**Dokumentation der Verarbeitungstätigkeiten**

**[„Verfahrensname“]**

**Kontaktdaten des Datenschutzbeauftragten der HafenCity Universität:**

Dr. Christian Paulsen

Henning-Voscherau-Platz 1
20457 Hamburg
Tel.: +49 (0)40 4 28 27-4359

E-Mail: hcu-datenschutz@vw.hcu-hamburg.de

Autor(en):

Dokumentenversion und Datum:

Vertraulichkeit: Verschlusssache, nur für den Dienstgebrauch

|  |
| --- |
| **Angaben zum Verantwortlichen***Bezeichnung der Hochschule*HafenCity Universität Hamburg*Fachbereich / verantwortliche Organisationseinheit oder Abteilung**Ansprechpartnerin/-partner*Vollständiger Name : Ggf. Vertretung : Vorgesetzte(r) : *Anschrift der Dienststelle* Straße : Henning-Voscherau-Platz 1Postleitzahl, Ort : 20457 HamburgTelefon : 040 428 27 -E-Mail-Adresse :  |
| **Falls vorhanden: Angaben zum gemeinsamen Verantwortlichen***Bezeichnung der Hochschule oder der Organisation:**Ggf. Fachbereich / verantwortliche Organisationseinheit:**Ansprechpartnerin/-partner*Vollständiger Name : Ggf. Vertretung : Vorgesetzte(r) : *Anschrift* Straße : Postleitzahl, Ort : Telefon : E-Mail-Adresse :  |

**Hinweis: Beachten Sie bitte vor dem Ausfüllen der folgenden Kapitel die zugehörige Ausfüllhilfe.**

# Kurzbeschreibung des (Fach)verfahrens / der Verarbeitungstätigkeit

# Art und Umfang der Datenverarbeitung

## Welche Daten werden verarbeitet?

### Kreis der Betroffenen

* *Beschäftigte*
* *Studierende*
* *Bewerber*
* *Interessenten*
* *(Bibliotheks-)Nutzer*
* *Lieferanten*
* *etc.*

[Beispiele, nicht Zutreffendes bitte löschen, ggf. sinnvoll ergänzen]

### Datenkatalog

#### Nicht personenbezogene Informationen

*- Forschungsergebnisse*

*- Quellcodes*

*- Patente*

*- etc.*

*[Beispiele, nicht Zutreffendes bitte löschen, ggf. sinnvoll ergänzen]*

#### Personenbezogene Daten

* Werden personenbezogene oder personenbeziehbare Daten verarbeitet?

 [ ]  ja [ ]  nein (weiter mit 3.)

* Beschreibung der Kategorien von personenbezogenen Daten:
* *Adressdaten*
* *Kommunikationsdaten*
* *Bankverbindung*
* *Personalnummer*
* *Matrikelnummer*
* *etc.*

*[Beispiele, nicht Zutreffendes bitte löschen, ggf. sinnvoll ergänzen]*

## Auflistung aller Verarbeitungszwecke: Zu welchen/m Zweck(en) werden die Daten verarbeitet? Geben Sie bitte die entsprechenden Rechtsgrundlagen mit an.

## Ergänzende Information zu den dargestellten verarbeiteten Datenkategorien:

[ ]  Es werden keine besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet

[ ]  Es werden besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet und zwar

* *rassische und ethnische Herkunft,*
* *politische Meinungen,*
* *religiöse oder weltanschauliche Überzeugungen,*
* *Gewerkschaftszugehörigkeit,*
* *genetische Daten,*
* *biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,*
* *Gesundheitsdaten,*
* *Daten zum Sexualleben oder der sexuellen Orientierung.*

 [Nicht Zutreffendes bitte löschen]

## Schwellwertanalyse:

Die folgenden Kriterien deuten auf hohe Risiken bei einer Datenverarbeitung hin:

Bewertung und Einstufung (Scoring) einschließlich Prognosen und Profilerstellung

[ ]  ja [ ]  nein

Automatisch erfolgende Entscheidungen mit rechtlichen oder ähnlich signifikanten Auswirkungen für Betroffene

[ ]  ja [ ]  nein

Systematische Überwachung

[ ]  ja [ ]  nein

Sensible personenbezogene Daten

[ ]  ja [ ]  nein

Verarbeitung sehr großer Datenmengen

[ ]  ja [ ]  nein

Vergleich oder Kombination von Datensätzen

[ ]  ja [ ]  nein

Verarbeitung von Daten schutzbedürftiger natürlicher Personen

[ ]  ja [ ]  nein

Einsatz innovativer Technologien oder neuartiger organisatorischer Lösungen?

[ ]  ja [ ]  nein

Verhinderung, dass die betroffene Person ein Recht ausüben, eine Dienstleistung in Anspruch nehmen oder einen Vertrag abschließen kann

[ ]  ja [ ]  nein

## Ist aufgrund der oben aufgeführten Kriterien eine Datenschutzfolgeabschätzung erforderlich?

[ ]  ja [ ]  nein

Falls ja, ist eine ausführliche Risikobetrachtung und Bewertung der technisch-organisatorischen Maßnahmen (Datenschutzfolgeabschätzung, DSFA) in einem gesonderten Dokument, ggf. unter Zuhilfenahme externer Unterstützung und des Datenschutzbeauftragten zu erarbeiten.

