhang 1: Vorgehen zur Ermittlung eines Schutzbedarfes

Um den Schutzbedarf einer Information sowie ggf. betroffener Personen zu ermitteln, kann man die folgenden Fragestellungen aus dem BSI-Grundschutz[2] zu Rate ziehen. Diese wurden um Aspekte des Standard-Datenschutzmodells der unabhängigen Datenschutzbehörden des Bundes und der Länder ergänzt.

Schadensszenario "Verstoß gegen Gesetze/Vorschriften/Verträge"

Sowohl aus dem Verlust der Vertraulichkeit als auch der Integrität und ebenso der Verfügbarkeit können derlei Verstöße resultieren. Die Schwere des Schadens ist dabei oftmals abhängig davon, welche rechtlichen Konsequenzen daraus für die UPB entstehen können.

Beispiele für relevante Gesetze sind (in Deutschland): Grundgesetz (GG), Bürgerliches Gesetzbuch (BGB), Strafgesetzbuch (StGB), Bundesdatenschutzgesetz (BDSG) und Datenschutzgesetze der Länder (bspw. DSG NRW), EU-Datenschutzgrundverordnung (DS-GVO), Sozialgesetzbuch (SGB), Handelsgesetzbuch (HGB), Personalvertretungsgesetz (PersVH), Urheberrechtsgesetz (UrhG), Patentgesetz (PatG), Telemediengesetz (TMG), Telekommunikationsgesetz (TKG), Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG).

Beispiele für relevante Vorschriften sind: Verwaltungsvorschriften, Verordnungen und Dienstvorschriften.

Beispiele für Verträge sind: Dienstleistungsverträge im Bereich Datenverarbeitung, Verträge zur Wahrung von Betriebsgeheimnissen, Kaufverträge, Lizenzverträge, Arbeitsverträge, Leihverträge.

Fragen:

Verlust der Vertraulichkeit

- Erfordern gesetzliche Auflagen die Vertraulichkeit der Informationen?
- Ist im Falle einer Veröffentlichung von Informationen mit Strafverfolgung oder Regressforderungen zu rechnen?
- Sind Verträge einzuhalten, die die Wahrung der Vertraulichkeit bestimmter Informationen beinhalten?

Verlust der Integrität

- Erfordern gesetzliche Auflagen die Integrität der Informationen?
- In welchem Maße wird durch einen Verlust der Integrität gegen Gesetze bzw. Vorschriftenverstoßen?

Verlust der Verfügbarkeit

- Schreiben Gesetze die dauernde Verfügbarkeit bestimmter Informationen vor? Gibt es vertragliche Bindungen für bestimmte einzuhaltende Termine?

Schadensszenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts“

Insbesondere in Verwaltungsabläufen fallen immer wieder personenbezogene Daten an. Beispiele für die Beeinträchtigung des informationellen Selbstbestimmungsrechts sind insbesondere:

- Unzulässige Verarbeitung personenbezogener Daten ohne Rechtsgrundlage,
- Unbefugte Kenntnisnahme bei der Datenverarbeitung bzw. der unbefugten Offenlegung von personenbezogenen Daten,
- Unbefugte Weitergabe personenbezogener Daten
- Nutzung von personenbezogenen Daten zu einem anderen als dem bei der Erhebung zulässigen Zweck und

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, abgerufen am 28.06.2022

- Verfälschung von personenbezogenen Daten

Die folgenden Fragen können zur Abschätzung möglicher Folgen und Schäden herangezogen werden:

Fragen:

Verlust der Vertraulichkeit

- Welche Schäden können für den Betroffenen entstehen, wenn seine personenbezogenen Daten nicht vertraulich behandelt werden?
- Werden personenbezogene Daten für unzulässige Zwecke verarbeitet?
- Ist es im Zuge einer zulässigen Verarbeitung personenbezogener Daten möglich, aus diesen Daten z. B. auf den Gesundheitszustand oder die wirtschaftliche Situation einer Person zu schließen?
- Welche Schäden können durch den Missbrauch der gespeicherten personenbezogenen Daten entstehen?
- Fehlt es an einer gesetzlichen oder vertraglich vereinbarten Verschwiegenheitspflicht der mit der Datenverarbeitung befassten Personen?

Verlust der Integrität

- Welche Schäden würden für den Betroffenen entstehen, wenn seine personenbezogenen Daten unabsichtlich verfälscht oder absichtlich manipuliert würden?
- Wann würde der Verlust der Integrität personenbezogener Daten frühestens auffallen?
- Welche Schäden würden für den Betroffenen entstehen, wenn seine personenbezogenen Daten nicht richtig oder fehlerhaft sind?
- Können die verfälschten personenbezogenen Daten eine Diskriminierung auslösen?

Verlust der Verfügbarkeit

- Können personenbezogene Daten verloren gehen oder so verfälscht werden, so dass der Betroffene in seiner gesellschaftlichen Stellung beeinträchtigt wird oder gar persönliche oder wirtschaftliche Nachteile zu befürchten hat?

Verlust der Nichtverkettung:

- Welche Schäden können entstehen, wenn personenbezogen Daten mit anderen Daten vermischt werden und die Verkettung von Daten missbraucht wird oder Unbefugten zur Kenntnis erlangt
- Werden personenbezogene Daten für unzulässige Zwecke verarbeitet?
- Sind die Zwecke nicht festgelegt?
- Sind die Zwecke nicht eindeutig?
- Sind die Zwecke nicht legitim?

Verlust der Transparenz

- Fehlt es an erforderlichen Informationspflichten gemäß Art. 13 und 14 DS-GVO?
- Sind Verarbeitungsprozesse von personenbezogenen Daten nicht dokumentiert?
- Fehlt es an einem Einwilligungsmanagement?
- Gibt es Informationen zu der Verarbeitung personenbezogener Daten für die betroffenen Person?
- Werden personenbezogene Daten schwer verständlich oder unter nur schwer zugänglichen Informationen verarbeitet?
- Ist die Überwachung der Verarbeitung nicht angemessen?
- Wurde eine Rechenschaftspflicht gegenüber den betroffenen Personen und/oder gegenüber der Aufsichtsbehörde nicht erfüllt?

