Verzeichnis von Verarbeitungstätigkeiten

(gem. Art. 30 Abs. 1 DSGVO) (Formular-Version 1.0)

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Lfd. Nummer |  |
| Benennung |  | | |

# Vorblatt

## Angaben zum Verantwortlichen

|  |  |
| --- | --- |
| Name | <Hochschule> |
|  | Die <Hochschule> ist eine vom Land getragene, rechtsfähige  Körperschaft des Öffentlichen Rechts. Sie wird vertreten durch die  Präsidentin / den Präsidenten. |
| Adresse |  |
| Telefon |  |
| E-Mail |  |
| Web | www… |

## Kontaktdaten der/des Datenschutzbeauftragten

|  |  |
| --- | --- |
| Adresse | <Hochschule>  Datenschutzbeauftragte/r  … |
| Telefon |  |
| E-Mail | datenschutz@... |

Verzeichnis von Verarbeitungstätigkeiten

(gem. Art. 30 Abs. 1 DSGVO)

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Lfd. Nummer |  |
| Benennung |  | | |

# Hochschulinterne Kontaktdaten

## Innerorganisatorische Ansprechpartner

|  |  |
| --- | --- |
| Verantwortliche Fachabteilung |  |
| Fachlicher Ansprechpartner |  |
| Telefon |  |
| E-Mail |  |
| Technischer Ansprechpartner |  |
| Telefon |  |
| E-Mail |  |

## Datenschutzbeauftragter

|  |  |
| --- | --- |
| Name |  |
| Telefon |  |
| E-Mail | datenschutz@... |

# Änderungshistorie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | geändert am | Kapitel | Änderungsgrund | Bearbeitung |
| *1.0* | *3.5.2019* |  | *finalisiert* | *Projekt DSMS* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Verzeichnis von Verarbeitungstätigkeiten

(gem. Art. 30 Abs. 1 DSGVO)

# Angaben zur Verarbeitungstätigkeit

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Lfd. Nummer | Klicken zur Eingabe. |
| Benennung | Klicken um Benennung einzugeben. | | |
| Datum der Einführung |  | | |
| Stand |  | | |
|  | Neue Verarbeitungstätigkeit | Änderung einer bestehenden Verarbeitungstätigkeit | |

## Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen

(Art. 26, Art. 30 Abs. 1 S. 2 lit. a DSGVO)

|  |  |
| --- | --- |
| Name |  |
| Adresse |  |
| Telefon |  |
| E-Mail |  |

## Zweck(e) und Rechtsgrundlage(n) der Verarbeitung

(Art. 30 Abs. 1 S. 2 lit. b sowie Art. 5 Abs. 1 lit. a i.V.m. Art.6 Abs.1 DSGVO)

|  |  |
| --- | --- |
| kurze Beschreibung der Verarbeitung  (was wird gemacht?) |  |

|  |  |  |
| --- | --- | --- |
| Zweck(e) | Rechtsgrundlage | **Erläuterung / Konkretisierung der Rechtsgrundlage** |
|  | Erforderlichkeit für eine Aufgabe, die im öffent­lichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt  (Art. 6 Abs. 1 lit. e) | Nennung der konkretisierten Rechtsgrundlage (bspw. HG NRW, Ordnung der Hochschule, …) andernfalls Beschreibung der übertragenen Aufgabe inkl. Begründung der Erforderlichkeit: |
|  | Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c) | Nennung der rechtlichen Verpflichtung: |
|  | Einwilligung in die Verarbeitung  (Art. 6 Abs. 1 lit. a) | Einwilligungserklärung im Anhang  Verweis auf Einwilligungserklärung |
|  | Erforderlichkeit zur Erfüllung eines Vertrags  (Art. 6 Abs. 1 lit. b) | Vertrag im Anhang  Verweis auf Vertrag  Erläuterungen zum Vertrag: |
|  | Erforderlichkeit zur Wahrung der berechtigten Interessen (nicht für Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitungen)  (Art. 6 Abs. 1 lit. f) | Begründung des berechtigten Interesses /  Ergebnis der Prüfung der Verhältnismäßigkeit: |
|  | Erforderlichkeit zum Schutz lebenswichtiger Interessen  (Art. 6 Abs. 1 lit. d) | Welche Interessen werden geschützt? |

