|  |  |
| --- | --- |
| **Verzeichnis von Verarbeitungstätigkeiten**  **Verantwortlicher**  **gem. Artikel 30 Abs. 1 DSGVO** | Vorblatt |
| **Angaben zum Verantwortlichen**  Name und Kontaktdatennatürliche Person/juristische Person/Behörde/Einrichtung etc.  Name Universität Potsdam  Straße Am Neuen Palais 10  Postleitzahl 14469  Ort Potsdam  Telefon 0331-977-0  E-Mail-Adresse buero.praesident@uni-potsdam.de  Internet-Adresse www.uni-potsdam.de | |
| **Angaben zum ggf. gemeinsam mit diesem Verantwortlichen[[1]](#footnote-1)**  Name  Straße  Postleitzahl  Ort  Telefon  E-Mail-Adresse | |
| **Angaben zum Vertreter des Verantwortlichen**  Name und Kontaktdatennatürliche Person/juristische Person/Behörde/Einrichtung etc.  Name Prof. Oliver Günther, Ph.D., Präsident  Straße Am Neuen Palais 10  Postleitzahl 14469  Ort Potsdam  Telefon 0331-977-0  E-Mail-Adresse buero.praesident@uni-potsdam.de | |
| **Angaben zur Person des Datenschutzbeauftragten** \*  \* sofern gem. Artikel 37 DS-GVO benannt  Name Dr. Marek Kneis  Straße Am Neuen Palais 10  Postleitzahl 14469  Ort Potsdam  Telefon 0331-977-124409  E-Mail-Adresse datenschutz@uni-potsdam.de | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verarbeitungstätigkeit: Benennung: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | lfd. Nr.: \_\_\_\_\_ | |
| Datum der Einführung: | | | | Datum der letzten Änderung: | | | | |
| Verantwortliche Stelle in der Universität Potsdam einschließlich des operativ verantwortlichen Ansprechpartners für die Datenverarbeitung  Adresse  Telefon  E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a) | |  | | | | | | |
| Zwecke der Verarbeitung[[2]](#footnote-2) (Art. 30 Abs. 1 S. 2 lit b) | |  | | | | | | |
| Beschreibung des Verfahrens der Datenverarbeitung[[3]](#footnote-3) | |  | | | | | | |
| Liste der verwendeten Geräte einschließlich Schnittstellen (z.B. WLAN und USB), Peripherie (z.B. Drucker) und Standort/Benutzer. Sind umfangreichere Angaben hierzu erforderlich, bitte ein separates Blatt anlegen[[4]](#footnote-4). | | Gerätenname | Inventarnr. | | Benutzer[[5]](#footnote-5) | Schnittstellen[[6]](#footnote-6) | | Peripherie[[7]](#footnote-7) |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
|  |  | |  |  | |  |
| Verwendete Software | |  | | | | | | |
| Beschreibung der  Kategorien betroffener  Personen[[8]](#footnote-8)  (Art. 30 Abs. 1 S. 2 lit. c) | |  | | | | | | |
| Beschreibung der Kategorien[[9]](#footnote-9) von personenbezogenen Daten, falls erforderlich aufgegliedert nach den Kategorien der betroffenen Personen. (Art. 30 Abs. 1 S. 2 lit. c) | | Besondere Kategorien personenbezogener Daten (Art. 9)[[10]](#footnote-10): | | | | | | |
| Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offen gelegt worden sind oder noch werden  (Art. 30 Abs. 1 S. 2 lit. d) | intern (Zugriffsberechtigte)  Abteilung/ Funktion | | | | | | | |
| extern (Empfängerkategorie)[[11]](#footnote-11) | | | | | | | |
| Empfänger im Drittland[[12]](#footnote-12) oder internationale Organisation[[13]](#footnote-13) (Kategorie) | | | | | | | |
| Ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine inter-nationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)  Nennung der konkreten Datenempfänger | Datenübermittlung findet nicht statt und ist auch nicht geplant  Datenübermittlung findet wie folgt statt:  Empfänger im Drittland oder internationale Organisation (Name) | | | | | | | |
| Wie wird sichergestellt, dass das Schutzniveau der DSGVO im Drittland nicht untergraben wird? | Angemessenheitsbeschluss der Kommission[[14]](#footnote-14)  Geeignete Garantien nach Art. 46:    Verbindliche interne Datenschutzvorschriften des Empfängers (Art. 47)  Ausdrückliche Einwilligung der betroffenen Personen im Einzelfall (Art. 49 Abs. 1 lit. a)[[15]](#footnote-15) | | | | | | | |
| Fristen für die Löschung der verschiedenen Datenkategorien[[16]](#footnote-16) |  | | | | | | | |
| Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO | Werden Systeme/Infrastruktur des Zentrums für Informationstechnologie und Medienmanagement (ZIM) genutzt?  a) Ja, und zwar (bitte nennen Sie das / die für das Verfahren genutzte/n System/e[[17]](#footnote-17)  b) Werden dazu noch weitere Systeme genutzt, die nicht vom ZIM administriert werden?  Nein  Ja, es werden noch weitere Systeme genutzt (weiter unter c)  c) Soweit Systeme genutzt werden, die nicht vom ZIM administriert werden: Welche Art von Systemen wird genutzt?  Bitte beschreiben Sie die Sicherheitsmaßnahmen für die nachfolgenden Anforderungen an die Systeme.  Sicherheitskonzept ist als Anhang beigefügt  Alternativ: Beschreibung der Sicherheitsmaßnahmen mithilfe der nachfolgenden Dokumentation über die getroffenen technischen und organisatorischen Maßnahmen | | | | | | | |

# Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO

für

[Name des Dienstes][[18]](#footnote-18)

## 1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

### 1.1. Zutrittskontrolle[[19]](#footnote-19)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Alarmanlage | Zutritt für Besucher/innen und externe Dienstleister zu den Serverräumen ist nur in Begleitung eines/r berechtigten Mitarbeiters/in  der Einrichtung /  des ZIM möglich |
| Chipkarten / Transpondersysteme | der Zutritt zu Räumen mit Servern ist ausschließlich mit personalisierten Transpondern oder Sicherheitsschlüsseln möglich, welche nur für berechtige Mitarbeiter/innen  der Einrichtung /  des ZIM freigeschaltet oder ausgegeben werden |
| Manuelles Schließsystem | für die ausgegebenen Schlüssel wird ein Schlüsselverzeichnis über Ausgabe, Rücknahme und Verlust von Schlüsseln geführt. |
| Sicherheitsschlösser | Reinigungspersonal hat keinen Zugang zu den Serverräumen |
| Schließsystem mit Codesperre | Arbeitsräume mit Arbeitsplatzrechnern die Zugriff auf die Server-Infrastruktur haben, müssen beim Verlassen verschlossen werden. |
| Absicherung der Gebäudeschächte | Pförtner |
| Türen mit Knauf Außenseite | Wachdienst (Securitas) |
| Videoüberwachung |  |

**Weitere Maßnahmen:**

### 1.2. Zugangskontrolle[[20]](#footnote-20)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| IT-Systeme werden nach Anwendungszweck in verschiedenen Netzwerksegmenten betrieben | Passwörter für den Zugang zur virtuellen Maschine liegen beim Ansprechpartner, der bei der Einrichtung einer solchen Maschine benannt werden muss |
| Login mit Benutzername + Passwort | Externe Dienstleister erhalten Zugriff auf interne IT-Systeme zum Zweck der Wartung von Infrastrukturkomponenten nur nach vorheriger Freischaltung durch den IT-Support. Der Zugriff erfolgt unter Beobachtung bzw. Anwesenheit eines/r Mitarbeiters/in des Supports oder der Technik. |
| Anti-Viren-Software Server | Das gesamte Netzwerk und die Netzwerksegmente werden durch den Einsatz von Firewalls voneinander getrennt, Zugang zu den jeweiligen Netzwerksegmenten erhalten nur die jeweils zugangsberechtigten Personenkreise. |
| Anti-Virus-Software Clients | Fernzugriffe (durch  Berechtigte der Einrichtung /  ZIM-Mitarbeiter/innen) während der Arbeit im Home-Office oder auf Dienstreisen erfolgen über einen gesicherten VPN-Tunnel mit personalisiertem Nutzerzertifikat und Passwort. |
| Anti-Virus-Software mobile Geräte | Alle Mitarbeiter/innen sind zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung (DSGVO) - Datengeheimnis/Vertraulichkeit (Art. 5, 24, 32 DSGVO) - verpflichtet. |
| Firewall | Spätestens nach dem Austritt von Mitarbeiter/innen erfolgt der Entzug von Zugriffsrechten für IT-Systeme, insbesondere für IT-Systeme, die aus dem Internet zu erreichen sind. |
| Intrusion Detection Systeme | Mitarbeiter/innen erhalten Zugriffsberechtigungen gemäß ihrem Aufgabenbereich. Eine Erweiterung der Zugangsberechtigung muss durch Vorgesetzte über das interne Ticketsystem beantragt werden, um eine entsprechende Protokollierung sicherzustellen. |
| Einsatz VPN bei Remote-Zugriffen | Richtlinie „Sicheres Passwort“ |
| Verschlüsselung von Datenträgern |  |
| Gehäuseverriegelung |  |
| BIOS Schutz |  |
| Sperre externe Schnittstellen (USB) |  |
| Verschlüsselung von Notebooks / Tablets |  |
| Die Eingabe von Passwörtern erfolgt immer über eine verschlüsselte Verbindung |  |
| Netzwerkverbindungen zu Außenstellen dürfen nur über verschlüsselte Verbindungen hergestellt werden, die in den jeweiligen Gebäuden beginnen bzw. enden |  |
| Authentifizierung / Login mit biometrischen Merkmalen (z.B. Fingerabdruck /Iris-Scan/Face-ID) |  |