## Datenoffenlegung: Wer kann die personenbezogenen Daten einsehen?

* Intern (Abteilung / Funktion):
* Extern (Empfängerkategorie):
* Extern in Drittland oder an internationale Organisation (Kategorie):

## Kann der Umfang der verarbeiteten Daten ggf. reduziert werden?

[ ]  ja [ ]  nein

Erläuterungen:

## Können personenbezogene Daten pseudonymisiert werden?

[ ]  ja [ ]  nein

Erläuterungen:

## Werden personenbezogene Daten nach geregelten Vorgaben gesperrt und gelöscht (Beachtung von Löschfristen)?

[ ]  ja [ ]  nein

Erläuterungen:

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

[ ]  Eine entsprechende Datenübermittlung findet nicht statt

[ ]  Eine entsprechende Datenübermittlung findet wie folgt statt:

* Nennung der konkreten Datenempfänger:

Übermittlung in Drittland:

"[Name(n) der konkreten Empfänger]"

Übermittlung an internationale Organisation:

"[Name(n) der konkreten Empfänger]"

[Nicht Zutreffendes bitte löschen]

* Dokumentation geeigneter Garantien sofern es sich um eine Datenübermittlung in ein Drittland oder an eine internationale Organisation handelt:

"[Darstellung der geeigneten Garantien für den Schutz personenbezogener Daten im Rahmen einer Datenübermittlung]"

## Datenquellen - Woher stammen die Daten?

Datenintegration - Werden Informationen / Daten aus anderen Verfahren genutzt?

[ ]  ja [ ]  nein

#### Falls ja, aus welchen Verfahren?

## Datennutzung – Wer nutzt die Daten?

# Feststellung des Schutzbedarfes nach Schutzzielen

Der Schutzbedarf wird hier für jedes der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, ermittelt und dokumentiert. Der Schutzbedarf orientiert sich an dem Ausmaß der **Schäden**, die durch Vorfälle entstehen können:

* **normal:** Die Schadensauswirkungen sind begrenzt und überschaubar.
* **hoch:** Die Schadensauswirkungen können beträchtlich sein.
* **sehr hoch:** Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

## Schutzziel Vertraulichkeit

Es ist zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können. Welcher Schaden kann entstehen, wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden? (Vertraulichkeitsanforderungen)

|  |  |  |
| --- | --- | --- |
| Schadensszenarien | Schutzbedarf | Begründung |
| * Verstoß gegen Gesetze/Vorschriften/Verträge
* Beeinträchtigung des informationellen Selbstbestimmungsrechts
* Negative Außenwirkung
 | [ ]  normal[ ]  hoch[ ]  sehr hoch |  |

## Schutzziel Integrität

Es ist zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben. Welcher Schaden kann entstehen, wenn die Korrektheit der zu schützenden Informationen nicht mehr gegeben ist?

|  |  |  |
| --- | --- | --- |
| Schadensszenarien | Schutzbedarf | Begründung |
| * Verstoß gegen Gesetze/Vorschriften/Verträge
* Beeinträchtigung der Aufgabenerfüllung
* Negative Außenwirkung
* Finanzielle Auswirkungen
 | [ ]  normal[ ]  hoch[ ]  sehr hoch |  |
|  |

## Schutzziel Verfügbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Welcher Schaden kann entstehen, wenn autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden?

|  |  |  |
| --- | --- | --- |
| Schadensszenarien | Schutzbedarf | Begründung |
| Beeinträchtigung der AufgabenerfüllungNegative AußenwirkungFinanzielle Auswirkungen | [ ]  normal[ ]  hoch[ ]  sehr hoch |  |
|  |

# Verwendete IT-Infrastruktur

## Beteiligte Systeme und Anwendungen

## Tolerierbare Ausfallzeit

## Wie ist die Vorgehensweise bei Änderung von Programmfunktionalitäten?

## Wer betreut die Anwendung(en)?

## Wie und durch wen erfolgt die Abnahme und Freigabe der IT-Anwendung(en)?

## Wie und durch wen erfolgt die Schulung, Einweisung oder Unterrichtung und die Betreuung der betroffenen Anwender?

# Sonstige Datenschutzverpflichtungen

[ ]  Datenschutzerklärung für Webseiten anpassen

[ ]  Vertrag / Verträge zur Auftragsverarbeitung vereinbaren mit den folgenden Drittanbietern:

[ ]  Information der Betroffenen

[ ]  Einwilligungserklärung(en) einholen

# Nächste Überprüfung dieser Verfahrensdokumentation

Erwartete Veränderung (mehrfaches Ankreuzen möglich):

[ ]  wesentliche Änderung durch technischen Fortschritt (z.B. neue Bedrohungsszenarien)

[ ]  Nutzung neuer Software-Versionen

[ ]  Nutzung neuer Hardware/Infrastrukturkomponenten

[ ]  Routinemäßige Überprüfung in X Jahr(en) am TT.MM.JJJJ

[ ]  Sonstiges:

# Auflistung der Anlagen

Anlage 1: Technisch-Organisatorische Maßnahmen

# Anlage 1 – Technisch-Organisatorische Maßnahmen (TOMs)

[Es folgen die Standard-Maßnahmen an der HCU. Bitte ggf. ergänzen, falls weitere Maßnahmen für dieses Verfahren umgesetzt sind bzw. Maßnahmen löschen, die nicht anwendbar sind.]