Verlust der Intervenierbarkeit

- Fehlt es an Möglichkeiten/Prozessen zur Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit von personenbezogenen Daten?
- Fehlt es an Prozessen, die eine Auskunftserteilung nicht ermöglichen?

- Fehlt es an datenschutzfreundlichen Voreinstellungen?
- Fehlt es an Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen?

Schadensszenario „Beeinträchtigung der Aufgabenerfüllung“

Gerade der Verlust der Verfügbarkeit oder der Integrität von Informationen oder personenbezogenen Daten kann die Aufgabenerfüllung in einer Institution erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele hierfür sind:

- Fristversäumnisse durch verzögerte Bearbeitung von Verwaltungsvorgängen und
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen

Fragen:

Verlust der Vertraulichkeit

- Gibt es Informationen, deren Vertraulichkeit die Grundlage für die Aufgabenerfüllung ist (z. B. Forschungsergebnisse oder Verwaltungsdaten)?

Verlust der Integrität

- Können Veränderungen an Informationen die Aufgabenerfüllung in der Art einschränken, dass die Institution handlungsunfähig wird?
- Entstehen erhebliche Schäden, wenn die Aufgaben trotz verfälschter Informationen wahrgenommen werden? Wann werden unerlaubte Veränderungen frühestens erkannt?
- Welche Folgen entstehen, wenn Informationen fälschlicherweise einer Person zugeordnet werden, die in Wirklichkeit diese Informationen nicht erzeugt hat?

Verlust der Verfügbarkeit

- Gibt es Informationen, bei denen eine Einschränkung der Verfügbarkeit schwerwiegende Auswirkungen auf die Institution oder deren Geschäftsprozesse hätte?
- Ist es für die Institution bedeutsam, dass der Zugriff auf erforderliche Informationen ständig gewährleistet ist?

Schadensszenario "Negative Innen- oder Außenwirkung"

Durch den Verlust einer der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit können verschiedenartige negative Innen- oder Außenwirkungen entstehen, zum Beispiel:

- Ansehensverlust der UPB,
- Vertrauensverlust gegenüber einer anderen Institution,
- Demoralisierung der Mitarbeiter*innen,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Institutionen,
- verlorenes Vertrauen in die Arbeitsqualität der UPB und
- Einbuße der Konkurrenzfähigkeit.

Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes oder des Verbreitungsgrades der Innen- oder Außenwirkung. Die Ursachen für solche Schäden können vielfältiger Natur sein:

- fehlerhafte Veröffentlichungen durch manipulierte Informationen,
- Nichteinhaltung von Verschwiegenheitserklärungen,
- Schuldzuweisungen an die falschen Personen,
- Verhinderung der Aufgabenerfüllung einer Abteilung durch Fehler in anderen Bereichen,
- Zuspielen vertraulicher Informationen an die Presse.

- Preisgabe von personenbezogenen Daten ohne Rechtsgrundlage, etwa an die Polizei aufgrund bloßer Anfrage

Fragen:

Verlust der Vertraulichkeit

- Welche Konsequenzen ergeben sich für die UPB durch die unerlaubte Veröffentlichung von schutzbedürftigen Informationen?
- Kann der Vertraulichkeitsverlust zu einer Schwächung der Wettbewerbsposition führen?
- Entstehen bei Veröffentlichung Zweifel an der Vertrauenswürdigkeit der UPB?
- Können Veröffentlichungen zur politischen oder gesellschaftlichen Verunsicherung führen?
- Können Mitarbeiter*innen durch die unzulässige Veröffentlichung das Vertrauen in die UPB verlieren?

Verlust der Integrität

- Welche Schäden können sich durch die Verarbeitung, Verbreitung oder Übermittlung falscher oder unvollständiger Informationen und/oder personenbezogener Daten ergeben?
- Wird die Verfälschung öffentlich bekannt?
- Entstehen bei einer Veröffentlichung von verfälschten Informationen und personenbezogenen Daten Ansehensverluste?
- Können Veröffentlichungen von verfälschten Informationen und personenbezogenen Daten zur politischen oder gesellschaftlichen Verunsicherung führen?

Verlust der Verfügbarkeit

- Verhindert die Nichtverfügbarkeit von Informationen und personenbezogenen Daten die Erreichung von Geschäftszielen?
- Ab wann wird die Nichtverfügbarkeit von Informationen und personenbezogenen Daten extern bemerkt?

Schadensszenario "Finanzielle Auswirkungen"

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Informationen und personenbezogene Daten, die Veränderung von Informationen und personenbezogene Daten oder den Ausfall von Anwendungen entstehen. Beispiele dafür sind:

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
- Manipulation von finanzwirksamen Informationen und
- unerlaubte Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen

Fragen:

Verlust der Vertraulichkeit

- Kann die Veröffentlichung vertraulicher Informationen und personenbezogene Daten Regressforderungen nach sich ziehen?
- Werden Forschungsdaten gespeichert, die einen erheblichen Wert darstellen? Was passiert, wenn sie unerlaubt kopiert und weitergegeben werden?
- Können durch vorzeitige Veröffentlichung von schutzbedürftigen Informationen finanzielle Schäden entstehen?

Verlust der Integrität

- Können durch Datenmanipulationen finanzwirksame Informationen so verändert werden, dass finanzielle Schäden entstehen?
- Kann die Veröffentlichung falscher Informationen Regressforderungen nach sich ziehen?
- Können durch verfälschte Bestelldaten finanzielle Schäden entstehen?
- Können verfälschte Informationen zu falschen Geschäftsentscheidungen führen?