**Weitere Maßnahmen:**

### 1.3. Zugriffskontrolle[[21]](#footnote-21)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Verwendung von Aktenschreddern entsprechend der erforderlichen Sicherheitsstufe nach DIN 66399. | Einsatz von Berechtigungskonzepten |
| Externer Aktenvernichter (DIN 32757) | Minimale Anzahl von Administrator/innen |
| Physische Löschung von Datenträgern | Verwaltung der Benutzerrechte durch Administrator/innen |
| Protokollierung von Zugriffen aus Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten | Mitarbeiter/innen erhalten Zugriffsberechtigungen gemäß ihrem Aufgabenbereich. |
| mittels Virtualisierung wird ein direkter Zugriff durch die Anwender auf die Hardware-Ebene verhindert |  |

**Weitere Maßnahmen:**

### 1.4. Trennungskontrolle[[22]](#footnote-22)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Trennung von Produktiv- und Testumgebung | Steuerung über Berechtigungskonzept |
| Physikalische Trennung (Systeme / Datenbanken / Datenträger) | Festlegung von Datenbankrechten |
| getrennte virtuelle Systeme mit einer eigenständigen Datenbank für jeden Datenbestand | Datensätze sind mit Zweckattributen versehen |
| getrennte Datenbanken auf einem System mit getrennten Zugriffsrechten |  |

**Weitere Maßnahmen:**

### 1.5. Pseudonymisierung[[23]](#footnote-23)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Trennung der Zuordnungsdaten (Klarnamenliste) von den restlichen Daten und Aufbewahrung in getrennten und abgesicherten Systemen | ☐ Beschränkung des Zugriffs auf die Klarnamenliste auf folgende Personen[[24]](#footnote-24): |
| ☐ Verschlüsselung / Passwortschutz der elektronisch aufbewahrten Klarnamenliste | ☐ Aufbewahrung der Klarnamenliste in Papierform in einem Stahlschrank/Safe |
|  | Interne Anweisung, personenbezogenen Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Löschfrist zu anonymisieren |

**Weitere Maßnahmen:**

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 2.1. Weitergabekontrolle[[25]](#footnote-25)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Einsatz von VPN | Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen |
| Protokollierung der Zugriffe und Abrufe | Weitergabe in anonymisierter oder pseudonymisierter Form |
| Bereitstellung über verschlüsselte Verbindungen wie sftp, https | Verwendung verschlossener Transportbehälter |
| Nutzung von Signaturverfahren | Persönliche Übergabe mit Protokoll |
| Passwortschutz/Verschlüsselung einzelner Dokumente mit getrennter Kennwortübermittlung |  |
| Verschlüsselung von zum Transport eingesetzten Datenträgern |  |

**Weitere Maßnahmen:**

### 2.2. Eingabekontrolle[[26]](#footnote-26)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Technische Protokollierung der Eingabe, Änderung und Löschung von Daten | Übersicht mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können |
| Manuelle oder automatisierte Kontrolle der Protokolle | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |
| Protokollierung von Administratoraktivitäten | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |
| Erfassung gescheiterter Zugriffsversuche | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden |
|  | Klare Zuständigkeiten für Löschungen |