## Beschreibung der Kategorien von personenbezogenen Daten

(Art. 30 Abs. 1 S. 2 lit. c)

Hinweis: Die laufende Nummer (Lfd. Nr.) dient dazu bei komplexeren Verarbeitungen den einzelnen Kategorien personenbezogener Daten im Folgenden die Kategorien betroffener Personen (4), Löschfristen () und die Kategorien von Empfängern (6) zuzuordnen.

|  |  |
| --- | --- |
| Lfd. Nr. | Kategorien personenbezogener Daten |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Werden besondere Kategorien personenbezogener Daten (Art. 9) verarbeitet? | | Ja /  Nein |
| Lfd. Nr. | Besondere Kategorien personenbezogener Daten | |
|  |  | |
|  |  | |

## Beschreibung der Kategorien betroffener Personen

(Art. 30 Abs. 1 S. 2 lit. c)

|  |  |
| --- | --- |
| Lfd. Nr. aus | Kategorien betroffener Personen |
|  | Mitglieder der Hochschule  Professoren / Dozenten  Beschäftigte  Studierende    … |
|  | Gäste  Gastdozenten  gastweise an der Hochschule tätige Personen  Kooperationspartner  Ehemalige (Alumni, Emeriti)    … |
|  | Geschäftspartner  Kontaktpersonen an anderen Hochschulen  Kontaktpersonen der Lieferanten  Kontaktpersonen der Auftraggeber    … |
|  | Datenverarbeitende Personen  Systemverwalter (Fachadministrator, Administrator)  externe IT-Betreiber  Bearbeiter der personenbezogenen Daten (Sachbearbeiter, Sekretäre, …)    … |
|  | Weitere  Bewerber auf Studienplätze  Stellenbewerber  Tagungs- / Konferenzteilnehmer  Studienteilnehmer / Probanden  Schüler  Nutzer von Webseiten / öffentlichen Diensten der Hochschule        … |

## Fristen für die Löschung der verschiedenen Datenkategorien

(Art. 30 Abs. 1 S. 2 lit. f)

Anm.: Daten sind dann zu löschen, wenn sie für die Erfüllung des Zwecks nicht mehr erforderlich sind und wenn darüber hinausgehend keine gesetzlichen Aufbewahrungsfristen gelten.

|  |  |  |
| --- | --- | --- |
| Ein Löschkonzept wird in einem eigenen Dokument (Anhang oder Verweis):  Es gelten die folgenden Löschregeln: | | |
|  | Löschregeln für die Datenkategorien (Abschnitt .) | | |
| Lfd. Nr. aus 3 | Startzeitpunkt des Fristlaufs / Auslöser der Frist  (bspw. Erhebung, Semesterende, Exmatrikulation, Vertragsende) | Löschfrist / Zeitraum bis zur Löschung (bspw. 3 Monate, 1 Jahr) | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |

Falls keine Möglichkeit besteht eine konkrete Löschregel anzugeben, sind Kriterien für die Festlegung der Speicherdauer anzugeben.

|  |  |
| --- | --- |
| Lfd. Nr. aus 3 | Kriterien für die Festlegung der Speicherdauer  (bspw. Löschung 6 Monate nach Abschluss der Forschungsarbeit, Löschung nach Beendigung der Rechtsstreitigkeiten) |
|  |  |
|  |  |

## Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden

**(Art. 30 Abs. 1 S. 2 lit. d)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lfd. Nr. aus 3 |  |  |  |  |
|  |  | Intern (Zugriffsberichte) | Abteilung(en) / Funktion |  |
|  |  | Extern | Empfängerkategorie |  |
|  |  | Drittland oder internationale Organisation (Kategorie) | dann weiter mit Pkt. 7 |  |

## ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

(Art. 30 Abs. 1 S. 2 lit. e)

Wenn Daten in irgendeiner Weise außerhalb der EU gelangen könnten (z. B. Nutzung eines Cloud-Services oder die Zusammenarbeit mit Unternehmen / Institutionen im EU-Ausland vorliegen) sollte der Datenschutzbeauftragte frühzeitig darüber informiert werden.

|  |  |  |  |
| --- | --- | --- | --- |
| Eine Datenübermittlung an Drittland oder internationale Organisation | | | |
|  | findet nicht statt und ist auch nicht geplant | | |
|  | findet wie folgt statt: | | |
| Nennung der konkreten Datenempfänger | | | |
|  |  | Drittland |  |
|  |  | internationale Organisation |  |
| Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung handelt. Dokumentation geeigneter Garantien | | | |
|  |  | Anerkannter Drittstaat  Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO) | |
|  |  | EU-Standardvertrag(-sklauseln)  Herstellung eines ausreichenden Datenschutzniveaus durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO | |
|  |  | Aufsichtsbehördlich genehmigter Vertrag  Herstellung eines ausreichenden Datenschutzniveaus durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO | |
|  |  | Binding Corporate Rules (BCR)  Herstellung eines ausreichenden Datenschutzniveaus durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DSGVO | |
|  |  | Herstellung eines ausreichenden Datenschutzniveaus durch ein Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO) | |
|  |  | Herstellung eines ausreichenden Datenschutzniveaus durch folgende sonstige Maßnahmen (Art. 46 Abs. 2 lit. a, Abs. 3 lit. a und b DSGVO): | |
|  |  | Aufgrund folgenden Ausnahmetatbestand des Art. 49 DSGVO: | |

# Weitere Angaben

## Welche Personengruppen haben Zugriff auf welche der erhobenen personenbezogenen Datenkategorien?

(Art.5 Abs.1 lit. b, c DSGVO)

|  |  |  |
| --- | --- | --- |
| Ein Berechtigungskonzept wird in einem eigenen Dokument beschrieben (Anhang oder Verweis):  Es existieren die folgenden Zugriffsberechtigungen: | | |
| Lfd. Nr. aus | Zugriffsberechtigte Personengruppen | Umfang |
|  |  | Lesen  Schreiben  Löschen |
|  |  | Lesen  Schreiben  Löschen |
|  |  | Lesen  Schreiben  Löschen |
|  |  | Lesen  Schreiben  Löschen |
|  |  | Lesen  Schreiben  Löschen |

## Transparenz / Informationspflichten

(Art. 5 Abs. 1 lit. a i.V.m. Art. 12ff)

|  |
| --- |
| Die Betroffenen werden mit einem Informationsblatt über die Datenerhebung informiert  (Anhang oder Verweis): |
| Die Betroffenen werden mit einer Online-Datenschutzerklärung über die Datenerhebung informiert; Verweis auf Datenschutzerklärung:  http://... |
| Die Betroffenen werden wie folgt informiert |

## Auftragsverarbeitung

(Art. 28)

|  |
| --- |
| Eine Auftragsverarbeitung findet nicht statt |
| Der Auftragsverarbeiter bietet hinreichend Garantien (Art. 28 Abs. 1) |
| Ein Vertrag zur Auftragsverarbeitung wurde geschlossen (Anhang oder Verweis): |

### Angaben zum Auftragsverarbeiter

|  |  |
| --- | --- |
| Name |  |
| Adresse |  |
| Telefon |  |
| E-Mail |  |

## Schwellwertanalyse

(Art. 35 Abs. 1)