Verlust der Verfügbarkeit

- Kann es durch Nichtverfügbarkeit von Informationen zu mangelnder Zahlungsfähigkeit oder zu Konventionalstrafen kommen?

Anhang 2: Klassen von Informationen und ihr üblicher Schutzbedarf

Einleitung

Eine vollständige Schutzbedarfsfeststellung für Informationen durchzuführen ist zeitaufwändig. Daher werden in diesem Anhang Klassen von Informationen definiert, die im Arbeitsalltag an der Universität Paderborn (UPB) häufig vorkommen. Jeder Klasse sind dabei die üblichen Schutzbedarfe der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen der Klasse beigefügt. So kann für zahlreiche Informationen ein angemessener Schutzbedarf abgeleitet werden, ohne dafür eine Schutzbedarfsfeststellung als Einzelfallprüfung durchzuführen. Die folgende Einteilung entspricht damit einem „Schnelltest“ – im Zweifel ersetzt die Klassifizierung NICHT die Einzelfallprüfung. An einigen Stellen unterscheiden sich die Schutzbedarfe bzgl. der Kategorien Vertraulichkeit, Verfügbarkeit und Integrität. In diesem Fall muss generell von dem höheren Schutzbedarf ausgegangen werden, um entsprechende Maßnahmen zur Sicherheit festzulegen.

Sofern personenbezogene Daten Gegenstand von Informationen sind, sind ferner die weiteren datenschutzrechtlichen Anforderungen zu beachten, namentlich die Datenminimierung (Daten werden nur beschränkt auf das notwendige Maß verarbeitet), die Nichtverkettung (Daten, die zu unterschiedlichen Zwecken verarbeitet werden, dürfen nicht zusammengeführt werden), die Transparenz (Erkennbarkeit, wer Daten von wem zu welchem Zweck, durch welche Systeme und auf welche Art und Weise verarbeitet) sowie die Intervenierbarkeit (Sicherstellung der Betroffenenrechte (z. B. Auskunft gemäß Art. 15 DS-GVO und ggf. Umsetzung von erforderlichen Maßnahmen)).

Verwaltungsdaten

Informationsklasse	Typischer Schutzbedarf der Vertraulichkeit	Typischer Schutzbedarf der Verfügbarkeit	Typischer Schutzbedarf der Integrität
Dienstliche Kontaktdaten von Beschäftigten, beispielsweise Telefonnummer oder E-Mail-Adresse, Anschrift	Normal	Normal	Normal
Private Kontaktdaten von Beschäftigten, beispielsweise Telefonnummer, E-Mail-Adressen	Normal bis Hoch	Normal bis Hoch	Normal bis Hoch
Daten ohne Personenbezug, die aus öffentlich zugänglichen Quellen stammen	Normal	Normal	Normal
Regelungen der Fakultäten und Einrichtungen wie beispielsweise Umläufe	Normal	Normal	Normal
Verträge mit Partnern der Universität, die keine Vertraulichkeit verlangen	Normal bis Hoch	Normal bis Hoch	Normal bis Hoch
Angebote	Normal bis Hoch	Normal bis Hoch	Normal bis Hoch
Auftragsbestätigungen	Normal	Normal bis Hoch	Normal bis Hoch
Kreditunterlagen	Hoch	Hoch	Hoch
Geschäftsbriefe	Normal bis Hoch	Normal bis Hoch	Normal bis Hoch
Versicherungspolicen	Normal	Hoch	Hoch
Abrechnungsunterlagen	Hoch	Hoch	Hoch
Bankbelege	Hoch	Hoch	Hoch
Eingangsrechnungen	Normal bis Hoch	Normal bis Hoch	Normal bis Hoch
Wareneingangs- und Zahlungsausgangsbücher	Hoch	Hoch	Hoch
Zahlungsanweisung	Hoch	Hoch	Hoch
Fahrtkostenerstattung	Normal bis Hoch	Normal	Normal bis Hoch
Infektionsschutzgesetz-Gesundheitszeugnis und letzte Dokumentation der Belehrung	Normal	Normal	Normal
Jugendarbeitsschutzunterlagen	Normal	Normal	Normal
Haushaltsdaten	Hoch	Hoch	Hoch

Personaldaten

Dateiklasse	Typischer Schutzbedarf der Vertraulich-keit	Typischer Schutzbedarf der Verfügbar-keit	Typischer Schutzbedarf der Integrität
Personalstammdaten	Hoch	Hoch	Hoch
Geburtsdatum	Hoch	Hoch	Hoch
Gehaltslisten	Hoch	Hoch	Hoch
Bruttolohnlisten	Hoch	Hoch	Hoch
Arbeitnehmerüberlassung – Ge-schäftsunterlagen des Verleihers	Hoch	Hoch	Hoch
Arbeitszeitnachweise	Normal	Hoch	Hoch
Lohnunterlagen (Sozialversicherung)	Hoch	Hoch	Hoch
Mutterschutzunterlagen	Hoch	Hoch	Hoch
Versorgungsaktendaten	Hoch	Hoch	Hoch
Unterlagen über Erholungsurlaub	Normal	Normal	Normal
Arbeitszeitnachweise bei gleitender Arbeitszeit	Normal	Hoch	Hoch

Studierendendaten

Dateiklasse	Typischer Schutzbedarf der Vertraulichkeit	Typischer Schutzbedarf der Verfügbarkeit	Typischer Schutzbedarf der Integrität
Studierendenstammdaten	Hoch	Hoch	Hoch
E-Mail-Adresse an der Universität	Normal	Normal	Normal
Zeugnisse	Hoch	Hoch	Hoch
Anwesenheitslisten	Hoch	Hoch	Hoch
Zuordnung von Matrikelnummer zum Namen	Hoch	Hoch	Hoch
Korrigierte Klausuren	Hoch	Hoch	Hoch
Übungszettel	Normal	Normal	Normal
Haus-/Seminararbeiten	Normal	Normal	Normal