**Weitere Maßnahmen:**

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

### Verfügbarkeitskontrolle[[27]](#footnote-27)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Feuer- und Rauchmeldeanlagen | Backup & Recovery Konzept |
| Feuerlöscher Serverraum | Kontrolle des Sicherungsvorgangs |
| Serverraumüberwachung Temperatur und Feuchtigkeit | Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |
| Serverraum klimatisiert | Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums |
| Unterbrechungsfreie Stromversorgung | Existenz eines Notfallplans |
| Schutzsteckdosen Serverraum | Getrennte Partitionen für Betriebssysteme und Daten |
| RAID System / Festplattenspiegelung |  |
| Alarmmeldung bei unberechtigten Zutritt zu Serverraum |  |

**Weitere Maßnahmen:**

## 4. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### 4.1. Datenschutz-Management[[28]](#footnote-28)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter/innen nach Bedarf / Berechtigung | Interner Datenschutzbeauftragte/r |
|  | Mitarbeiter/innen geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet |
|  | Regelmäßige Sensibilisierung der Mitarbeiter/innen der  eigenen Einrichtung /  des ZIM |
|  | Die Einrichtung  das ZIM kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach |
|  | Formalisierter Prozess zur Bearbeitung von Auskunftsfragen seitens Betroffener ist vorhanden |

**Weitere Maßnahmen:**

### 4.2. Incident Response Management[[29]](#footnote-29)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Einsatz von Firewall und regelmäßige Aktualisierung | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen |
| Einsatz von Spamfilter und regelmäßige Aktualisierung | Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen |
| Einsatz von Virenscanner und regelmäßige Aktualisierung | Einbindung von  DSB und  ISB in Sicherheitsvorfälle und Datenpannen |
| Intrusion Detection System (IDS) | Dokumentation von Sicherheitsvorfällen und Datenpannen im Ticketsystem |
| Intrusion Prevention System (IPS) | Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen |

**Weitere Maßnahmen:**

### 4.3. Datenschutzfreundliche Voreinstellungen

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Anwendungen / Apps sind so eingestellt, dass nicht mehr personenbezogene Daten erhoben werden, als für den jeweiligen Zweck erforderlich sind |  |
| Einfache Ausübung des Widerrufsrechts des/r Betroffenen durch technische Maßnahmen |  |

**Weitere Maßnahmen:**

### 4.4. Auftragskontrolle[[30]](#footnote-30)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  | Vorherige Prüfung der von Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation |
|  | Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) |
|  | Abschluss der notwendigen Vereinbarungen zur Auftragsdatenverarbeitung |
|  | Schriftliche Weisungen an den Auftragnehmer |
|  | Verpflichtung der Mitarbeiter/innen des Auftragnehmers auf Datengeheimnis |

**Weitere Maßnahmen:**

Es liegen schriftlich vor:

|  |
| --- |
| interne Verhaltensregeln  Risikoanalyse  allgemeine Datensicherheitsbeschreibung  umfassendes Datensicherheitskonzept  Wiederanlaufkonzept  Zertifikat:  Sonstiges: |
| Ist eine Beeinträchtigung der Sicherheit des Verfahrens bei Gewährung der Einsicht in die Dokumentation der technischen und organisatorischen Maßnahmen zu befürchten?  Ja  Nein  Bejahendenfalls ist die Dokumentation der technischen und organisatorischen Maßnahmen von der Einsichtnahme durch Betroffene gemäß § 4 Abs. 3 BbgDSG ausgenommen. |

……………………………… …………………… ...........................................................