Eine Schutzbedarfsfeststellung / Schwellwertanalyse wurde zusammen mit der Informationssicherheit durchgeführt und hat die folgende Risikoeinschätzung ergeben:

|  |
| --- |
| Normales Risiko für die Betroffenen |
| Hohes Risiko für die Betroffenen |
| Sehr Hohes Risiko für die Betroffenen |

## Datenschutzfolgenabschätzung

(Art. 35)

|  |
| --- |
| nicht erforderlich |
| wurde durchgeführt |
| mit folgendem Ergebnis |
| hinreichend Maßnahmen zur Bewältigung der Risiken vorhanden |
| zusätzliche Maßnahmen wurden ergriffen |
| keine Maßnahmen zur Eindämmung des Risikos möglich bzw. es werden keine Maßnahmen ergriffen |
| dann |
| Konsultation der Aufsichtsbehörde (Art. 36) wurde mit folgendem Ergebnis durchgeführt: |

# Technische und organisatorische Maßnahmen (TOM)

(Art. 30 Abs. 1 S. 2 lit. g i.V.m. Art. 32 Abs.1 DSGVO)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Die Verarbeitung ist geprüft und zertifiziert (bspw. BSI, ISO 27000) (Anhang oder Verweis)  Es liegt ein umfassendes Datensicherheitskonzept vor (Anhang oder Verweis)  Es liegt eine Beschreibung der für die Verarbeitung getroffenen Maßnahmen vor (Anhang oder Verweis)  Es wurden folgende Maßnahmen getroffen  (Erläutern Sie die zu den vorgegebenen Schutzzielen jeweils getroffenen Maßnahmen) | | | | | | | | | |
| Psudonymisierung gemäß Art. 32 Abs. 1 lit. a) DSGVO | | | | | | | | | |
| Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. | | | | | | | | | |
| Technische Maßnahmen | | | | | | Organisatorische Maßnahmen | | | |
|  | | Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. Verschlüsselt) | | | |  | Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren | | |
| Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | | | | |
| Verschlüsselung gemäß Art. 32 Abs. 1 lit. b) DSGVO | | | | | | | | | |
| Details und Maßnahmen bitte beschreiben: | | | | | | | | | |
| Gewährleistung der Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO | | | | | | | | | |
| **Zutrittskontrolle**  Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitsungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. | | | | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Manuelles Schließsystem | | |  | Schlüsselregelung / Liste |
|  | | |  | | Sicherheitsschlösser | | |  | Empfang / Rezeption / Pförtner |
|  | | |  | | Türen mit Knauf Außenseite | | |  | Besucherbuch / Protokoll der Besucher |
|  | | |  | | Automatisches Zugangskontrollsystem | | |  | Mitarbeiter- / Besucherausweise |
|  | | |  | | - Biometrische Zugangssperren | | |  | Besucher in Begleitung durch Mitarbeiter |
|  | | |  | | - Chipkarten / Transpondersysteme | | |  | Sorgfalt bei Auswahl des Wachpersonals |
|  | | |  | | - Schließsystem mit Codesperre | | |  | Sorgfalt bei Auswahl Reinigungsdienste |
|  | | |  | | Klingelanlage mit Kamera | | |  |  |
|  | | |  | | Videoüberwachung der Eingänge | | |  |  |
|  | | |  | | Alarmanlage | | |  |  |
|  | | |  | | Absicherung der Gebäudeschächte | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Zugangskontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.  Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Authentifizierungsverfahren | | |  | Verwalten von Benutzerberechtigungen |
|  | | |  | | - Login mit Benutzername + Passwort | | |  | Zentrales Zugangsmanagement und Passwortvergabe |
|  | | |  | | - Login mit biometrischen Daten | | |  | Lokale Benutzerverwaltung durch Administrator |
|  | | |  | | - Login mit Chipkarte / Zertifikat | | |  | Richtlinie „Sicheres Passwort“ |
|  | | |  | | - Tokenbasierte Authentifizierung | | |  | Anleitung „Manuelle Desktopsperre“ |
|  | | |  | | Automatische Desktopsperre | | |  | Erstellen von Benutzerprofilen |