Kommunikation mit Studierenden	Normal	Normal	Normal
Abschlussarbeiten	Normal	Hoch	Hoch
Anträge für Abschlussarbeiten	Normal	Normal	Normal
Gutachten für einzelne Abschlussarbeiten	Hoch	Normal	Hoch
Noten für einzelne Veranstaltungen	Normal bis Hoch	Normal	Hoch
Noten die einen Überblick über die Gesamtleistung Studierender geben	Hoch	Normal	Hoch

Wissenschaftliche Daten

Dateiklasse	Typischer Schutzbedarf der Vertraulichkeit	Typischer Schutzbedarf der Verfügbarkeit	Typischer Schutzbedarf der Integrität
Wissenschaftliche Daten (z. B. Untersuchungsergebnisse, Messreihen), die noch nicht publiziert worden sind	Normal bis Hoch	Normal bis Hoch	Normal bis Hoch
Wissenschaftliche Daten, die durch vertragliche Vereinbarungen (z. B. aus Kooperationen) einen besonderen Schutzbedarf haben.	Hoch	Hoch	Hoch

Gesundheitsdaten

Dateiklasse	Typischer Schutzbedarf der Vertraulichkeit	Typischer Schutzbedarf der Verfügbarkeit	Typischer Schutzbedarf der Integrität
Unterlagen über Beihilfe, Heilfürsorge, Heilverfahren, Unterstützungen, Erkrankungen	Hoch	Hoch	Hoch
Berufsgenossenschaftliche Verletzungsverfahren	Hoch	Hoch	Hoch
Weitere Gesundheitsdaten	Hoch bis Sehr hoch	Hoch bis Sehr hoch	Hoch bis Sehr hoch

Arbeitsschutz

Dateiklasse	Typischer Schutzbedarf der Vertraulich-keit	Typischer Schutzbedarf der Verfügbar-keit	Typischer Schutzbedarf der Integrität
Chemikalien (Prüfpläne, vorgenom-mene Inspektionen, Einweisungen, u.a.m.)	Normal	Hoch	Normal
Gefährliche Arbeitsstoffe	Normal	Normal	Normal
Kartei über arbeitsmedizinische Vor-sorgeuntersuchungen im Gefahrstoff-bereich	Hoch bis Sehr hoch	Hoch bis Sehr hoch	Hoch bis Sehr hoch
Psychologische Gefährdungen am Ar-beitsplatz	Normal	Normal	Normal

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Guideline for classifying the need for protection of information taking into ac-count the protection of personal data at Paderborn University

24 April 2024

Document properties

Responsibility	CIO / Information Security Officer
Classification	S2 Internal
Validity period	Unlimited
Revision interval	Annually
Next revision	March 2025
Storage location / file name	Sharepoint Information Security RL016

Document status and release

Status	Version	Date	Name / Department / Company
Creation	0.1	2022-06-21	Kampmeyer / IST
Release	1.0	2023-09-06	Presidium

Document history

Version	Amendment	Date	Author of the change
0.1	Summary of the individual documents • RL001 2020 Definition of protection require-ment categories • RL002 2020 Classes of information and their common protection needs • RL003 2020 Guideline for classifying the protection requirements of information Version tracking added	2022-06-21	Kampmeyer / IST
0.2	Link and spelling corrected	2022-07-04	Kampmeyer / IST
1.1	Editorial changes	2024-02-20	Porombka / IST
1.2	Header and footer formatting Document classification is now S1 Public Added Effective Date(s) section	2024-04-24	Kampmeyer / IST

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

1) Introduction

In their day-to-day work, members of Paderborn University (UPB) regularly come into contact with a wide variety of information. The publication, modification or loss of some of this information can have serious consequences for UPB, but also for the individuals whose data is processed.

The subject matter of information regularly includes personal data. Personal data is any information relating to an identified or identifiable natural person (hereinafter "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art. 4 No. 1 of the EU General Data Protection Regulation (GDPR)). In this respect, there is a fundamental right to informational self-determination, which arises from the general right of personality (Art. 2 para. 1 in conjunction with Art. 1 para. V. m. Art. 1 para. 1 of the German Basic Law (GG)). In addition, the protection of personal data is expressly enshrined in Art. 8 of the EU Charter of Fundamental Rights (CFR), which all EU citizens can invoke. These fundamental rights guarantees are implemented by European and national legal requirements. Accordingly, risks for natural persons with regard to data processing concerning them must be prevented, in particular on the basis of the basic principles set out in Art. 5 GDPR (lawfulness, purpose limitation, ...), which may also indirectly have consequences for the UPB.

This guideline deals with the determination of the need for protection of information and the need for protection of data subjects of the data concerning them. Once the need for protection has been determined, rules for handling the information and/or personal data can be defined and implemented on this basis.

2) Scope of application

This policy is binding for all employees of the UPB. It specifies how UPB employees must classify the need for protection of information, including personal data.

3) Objective

The aim of this document is to define binding rules for determining the need for protection of information and personal data at UPB. The need for protection indicates the severity of the consequences of a breach of the security and guarantee objectives defined below for UPB and, if applicable, for the data subject. Other guidelines or recommendations can then use this determination of the need for protection to define rules for handling the information and personal data.

However, protection needs assessments do not have to be carried out by employees for each individual piece of information, but are usually carried out centrally for individual processing activities (student administration, application procedures, examination administration, ...) as part of the creation of the list of processing activities required for each processing activity of personal data. The assessment of protection requirements is supported by the data protection coordinators, the data protection officer and the security officers.