1. **Zutrittskontrolle**

Ziel: Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

* 1. **Zutrittskontrolle zum Gebäude (Überseeallee 16)**
* Definition öffentlicher Zutrittszeiten
* Wach- und Pförtnerdienst außerhalb der öffentlichen Zutrittszeiten
* Automatischer Verschluss außerhalb der öffentlichen Zutrittszeiten
* Türsicherungen (Transponder) in Verbindung mit dem Zutrittskontrollsystem
* revisionssicheres Verfahren für die Beantragung von Zutrittsberechtigungen außerhalb der öffentlichen Öffnungszeiten für einen überschaubaren Personenkreis
* zeitlich limitierte Vergabe von Zutrittsberechtigungen
* organisatorische Maßnahmen für die Sperrung von Zutrittsberechtigungen
* organisatorische Maßnahmen bei Feststellung eines unberechtigten Zutritts.
	1. **Zutrittskontrolle zu den Büroräumen (Administratoren, Sachbearbeiter)**
* Elektronisches Zutrittskontrollsystem

Die Räumlichkeiten, in denen sich die PCs der Administratoren und Sachbearbeiter befinden, sind bei Abwesenheit der Beschäftigten grundsätzlich verschlossen. Zugang zu diesen Räumlichkeiten erhalten nur autorisierte Beschäftigte mit Hilfe einer elektronischen Zutrittsberechtigung. Die Berechtigungsvergabe erfolgt im Rahmen eines genehmigungspflichtigen schriftlichen Antragsverfahrens. Schlüsselberechtigte können für die ihnen zugewiesenen Mitarbeiter einen Schlüssel beim zuständigen Administrator beantragen.

* 1. **Zutrittskontrolle zum Serverraum (Überseeallee 16)**
* Einschränkung des Zugangs zum Server­raum
* Schlüsselverwaltung / Dokumentation der Schlüsselvergabe (Transponder DB Zutrittskontrolle)
* Türsicherungen (Transponder) in Verbindung mit dem Zutrittskontrollsystem
* Wach- und Pförtnerdienst
1. **Zugangskontrolle**

Ziel: Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

* Persönlicher und individueller User-Log-In bei Anmeldung an Clients und dem jeweiligen System
* Kennwortvorgaben (Wechseln des Passworts in regelmäßigen Abständen, mindestens 10 Zeichen, gemischte Zeichen, Passworthistorie)
* Zusätzlicher System-Log-ln für bestimm­te Anwendungen
* Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirm­schoner oder automatische Pausenschal­tung)
* Dokumentation der Gruppenzugehörigkeit im Active Directory

**3. Zugriffskontrolle**

Ziel: Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

* Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
* Verwaltung von Berechtigungen
* Profile / Rollen
* Dokumentation von Berechtigungen
* Genehmigungsroutine
* Auswertungen / Protokollierungen

**4. Weitergabekontrolle**

Ziel: Aspekte der Weitergabe personenbezogener Daten sind zu regeln.

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

* Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
* Protokollierung
* Transportsicherung

Weitergabe-Kontrolle innerhalb des WI-Netzes:

* gesicherte Verbindung / SSL-Verschlüsselung bei Web-Access

Weitergabe Kontrolle innerhalb des FHH-Netzes:

* SSL-Verschlüsselung bei Web-Access
* Einsatz verschlüsselter USB-Sticks

**5. Eingabekontrolle**

Ziel: Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Eingabekontrolle innerhalb des WI-Netzes:

* Zugriffsrechte (Steuerung über AD)
* Systemseitige Protokollierungen
* funktionelle Verantwortlichkeiten

Eingabekontrolle innerhalb des FHH-Netzes:

* Zugriffsrechte
* Systemseitige Protokollierungen
* funktionelle Verantwortlichkeiten

**6. Auftragskontrolle**

Ziel: Die weisungsgemäße Auftragsverarbeitung ist zu gewährleisten. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeberin und Auftragnehmer:

* Eindeutige Vertragsgestaltung
* Kontrolle der Vertragsausführung

**7. Verfügbarkeitskontrolle**

Ziel: Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

* Backup-Verfahren
* Spiegeln von Festplatten
* Unterbrechungsfreie Stromversorgung (USV)
* Netzersatzanlage (Dieselgenerator)
* Backups (getrennter Brandabschnitt)
* Virenschutz / Firewall
* Klimaanlagen

**8. Trennungskontrolle**

Ziel: Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

* getrennte Systeminstanzen (logische Trennung)
* getrennte Datenbanken
* Zugriffsberechtigungen