|  | | |  | | Schutz der Rechner | | |  | Richtlinie „Löschen / Vernichten“ |
|  | | |  | | - Gehäuseverriegelung | | |  | Richtlinie „Clean desk“ |
|  | | |  | | - Sperre externer Schnittstellen (USB, Bluetooth, …) | | |  | Allg. Richtlinie Datenschutz und / oder Sicherheit |
|  | | |  | | - BIOS Schutz (separates Passwort) | | |  | Mobile Device Policy |
|  | | |  | | Anti-Viren-Software Server | | |  |  |
|  | | |  | | Anti-Virus-Software Clients | | |  |  |
|  | | |  | | Anti-Virus-Software mobile Geräte | | |  |  |
|  | | |  | | Firewall | | |  |  |
|  | | |  | | Einsatz VPN bei Remote-Zugriffen | | |  |  |
|  | | |  | | Schutz mobiler Geräte | | |  |  |
|  | | |  | | Mobile Device Management | | |  |  |
|  | | |  | | Intrusion Detection Systeme | | |  |  |
|  | | |  | | Verschlüsselung | | |  |  |
|  | | |  | | Verschlüsselung von Datenträgern | | |  |  |
|  | | |  | | Verschlüsselung Smartphones | | |  |  |
|  | | |  | | Verschlüsselung von Notebooks / Tablet | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Zugriffskontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Rollenbasierte Berechtigungsvergabe | | |  | Zentrales Berechtigungskonzept |
|  | | |  | | Vergabe und Änderung von Berechtigungen über ein zentrales Identitätsmanagement | | |  | Dezentrales Berechtigungskonzepte |
|  | | |  | | Aktenschredder (mind. Stufe 3, cross cut) | | |  | Verwaltung Benutzerrechte durch Administratoren |
|  | | |  | | Externer Aktenvernichter (DIN 32757) | | |  | Minimale Anzahl an Administratoren |
|  | | |  | | Physische Löschung von Datenträgern | | |  | Datenschutztresor |
|  | | |  | | Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Trennungskontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Trennung von Produktiv- und Testumgebung | | |  | Steuerung über Berechtigungskonzept |
|  | | |  | | Physikalische Trennung (Systeme / Datenbank / Datenträger) | | |  | Festlegung von Datenbankrechten |
|  | | |  | | Mandantenfähigkeit relevanter Anwendungen | | |  | Datensätze sind mit Zweckattributen versehen |
|  | | |  | | Sicherer Schnittstellenbetrieb | | |  | Schnittstellenbeschreibung |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| Gewährleistung der Integrität gemäß Art. 32 Abs. 1 lit. b) DSGVO | | | | | | | | | |
| **Weitergabekontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | E-Mail Verschlüsselung | | |  | Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen |
|  | | |  | | Bereitstellung über verschlüsselte Verbindungen wie sftp, https | | |  | Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen |
|  | | |  | | Nutzung von Signaturverfahren | | |  | Weitergabe in anonymisierter oder pseudonymisierter Form |
|  | | |  | | Einsatz von VPN | | |  | Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen |
|  | | |  | | Protokollierung der Zugriffe und Abrufe | | |  | Persönliche Übergabe mit Protokoll |
|  | | |  | | Sichere Transportbehälter | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| **Eingabekontrolle** | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollieren erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet. | | | | | | |
|  | | | 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) |
|  | | |  | |  | | |  | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis ein Berechtigungskonzepts |
|  | | |  | |  | | |  | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden |
|  | | |  | |  | | |  | Klare Zuständigkeiten für Löschungen |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| Gewährleistung der Verfügbarkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO | | | | | | | | | |
|  | | | Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Feuer- und Rauchmeldeanlagen | | |  | Backup & Recovery-Konzept (ausformuliert) |