The UPB thus carries out basic assessments of protection requirements for certain categories of data (course registrations, personnel files, grant data, etc.) and makes them available to employees, so that

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

an assessment of protection requirements generally only has to be carried out for new processing activities that have not yet been documented.

4) Definitions of terms

The following table defines important terms for understanding the document and explains them using examples.

Safety targets and warranty targets	*Definition:* A security target is a property of information whose violation can have negative consequences. The protection of personal data is reflected in legally enshrined requirements. In particular, the GDPR and state-specific national regulations, such as the North Rhine-Westphalia Data Protection Act (DSG NRW) plus more specific regulations, are decisive for this. The resulting legal requirements can be bundled and structured by so-called guarantee objectives with the aim of mitigating the risks associated with data processing for the rights and freedoms of natural persons through technical and organizational measures. The following table looks specifically at the three security objectives of confidentiality, integrity and availability, as well as the additional security objectives of data minimization, non-linking, transparency and intervenability, which are also relevant for personal data.
Confidentiality	*Definition: Confidentiality* refers to the requirement that information and personal data may only be accessible to a limited group of authorized persons. Unauthorized persons are generally all persons who have no connection to the content of data processing or to the person concerned.
	Examples: A typical example with a high need for confidentiality is personnel files (data).
Integrity	*Definition: Integrity* refers to the requirement that information and personal data remain unchanged since the last authorized change. They must be complete, correct and up-to-date. Any changes to stored information by unauthorized third parties must be excluded or at least made recognizable in such a way that they can be corrected.
	Examples: If exam results are stored, integrity is required for storage, as otherwise exam results could be changed by unauthorized third parties.
Availability	*Definition: Availability* refers to the requirement that information and personal data must be retrievable. Personal data must and may (only) be processed for as long as there is a purpose for processing the data.
	Example: Information for payslips, for example, has a high protection requirement for availability, as the correct salaries can no longer be paid without it.
Additional requirements in relation to personal data*) :	

READING COPY

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Data minimization	*Definition:* Data minimization refers to the requirement that the processing of personal data must be limited to what is appropriate, relevant and necessary for the purpose. This applies equally to the amount and scope of personal data processed as well as their retention period and accessibility.
	Example: As part of a study, personal data is pseudonymized before it is evaluated,
Non-linking	*Definition:* Non-interlinking refers to the requirement that personal data is not merged. It is particularly relevant when personal data is collected for different purposes.
	Example: The HR department processes account data for the purpose of transferring monthly salary payments. In addition, account data is processed elsewhere in connection with a fundraising campaign. The personal data collected in each case must be processed separately. The employees entrusted with the processing operations may only have access to the data processing operation they are processing.
Transparency	*Definition:* Transparency refers to the requirement that all parties involved in the processing of personal data (data subjects, system operators, supervisory authorities) are able to recognize and understand from its origin to its end whether, when, by whom, for what purpose, through which systems and in what way personal data is processed.
	Example: Documentation in the form of an inventory of all processing activities ensures transparency.
Intervenability	*Definition:* Intervenability means the requirement that any person affected by data processing can, at any time, exercise their rights to notification, access, rectification, erasure, restriction of data portability, objection and intervention in automated individual decisions if the legal requirements are met, and that the data controller must effectively implement these rights together with the necessary measures.
	Example: Any person affected by data processing has the right to obtain information at any time as to whether personal data concerning them is being processed; if this is the case, they have the right to access their personal data. If it turns out, for example, that this data may no longer be processed, the person has the right to have the personal data concerning them deleted, provided that the legal requirements are met.
Damage effect	*Definition:* If the safety and warranty objectives are not met, this can lead to damage in various ways. One specific way in which damage occurs is called *the damage effect.*
	Examples: As part of a research cooperation with industry, a chair receives business secrets from a company. The chair is therefore contractually obliged to keep the information secret. Now the information is accidentally published by the chair. As a result, it must now pay a contractual penalty. The *damages in*

REFERENCE

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

	this case are of a financial nature. Of course, this case can also result in other damages, such as loss of public reputation. An employer has been informed by one of his employees that he has recently professed a particular religion. The information becomes a topic of discussion at a company outing, as a result of which the employee concerned is denounced by contemptuous statements from some colleagues and suffers considerable non-material damage (discrimination).
Protection requirements and risk	*Definition:* The *need for protection* of information in relation to one of the above security objectives results from the consequences that may arise from a breach of the property. Precautions already taken are *not* taken into account. In contrast to risk analysis, the probability of occurrence does not play a role; the damage that may result from a breach is assessed. The need for protection of data subjects results from the fundamental risk posed to them. A risk within the meaning of the GDPR is the existence of the possibility of the occurrence of an event which may result in damage to the rights and freedoms of natural persons or damage to one or more natural persons. Physical, material and immaterial damage can be relevant. A person's need for protection arises from the risks that a processing activity involving a person would create without technical and organizational measures. In addition to the determination of protection requirements, the risk for the data subjects is assessed for the individual processing of personal data as part of a so-called threshold value analysis in order to carry out a data protection impact assessment required under data protection law if necessary. Individual consultation is necessary in individual cases.
	Example: The need to protect the confidentiality of patient data stored by a doctor is considered. If these were to be published without the existence of an effective legal basis, i.e. if confidentiality were to be breached, this would have serious consequences for both the doctor and the patient. These consequences can take the form of damage, for example financial damage, damage to the doctor's reputation or damage to the patient's social standing. Due to these very high potential damages, the doctor will therefore classify the need to protect the confidentiality of his patient data as very high and take appropriate measures to protect it. The measures taken are a consequence of the need for protection, but do not influence it.

*) For reasons of readability, the specific data protection regulations associated with the individual warranty objectives have been omitted.

REPRINTED

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

5) Definition of protection requirement categories at Paderborn University

The purpose of the following specifications is to define a binding framework for classifying protection requirements.

