# NR. 1172

10.02.2023

## **AMTLICHE BEKANNTMACHUNGEN** der HS Bochum




Hochschule Bochum
Bochum University
of Applied Sciences

Hochschule Bochum
Der Präsident/Der Kanzler
Dez. 6/J – CW

16.12.2022

# Datenschutzleitlinie der Hochschule Bochum

Vom 16. Dezember 2022

Aufgrund des § 16 Abs. 1 S. 2 des Hochschulgesetzes in der Fassung der Bekanntmachung vom 16. September 2014 (GV. NRW S. 547), das zuletzt durch Artikel 1 des Gesetzes betreffend die Mitgliedschaft der Universitätskliniken im Arbeitgeberverband des Landes (GV. NRW S. 780b) geändert worden ist, erlässt das Präsidium der Hochschule Bochum folgende Leitlinie:

**Inhalt:**

## 1. Präambel

Die Hochschule Bochum verarbeitet eine Vielzahl von personenbezogenen Daten von ihren Mitgliedern, Angehörigen, Bewerbern, von Forschung betroffenen Personen und externen Kooperationspartnern, Dienstleistern und Lieferanten, um ihre Aufgaben nach dem Hochschulgesetz zu erfüllen. Der Schutz der informationellen Selbstbestimmung von betroffenen Einzelpersonen verwirklicht deren Grundrecht aus Art. 8 der EU-Grundrechte-Charta, das durch die EU-Datenschutzgrundverordnung, das Landesdatenschutzgesetz und die bereichsspezifischen Regelungen zum Datenschutz an Hochschulen weiter konkretisiert wird. Die Hochschule Bochum als öffentliche Stelle und Stätte der freien geistigen Entfaltung, ist sich der Bedeutung des Grundrechts auf informationelle Selbstbestimmung bewusst und setzt sich aktiv für dessen Verwirklichung ein. Zur Erfüllung dieser Anforderungen baut die Hochschule ein Datenschutz-Managementsystem auf, mit dem der gesetzeskonforme Schutz personenbezogener Daten gewährleistet wird. Grundlage des Datenschutz- Managementsystems ist diese Leitlinie. Während der Datenschutz den Schutz **personenbezogener** Daten zum Ziel hat, geht es in der Informationssicherheit um die Aufrechterhaltung des **Schutzes von Informationen, Daten und Systemen**. Dazu ist es bei der Informationssicherheit notwendig, Geschäftsprozesse und deren Abhängigkeiten von Informationen aus dem Blickwinkel auf mögliche Risiken zu analysieren, um diese durch angemessene und wirtschaftlich vertretbare Gegenmaßnahmen zu minimieren. Auf diese Weise unterstützen die in der Informationssicherheit verankerten Ziele, wie Vertraulichkeit, Integrität und Verfügbarkeit auch den Datenschutz. Ein Datenschutz-Managementsystem kann kein Informationssicherheits-Managementsystem ersetzen und umgekehrt. Beide Systeme sind notwendig.

## 2. Zielsetzung und Gegenstand

Ziel und Gegenstand dieser Leitlinie ist die Sicherstellung der Einhaltung des Datenschutzes durch organisatorische, prozessuale und technische Maßnahmen.
Zur Erreichung des Ziels ist der Aufbau eines Datenschutz-Managements erforderlich, das insbesondere die folgenden materiellen Anforderungen nachweisbar sicherstellen soll:

a) Gewährleistung einer rechtmäßigen, fairen und transparenten Verarbeitung:
    a. Eine Verarbeitung erfolgt nur mit Rechtsgrundlage (Gesetz, Einwilligung).
    b. Vorrang der Direkterhebung bei der betroffenen Person.
    c. Transparente Informationen über Art und Umfang der Verarbeitung, Betroffenen- und Beschwerderechte.
    d. Führung eines Verzeichnisses von Verarbeitungstätigkeiten zur Ermöglichung von internen und externen Kontrollen durch die Aufsichtsbehörde.
b) Einhaltung der Anforderungen zur Zweckbindung, indem Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
c) Einhaltung des Grundsatzes der Datenminimierung, indem nur die für die Aufgabenerfüllung erforderlichen Daten erhoben und verarbeitet werden.
d) Gewährleistung der sachlichen Richtigkeit der Daten durch Maßnahmen, die sicherstellen, dass alle Teile der personenbezogenen Daten vollständig wiedergegeben werden, richtig und unverfälscht sind und falsche oder verfälschte personenbezogene Daten unverzüglich gelöscht oder berichtigt werden. (Integrität der personenbezogenen Daten)

e) Speicherbegrenzung, indem Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person mit den gebotenen gesetzlichen Ausnahmen nur so lange ermöglicht wie es für den Zweck der Verarbeitung erforderlich ist.
f) Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit, indem die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, insbesondere den Schutz vor:
    a. Unbefugter oder unrechtmäßiger Verarbeitung
    b. Unbeabsichtigtem Verlust
    c. Unbeabsichtigter Zerstörung oder Schädigung

    Hier soll die Verzahnung mit dem bestehenden Informationssicherheits-Management an der Hochschule zu größtmöglichen Synergien führen, soweit kein Konflikt zwischen Sicherheitsmaßnahmen und Datenschutz besteht.
g) Verwirklichung der Betroffenenrechte, durch Strukturen und Meldewege, die Auskünfte und daran anknüpfende weitere Betroffenenrechte ermöglichen.
h) Einhaltung der gesetzlichen Anforderungen bei der Einbindung von Dritten in die eigene oder gemeinsame Datenverarbeitung.
i) Prüfung der Rechtmäßigkeit vor Datentransfers an Stellen außerhalb der EU.
j) Strukturelle und organisatorische Sicherstellung der Meldepflichten aus Art. 33 und 34 EU-DSGVO bei Datenschutzverstößen gegenüber Aufsichtsbehörde und betroffenen Personen. Hierzu gehört insbesondere die Sensibilisierung und Schulung der Mitarbeiter damit Vorfälle vermieden, richtig erkannt, richtig eingeordnet und richtig gemeldet werden.
k) Durchführung von Datenschutz-Folgeabschätzungen bei Vorliegen der Voraussetzungen aus Art. 35 EU-DSGVO

Die Umsetzung dieser Maßnahmen erfolgt durch Erstellung eines Datenschutzkonzepts. Dieses beinhaltet eine Organisationsstruktur mit Verantwortlichkeiten, Prozessen und Aufgaben, Anleitungen, Handreichungen sowie die die technische Unterstützung der Prozesse und der Dokumentation (Dokumentationssystem).
Die Hochschulleitung unterstützt diese Anstrengungen auf allen Ebenen und stellt die erforderlichen Ressourcen zur Verfügung.

## 3. Verantwortlichkeiten

- **Präsidium:** Das Präsidium trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Es ist verantwortlich für die Einführung und Weiterentwicklung eines Datenschutzmanagementsystems (DSMS). Es trägt durch seine Entscheidungen dem Organisationsziel Rechnung und stellt die erforderlichen finanziellen, personellen und zeitlichen Ressourcen für die Umsetzung des Datenschutzes zur Verfügung. Das Präsidium trägt dafür Sorge, dass Mitglieder und Angehörige der Hochschule Bochum durch Informationsangebote oder Schulungen für den Datenschutz und die Sicherheit personenbezogener Daten sensibilisiert werden.
- **Behördliche Datenschutzbeauftragte oder Datenschutzbeauftragter:** Die oder der bestellte Datenschutzbeauftragte überwacht und unterstützt die Einhaltung der gesetzlichen Vorgaben zum Datenschutz sowie die Mitarbeitersensibilisierung durch Schulungen und berät das Präsidium und auf Anfrage Mitarbeitende, die Verarbeitungen durchführen, bei der Umsetzung des Datenschutzes. Die/der behördliche Datenschutzbeauftragte wird dabei unterstützt durch die Datenschutzkoordinatorinnen oder Datenschutzkoordinatoren. Sie oder er ist Ansprechpartner für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde.