Verantwortlicher Datum Unterschrift

1. Bei mehreren gemeinsam Verantwortlichen bitte zusätzliche Zeilen einfügen, damit alle Verantwortlichen aufgenommen werden können. Verantwortlicher für die Datenverarbeitung ist, wer allein oder gemeinsam mit anderen Stellen über Zweck (Grund und Ziel) sowie Mittel (Technik und Methoden) der Datenverarbeitung entscheidet. [↑](#footnote-ref-1)
2. Beweggrund und Ziel der Verarbeitung. [↑](#footnote-ref-2)
3. Wie werden die Daten erhoben, wo werden sie gespeichert, welche Verarbeitungsschritte sind vorgesehen (Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, die Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung). [↑](#footnote-ref-3)
4. Bitte ggf. auch angeben, ob die Daten auf einer nicht von vornherein beschränkten/bekannten Anzahl von Geräten verarbeitet werden sollen. [↑](#footnote-ref-4)
5. Funktionsbezeichnung genügt. [↑](#footnote-ref-5)
6. Muss für Geräte der ZUV nicht ausgefüllt werden. [↑](#footnote-ref-6)
7. Muss für Geräte der ZUV nicht ausgefüllt werden. [↑](#footnote-ref-7)
8. Z.B. Studierende, Beschäftigte. [↑](#footnote-ref-8)
9. Z.B. Personaldaten, Adressdaten, E-Mail-Adresse. [↑](#footnote-ref-9)
10. „Rassische“ und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. [↑](#footnote-ref-10)
11. Z.B. Finanzamt, Krankenkassen, Berufsgenossenschaften, Deutsche Rentenversicherung, Kunden, Spediteure, Rechtsanwälte, Steuerberater. [↑](#footnote-ref-11)
12. Drittländer sind Länder, die nicht Mitglied der EU/des EWR sind. [↑](#footnote-ref-12)
13. Völkerrechtliche Organisationen und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehreren Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde. [↑](#footnote-ref-13)
14. Alle existierenden Angemessenheitsbeschlüsse können eingesehen werden unter: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. [↑](#footnote-ref-14)
15. Hinweis: Eine Datenübermittlung in unsicherere Drittländer auf der Grundlage einer Einwilligung der betroffenen Person darf nicht stattfinden, soweit sie im Rahmen von Tätigkeiten im Zusammenhang mit der Ausübung hoheitlicher Befugnisse der UP erfolgt. [↑](#footnote-ref-15)
16. Bitte ggf. gesetzliche Grundlagen für die Dauer der Datenspeicherung mit angeben. [↑](#footnote-ref-16)
17. Beispiele sind: Box.UP, Media.UP, Mail.UP, LDAP, Filebox, Moodle.UP, Server Hosting, Git.UP, PM.UP, u.a. [↑](#footnote-ref-17)
18. Bei Verwendung mehrerer lokaler Dienste, für die unterschiedliche technische und organisatorische Maßnahmen gelten, sollte diese Anlage für jeden Dienst separat ausgefüllt werden. [↑](#footnote-ref-18)
19. Maßnahmen der **Zutrittskontrolle** dienen dazu, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. [↑](#footnote-ref-19)
20. Durch die Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme/Datenträger von Unbefugten genutzt/gelesen werden können. [↑](#footnote-ref-20)
21. Mit Maßnahmen der Zugriffskontrolle soll sichergestellt werden, dass jede/r Mitarbeiter/in im Rahmen seiner/ihrer Tätigkeit nur auf solche Daten zugreifen kann, die er/sie zur Erfüllung seiner Aufgaben tatsächlich benötigt (Need-to-know-Prinzip). [↑](#footnote-ref-21)
22. Maßnahmen der Trennungskontrolle sollen sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (keine gleichzeitige Arbeit an Daten aus unterschiedlichen Beständen). [↑](#footnote-ref-22)
23. Die Pseudonymisierung ist eine Maßnahme der Erhöhung der Sicherheit der Datenverarbeitung. Sie erfolgt indem die Klarnamen in Datensätzen durch einen Code/eine Kennung ersetzt werden. Eine Klarnamenliste, mit der eine Zuordnung der Daten zu bestimmten Personen möglich bleibt, wird erstellt und sicher mit beschränkten Zugriffsmöglichkeiten verwahrt. [↑](#footnote-ref-23)
24. Angabe von Funktionsbezeichnungen sind ausreichend. [↑](#footnote-ref-24)
25. Die Weitergabekontrolle soll die Integrität und Vertraulichkeit der Daten im Zusammenhang mit ihrer Weitergabe gewährleisten. [↑](#footnote-ref-25)
26. Mit Maßnahmen der Eingabekontrolle soll die Integrität der Daten sichergestellt werden. Dazu muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. [↑](#footnote-ref-26)
27. Maßnahmen der Verfügbarkeitskontrolle dienen dem Schutz der Daten vor Verlust und Zerstörung sowie vorübergehenden Verfügbarkeitsbeschränkungen. [↑](#footnote-ref-27)
28. Das Datenschutz-Management ist eine Methode, um die gesetzlichen und innerorganisatorischen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren. [↑](#footnote-ref-28)
29. Das Incident Response Management umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Betriebsstörungen in IT-Bereichen sowie entsprechende vorbereitende Maßnahmen und Prozesse. [↑](#footnote-ref-29)
30. Mit Maßnahmen der Auftragskontrolle soll gewährleistet werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. [↑](#footnote-ref-30)