Damage effect	Normal	High	Very high
Violation of laws, regulations and contracts in general	Violations of regulations and laws with minor consequences. Minor breaches of contract with maximum minor contractual penalties. Penalties are contestable without financial penalties.	Violations of regulations and laws with considerable consequences. Breaches of contract with high contractual penalties. Penalties cannot be disputed without financial losses.	Fundamental breach of regulations and laws Breaches of contract whose liability damages are ruinous.
Impairment of the right to informational self-determination / protection of personal data in particular	Any misuse of personal data would have at most a minor impact on the social position and/or economic circumstances of the persons concerned. Examples of such data are attendance lists for courses, contracts, construction files or offers with details of the persons processing them.	Any misuse of personal data would have a considerable impact on the social status and/or economic circumstances of the persons concerned. Examples of such data are health data, trade union membership, religious or political views, or administrative offenses.	Misuse of personal data could mean social and/or economic ruin or a danger to life and limb for the persons concerned. Examples of such data are addresses of potential informants or persons subject to the witness protection program.
Impairment of personal integrity	Impairment does not appear possible.	Impairment of personal integrity cannot be absolutely ruled out.	Serious damage to personal integrity is possible. There is a risk to life and limb.
Impairment of the fulfillment of tasks	The impairment would be considered tolerable by the persons affected. The maximum tolerable downtime is more than 24 hours.	The impairment would not be considered tolerable by individual affected persons. The maximum tolerable downtime is between four hours and one day.	The impairment would be considered intolerable by all affected persons. The maximum tolerable downtime is less than four hours.

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Negative internal or external impact	Misuse of data leads at most to a slight loss of reputation and/or trust of a part of the university among a limited public.	Misuse of data leads to a loss of reputation and/or trust of the university among a limited public or to a high loss of reputation and/or trust of a part of the university.	Misuse of data leads to a nationwide loss of reputation and/or trust in the university among the general public. It could even jeopardize the existence of the university.
Financial impact	The total financial impact is tolerable, amounting to less than 150,000 euros.	The total financial impact is considerable but not life-threatening, i.e. less than EUR 5,000,000.	The total financial impact is life-threatening, i.e. amounts to more than EUR 5,000,000.

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

6) Guidance on classifying the need for protection of information

The protection requirements of information and, where applicable, affected persons must be determined using the above table of protection requirement categories defined for Paderborn University. Various damage effects are listed therein.

All safety or warranty objectives must be considered separately for each piece of information processed. For each security or guarantee objective, the extent to which the various damage effects will occur if the security objective is not achieved must be assessed. In this way, the need for protection is assessed for each piece of information in relation to each safety or guarantee objective. In concrete terms, the procedure is as follows:

5. Each combination of safety or warranty objective and damage effect from the table with the protection requirement categories is considered.
6. The protection requirements of the information are classified as "normal", "high" or "very high" in relation to the security objective and impact of the damage according to the levels specified.
7. The protection requirement of a security target in relation to a piece of information is calculated as the highest classification that was determined for the security target across all damage effects.
8. If personal data is the subject of information, the other data protection requirements must always be observed, namely data minimization (limiting data processing to what is necessary), ensuring non-linking (data that is processed for different purposes must not be merged), transparency (recognizability of who processes data, by whom, for what purpose, through which systems and in what way) and intervenability (ensuring the rights of data subjects (e.g. information in accordance with Art. 15 GDPR and, if necessary, implementation of necessary measures)).

Example: The names, student numbers and grades of students are entered on a list of exam results. The need to protect the security objectives of confidentiality, integrity and availability of this information must be assessed.

5. The first step is to classify the need to protect the confidentiality of the information. In order to carry out this classification, it is assumed that the confidentiality of the information is breached, i.e. the list is made public and unauthorized persons gain knowledge of the information.
6. In this example, the impairment of the right to informational self-determination is considered as a damaging effect.
7. Looking at the protection requirement categories, it seems plausible that individual data subjects are at risk of a not inconsiderable loss of social standing if confidentiality is breached by leaking notes to the public. This leads to the conclusion that the confidentiality of this information must be classified as at least high.
8. If one assumes for this example that there is no higher need to protect the confidentiality of the information for other damaging effects, the need to protect the confidentiality of the information can be classified as *high.*

This procedure must now be carried out for all further combinations of safety objective and damage effect. The questions in the appendix can be used as an aid. These are based on the BSI basic protection and - with regard to personal data - on the standard data protection model of the independent federal and state data protection authorities. In addition, the protection requirements for many classes of information can already be taken from the table with information classes and their usual protection requirements.

FREIGEGEBEN

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

7) Coming into force

This guideline comes into force on the day after its publication in the Official Notices of Paderborn University.

Issued due to the introduction of an information security management system at Paderborn University and after approval by the Presidential Board of Paderborn University on September 6, 2023

Paderborn, on April 24, 2024,

The President
of the Paderborn University

Professor Dr. Birgitt Riegraf

READING AID

Appendix 1: Procedure for determining a protection requirement

The following questions from the BSI baseline protection[3] can be used to determine the protection requirements of information and any affected persons. These have been supplemented by aspects of the standard data protection model of the independent federal and state data protection authorities.

Damage scenario "Violation of laws/regulations/contracts"

Such breaches can result from the loss of confidentiality as well as integrity and availability. The severity of the damage often depends on the legal consequences for the UPB.

Examples of relevant laws are (in Germany): Basic Law (GG), Civil Code (BGB), Criminal Code (StGB), Federal Data Protection Act (BDSG) and data protection laws of the federal states (e.g. DSG NRW), EU General Data Protection Regulation (DS-GVO), Social Security Code (SGB), Commercial Code (HGB), Personnel Representation Act (PersVH), Copyright Act (UrhG), Patent Act (PatG), Telemedia Act (TMG), Telecommunications Act (TKG), Corporate Control and Transparency Act (KonTraG).