- **Informationssicherheitsbeauftrage oder Informationssicherheitsbeauftragter:** Die oder der Informationssicherheitsbeauftragte berät das Präsidium bei allen Fragen zur IT-/Informationssicherheit und ist zuständig für die Konzeptionierung, Steuerung, Dokumentation und Weiterentwicklung des Informationssicherheits-Managementsystems. Sie oder er tauscht sich regelmäßig und darüber hinaus anlassbezogen mit der oder dem behördlichen Datenschutzbeauftragten zur Ordnungsmäßigkeit der Verarbeitungstätigkeiten, Maßnahmen der Informationssicherheit und zu datenschutzrelevanten Sicherheitsvorfällen aus. Im Falle eines Konflikts einer Sicherheitsmaßnahme mit dem Datenschutz verpflichtet sich die oder der Informationssicherheitsbeauftragte, an einer Lösung mitzuwirken, die beiden Aspekten angemessen Rechnung trägt.
- Die weiteren Zuständigkeiten und die Organisationstruktur mit Verantwortlichkeiten werden in Abstimmung mit der Hochschulleitung in den der Leitlinie folgenden Richtlinien und Ordnungen festgelegt.

## 4. Verstöße

Die Nichtbeachtung datenschutzrechtlicher Bestimmungen kann für die Hochschule rechtliche Folgen nach sich ziehen und ist eine objektive Verletzung der Dienstpflichten, die dienst- arbeits-, straf- und zivilrechtliche Folgen nach sich ziehen können. Sie können unter Umständen auch zu Regressansprüchen gegen die Verursacher führen.

## 5. Inkrafttreten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Hochschule Bochum in Kraft.

Ausgefertigt aufgrund des Beschlusses des Präsidiums der Hochschule Bochum vom 23.01.2023.

Bochum, 13.02.2023
Der Präsident

gez. *Wytzisk-Arens*

(Prof. Dr. Andreas Wytzisk-Arens)

Bochum, 10.02.2023
Der Kanzler

gez. *Hinsenkamp*

(Dipl.-Ök. Markus Hinsenkamp)

Hochschule Bochum
Der Präsident/Der Kanzler
Dez. 6/J - CW

16.12.2022

# Leitlinie zur Informationssicherheit

Vom 16. Dezember 2022

Aufgrund des § 16 Abs. 1 S. 2 des Hochschulgesetzes in der Fassung der Bekanntmachung vom 16. September 2014 (GV. NRW S. 547), das zuletzt durch Artikel 1 des Gesetzes betreffend die Mitgliedschaft der Universitätskliniken im Arbeitgeberverband des Landes (GV. NRW S. 780b) geändert worden ist, erlässt das Präsidium der Hochschule Bochum folgende Leitlinie:

**Inhalt**:

## Präambel

Alle Bereiche der Hochschule Bochum verarbeiten in ihren Prozessen, Verfahren oder Arbeitsabläufen Informationen und Daten. Die Hochschulleitung ist sich darüber bewusst, dass die Informationsverarbeitung mit Risiken verbunden ist und durch angemessene Sicherheitsmaßnahmen geschützt werden muss.

Das Präsidium hat aus diesem Anlass die Initiierung des Informationssicherheitsprozesses beschlossen sowie der Einführung eines Informationssicherheits-Managementsystems zugestimmt.