|  | | |  | | Feuerlöscher im Serverraum | | |  | Kontrolle des Sicherungsvorgangs |
|  | | |  | | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | | |  | Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |
|  | | |  | | Serverraum klimatisiert | | |  | Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums |
|  | | |  | | Unterbrechungsfreie Stromversorgung (USV) | | |  | Keine sanitären Anschlüsse im oder oberhalb des Serverraums |
|  | | |  | | Schutzsteckdosenleisten in Serverräumen | | |  | Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4) |
|  | | |  | | Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.) | | |  | Getrennte Partitionen für Betriebssysteme und Daten |
|  | | |  | | Serverredundanz / Clustering | | |  |  |
|  | | |  | | RAID System / Festplattenspiegelung | | |  |  |
|  | | |  | | Videoüberwachung Serverraum | | |  |  |
|  | | |  | | Alarmmeldung bei unberechtigtem Zutritt zum Serverraum | | |  |  |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| Gewährleistung der Belastbarkeit der Systeme gemäß Art. 32 Abs. 1 lit. b) DSGVO | | | | | | | | | |
|  | | | Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | | | | | | |
|  | | | Technische Maßnahmen | | | | | Organisatorische Maßnahmen | |
|  | | |  | | Einsatz vor Firewall und regelmäßige Aktualisierung | | |  | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber der Aufsichtsbehörde) |
|  | | |  | | Einsatz von Spamfilter und regelmäßige Aktualisierung | | |  | Dokumentierte Vorgehensweis 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 Datenpassen z.B. via Ticketsystem |
|  | | |  | | Intrusion Prevention System (IPS) | | |  | Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall gemäß Art. 32 Abs. 1 lit. c) DSGVO | | | | | | | | | |
|  | | |  | | Umsetzung des BSI Standard 100-4 Notfallmanagement | | | | |
|  | | |  | | Notfallkonzept | | | | |
|  | | |  | | Notfallhandbuch | | | | |
|  | | |  | | Integration des Notfallmanagements in Geschäftsprozesse | | | | |
|  | | |  | | Durchführung von Notfallübungen | | | | |
|  | | |  | | Erprobung von Wiederanlaufszenarien | | | | |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 lit. d) DSGVO | | | | | | | | | |
|  | | |  | | Regelmäßige Revision des Sicherheitskonzepts | | | | |
|  | | |  | | Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und –bewertung | | | | |
|  | | |  | | Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme | | | | |
|  | | |  | | Externe Prüfungen, Audits, Zertifizierungen | | | | |
|  | | | Details und weitere Maßnahmen bitte hier beschreiben: | | | | | | |
| Weitere Maßnahmen | | | | | | | | | |
|  |  | | | Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. | | | | | |
|  |  | | | Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen. | | | | | |
|  |  | | | Sensibilisierung und/oder Schulung der an Verarbeitungsvorgängen Beteiligten | | | | | |
|  |  | | | Beteiligung des/der zuständigen Datenschutzbeauftragten | | | | | |
|  |  | | | Hinweis/Verpflichtung der an Verarbeitungsvorgängen Beteiligten auf das Datengeheimnis | | | | | |
|  |  | | | Folgende Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind: | | | | | |
|  |  | | | Im Falle einer Übermittlung oder Zweckänderung:  Folgende spezifischen Verfahrensregelungen werden getroffen, um die Einhaltung des LDSG und der DS-GVO sicherzustellen: | | | | | |
|  |  | | | Sonstiges: | | | | | |

# Bestätigung

Hiermit bestätige ich die Richtigkeit der für die Verarbeitungstätigkeit gemachten Angaben

|  |  |  |
| --- | --- | --- |
| ……………………………… | …………………… | ........................................................... |
| Name der/des Vertreterin/s  der verantwortlichen Fachabteilung | Datum | Unterschrift |