Examples of relevant regulations are Administrative regulations, ordinances and service regulations.

Examples of contracts are Service contracts in the field of data processing, contracts for the protection of trade secrets, purchase contracts, license agreements, employment contracts, loan agreements.

Questions:

Loss of confidentiality

- Do legal requirements require the confidentiality of information?

[3] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, retrieved on 28.06.2022

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

- Is criminal prosecution or recourse claims to be expected if information is published?
- Are contracts that include the confidentiality of certain information to be observed?

Loss of integrity

- Do legal requirements demand the integrity of the information?
- To what extent does a loss of integrity violate laws or regulations?

Loss of availability

- Do laws stipulate the permanent availability of certain information? Are there contractual obligations for certain deadlines to be met?

Damage scenario "Impairment of the right to informational self-determination"

In particular, personal data is repeatedly generated in administrative processes. Examples of the impairment of the right to informational self-determination are in particular

- Unlawful processing of personal data without a legal basis,
- Unauthorized access during data processing or unauthorized disclosure of personal data,
- Unauthorized disclosure of personal data
- use of personal data for a purpose other than that permitted at the time of collection and
- Falsification of personal data

The following questions can be used to assess possible consequences and damage:

Questions:

Loss of confidentiality

- What damage can be caused to the data subject if their personal data is not treated confidentially?
- Is personal data processed for unauthorized purposes?
- Is it possible in the course of permissible processing of personal data to draw conclusions from this data, e.g. about a person's state of health or economic situation?
- What damage can be caused by the misuse of stored personal data?
- Is there no legal or contractually agreed confidentiality obligation for the persons involved in data processing?

Loss of integrity

- What damage would be caused to the data subject if their personal data were unintentionally falsified or intentionally manipulated?
- When would the loss of integrity of personal data become apparent at the earliest?
- What damage would be caused to the data subject if their personal data is incorrect or inaccurate?
- Can the falsified personal data trigger discrimination?

Loss of availability

- Can personal data be lost or falsified in such a way that the person concerned is impaired in his or her social position or even has to fear personal or economic disadvantages?

Loss of non-linking:

- What damage can occur if personal data is mixed with other data and the concatenation of data is misused or becomes known to unauthorized persons?
- Is personal data processed for unauthorized purposes?

READINGAID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

- Are the purposes not defined?
- Are the purposes not clear?
- Aren't the purposes legitimate?

Loss of transparency

- Is there a lack of necessary information obligations pursuant to Art. 13 and 14 GDPR?
- Are processing procedures for personal data not documented?
- Is there a lack of consent management?
- Is there information on the processing of personal data for the data subject?
- Is personal data processed in a manner that is difficult to understand or with information that is difficult to access?
- Is the monitoring of processing not appropriate?
- Has an accountability obligation towards the data subjects and/or the supervisory authority not been fulfilled?

Loss of the ability to intervene

- Is there a lack of options/processes for rectification, erasure, restriction, data portability of personal data?
- Is there a lack of processes that do not allow information to be provided?
- Is there a lack of data protection-friendly default settings?
- Is it not possible to intervene in automated decision-making processes?

Damage scenario "Impairment of task fulfillment"

The loss of availability or integrity of information or personal data in particular can significantly impair the performance of an institution's tasks. The severity of the damage depends on the duration of the impairment and the extent to which the services offered are restricted.

Examples of this are

- missed deadlines due to delayed processing of administrative procedures and
- Delayed delivery due to delayed processing of orders

Questions:

Loss of confidentiality

- Is there information whose confidentiality is the basis for the fulfillment of tasks (e.g. research results or administrative data)?

Loss of integrity

- Can changes to information restrict the fulfillment of tasks in such a way that the institution becomes incapable of acting?
- Does significant damage occur if the tasks are performed despite falsified information? When are unauthorized changes detected at the earliest?
- What are the consequences if information is wrongly attributed to a person who did not actually generate this information?

Loss of availability

- Is there any information for which a restriction of availability would have a serious impact on the institution or its business processes?
- Is it important for the institution that access to necessary information is guaranteed at all times?

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Damage scenario "Negative internal or external impact"

The loss of one of the fundamental values of confidentiality, integrity or availability can have various negative internal or external effects, for example:

- Loss of reputation of the UPB,
- Loss of trust in another institution,
- Demoralization of employees,
- Impairment of economic relations between cooperating institutions,
- lost confidence in the quality of UPB's work and
- Loss of competitiveness.

The amount of the damage depends on the severity of the loss of trust or the degree of dissemination of the internal or external impact. The causes of such damage can be manifold:

- incorrect publications due to manipulated information,
- Non-compliance with confidentiality agreements,
- Blaming the wrong people,
- Preventing a department from fulfilling its tasks due to errors in other areas,
- Leaking confidential information to the press.
- Disclosure of personal data without a legal basis, for example to the police on the basis of a simple request

Questions:

Loss of confidentiality

- What are the consequences for the UPB of the unauthorized publication of sensitive information?
- Can the loss of confidentiality lead to a weakening of the competitive position?
- Does publication cast doubt on the trustworthiness of the UPB?
- Can publications lead to political or social uncertainty?
- Could employees lose trust in the UPB as a result of the unauthorized publication?

Loss of integrity

- What damage may result from the processing, dissemination or transmission of incorrect or incomplete information and/or personal data?
- Will the falsification become public knowledge?
- Does the publication of falsified information and personal data result in a loss of reputation?
- Can the publication of falsified information and personal data lead to political or social uncertainty?

Loss of availability

- Does the unavailability of information and personal data prevent the achievement of business objectives?
- When will the unavailability of information and personal data be noticed externally?

Damage scenario "Financial impact"

Direct or indirect financial losses may result from the loss of confidentiality of sensitive information and personal data, the alteration of information and personal data or the failure of applications. Examples of this are

PREPRINT AD

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

- unauthorized disclosure of research and development results,
- Manipulation of financially relevant information and
- unauthorized access to marketing strategy papers or sales figures

Questions:

Loss of confidentiality

- Can the publication of confidential information and personal data result in recourse claims?
- Is research data of considerable value stored? What happens if it is copied and passed on without permission?
- Can premature publication of sensitive information cause financial damage?

Loss of integrity

- Can financially relevant information be altered through data manipulation in such a way as to cause financial damage?
- Can the publication of false information lead to recourse claims?
- Can falsified order data result in financial losses?
- Can falsified information lead to wrong business decisions?

Loss of availability

- Can the non-availability of information lead to a lack of solvency or to contractual penalties?

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Appendix 2: Classes of information and their usual protection requirements

Introduction

Performing a complete protection requirements assessment for information is time-consuming. This appendix therefore defines classes of information that frequently occur in everyday work at Paderborn University (UPB). Each class is accompanied by the usual protection requirements for confidentiality, availability and integrity of information in the class. In this way, an appropriate protection requirement can be derived for a large amount of information without having to carry out a protection requirement assessment as a case-by-case examination. The following classification therefore corresponds to a "quick test" - in case of doubt, the classification does NOT replace a case-by-case assessment. In some places, the protection requirements differ with regard to the categories of confidentiality, availability and integrity. In this case, the higher protection requirement must generally be assumed in order to define appropriate security measures.

If personal data is the subject of information, the other data protection requirements must also be observed, namely data minimization (data is only processed to the extent necessary), non-linking (data that is processed for different purposes must not be merged), transparency (recognizability of who processes data, for what purpose, through which systems and in what way) and intervenability (ensuring the rights of data subjects (e.g. information in accordance with Art. 15 GDPR and, if necessary, implementation of necessary measures)).

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Administrative data

Information class	Typical protection requirements for confidentiality	Typical protection requirements for availability	Typical protection requirements for integrity
Employees' business contact details, e.g. telephone number or e-mail address, address	Normal	Normal	Normal
Private contact details of employees, e.g. telephone number, e-mail addresses	Normal to high	Normal to high	Normal to high
Non-personal data from publicly accessible sources	Normal	Normal	Normal
Regulations of the faculties and institutions such as circulation	Normal	Normal	Normal
Contracts with partners of the university that do not require confidentiality	Normal to high	Normal to high	Normal to high
Offers	Normal to high	Normal to high	Normal to high
Order confirmations	Normal	Normal to high	Normal to high
Credit documents	High	High	High
Business letters	Normal to high	Normal to high	Normal to high
Insurance policies	Normal	High	High
Accounting documents	High	High	High
Bank documents	High	High	High
Incoming invoices	Normal to high	Normal to high	Normal to high
Goods receipt and outgoing payment ledgers	High	High	High
Payment order	High	High	High
Reimbursement of travel expenses	Normal to high	Normal	Normal to high
Infection Protection Act- Health certificate and last Documentation of the instruction	Normal	Normal	Normal
Youth employment protection documents	Normal	Normal	Normal
Household data	High	High	High

READ

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Personnel data

File class	Typical confidentiality protection requirements	Typical protection requirements for availability	Typical protection requirements for integrity
Personnel master data	High	High	High
Date of birth	High	High	High
Salary lists	High	High	High
Gross payrolls	High	High	High
Temporary employment - business documents of the lender	High	High	High
Time sheets	Normal	High	High
Wage documents (social insurance)	High	High	High
Maternity protection documents	High	High	High
Supply file data	High	High	High
Documents on recreational leave	Normal	Normal	Normal
Time sheets with flexible working hours	Normal	High	High

READING AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Student data

File class	Typical confidentiality protection requirements	Typical protection requirements for availability	Typical protection requirements for integrity
Student master data	High	High	High
E-mail address at the university	Normal	Normal	Normal
Certificates	High	High	High
Attendance lists	High	High	High
Assignment of matriculation number to name	High	High	High
Corrected exams	High	High	High
Exercise sheet	Normal	Normal	Normal
Term papers/seminar papers	Normal	Normal	Normal
Communication with students	Normal	Normal	Normal
Final theses	Normal	High	High
Applications for theses	Normal	Normal	Normal
Expert opinions for individual theses	High	Normal	High
Grades for individual courses	Normal to high	Normal	High
Grades that provide an overview of students' overall performance	High	Normal	High

Scientific data

File class	Typical confidentiality protection requirements	Typical protection requirements for availability	Typical protection requirements for integrity
Scientific data (e.g. test results, measurement series) that have not yet been published	Normal to high	Normal to high	Normal to high
Scientific data that require special protection due to contractual agreements (e.g. from collaborations).	High	High	High

READ AID

This English version is a translated reading aid.
In the event of difficulties of interpretation, the German version shall prevail.

Health data

File class	Typical confidentiality protection requirements	Typical protection requirements for availability	Typical protection requirements for integrity
Documents on benefits, military welfare, medical treatment, support, illnesses	High	High	High
Occupational accident insurance injury procedures	High	High	High
Further health data	High to very high	High to very high	High to very high

Occupational safety

File class	Typical confidentiality protection requirements	Typical protection requirements for availability	Typical protection requirements for integrity
Chemicals (test plans, inspections carried out, instructions, etc.)	Normal	High	Normal
Hazardous substances	Normal	Normal	Normal
File on occupational medical check-ups in the field of hazardous substances	High to very high	High to very high	High to very high
Psychological hazards in the workplace	Normal	Normal	Normal

READ AID

HERAUSGEBER
PRÄSIDIUM DER UNIVERSITÄT PADERBORN
WARBURGER STR. 100
33098 PADERBORN

HTTP://WWW.UNI-PADERBORN.DE

ISSN 2199-2819