Übergeordnetes Kriterium für geeignete Sicherheitsmaßnahmen ist deren Wirksamkeit in Verbindung mit einem tolerierbaren Restrisiko. Dabei werden insbesondere die wirtschaftliche Angemessenheit, die Ergonomie und die größtmögliche Handlungsfreiheit für Forschung und Lehre berücksichtigt. Ziel ist es, die zentrale Verwaltung und die damit verbundenen zentralen Dienstleistungen kontinuierlich auf höchstem Niveau betreiben zu können, um sowohl Studium als auch Forschung und Lehre optimal zu unterstützen.

Die vorliegende Leitlinie beschreibt die allgemeinen Grundsätze, Ziele und Sicherheitsmaßnahmen, die für die Initiierung, Etablierung und Aufrechterhaltung eines ganzheitlichen Informationssicherheitsprozesses an der Hochschule Bochum erforderlich sind. Während der Datenschutz den Schutz **personenbezogener** Daten zum Ziel hat, geht es in der Informationssicherheit um die Aufrechterhaltung des **Schutzes von Informationen, Daten und Systemen**. Dazu ist es bei der Informationssicherheit notwendig, Geschäftsprozesse und deren Abhängigkeiten von Informationen aus dem Blickwinkel auf mögliche Risiken zu analysieren, um diese durch angemessene und wirtschaftlich vertretbare Gegenmaßnahmen zu minimieren. Auf diese Weise unterstützen die in der Informationssicherheit verankerten Ziele, wie Vertraulichkeit, Integrität und Verfügbarkeit auch den Datenschutz. Ein Datenschutz-Managementsystem kann kein Informationssicherheits-Managementsystem ersetzen und umgekehrt. Beide Systeme sind notwendig.

## § 1 Zielsetzung

Ziel der Informationssicherheit ist es, den Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff, Verwendung, Offenlegung, Unterbrechung, Änderung oder Zerstörung zu gewährleisten, sowie die Risiken, die auf die folgenden drei Grundwerte einwirken, auf ein vertretbares Maß zu reduzieren:

(1) Vertraulichkeit
Schutz vor unberechtigtem Zugriff und Offenlegung von Informationen.

(2) Integrität
Schutz vor unbefugter Änderung oder Zerstörung von Informationen, einschließlich der Gewährleistung ihrer Authentizität.

(3) Verfügbarkeit
Die Nutz- und Erreichbarkeit aller für die Aufrechterhaltung des Betriebs erforderlichen Informationen und der zugehörigen IT-gestützten Dienste, Daten und der IT-Infrastruktur ist zu gewährleisten.

Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.

Die vorliegende Informationssicherheitsleitlinie definiert den Rahmen der Informationssicherheitspolitik der Hochschule Bochum. Sie ist die Grundlage für das Informationssicherheitskonzept, das detaillierte Maßnahmen in Informationssicherheits-richtlinien beschreibt.

## § 2 Geltungsbereich

Diese Leitlinie gilt für die Hochschulverwaltung, die Fachbereiche und alle Einrichtungen der Hochschule Bochum sowie für alle Mitglieder, Angehörige und Externe, die im Auftrag der Hochschule Bochum Informationen verarbeiten oder IT-Systeme der Hochschule Bochum nutzen.

## § 3 Organisationsstruktur und Verantwortlichkeiten

Die Gesamtverantwortung für die Informationssicherheit an der Hochschule Bochum trägt das Präsidium der Hochschule. Das Präsidium stellt die notwendigen Ressourcen zur Erreichung und Aufrechterhaltung der Schutzziele bereit und verabschiedet die vorliegende Leitlinie zur Informationssicherheit.

Das Präsidium bestellt die Informationssicherheitsbeauftragte oder den Informations-sicherheitsbeauftragten (ISB) für die Hochschule Bochum. Die oder der Beauftragte für Informationssicherheit ist zuständig für die Konzeptionierung, Steuerung, Dokumentation und Weiterentwicklung des Informationssicherheits-Managementsystems und berichtet über dessen Entwicklung und den allgemeinen Stand zur Informationssicherheit dem Präsidium.

Die weiteren Zuständigkeiten und die Organisationstruktur mit Verantwortlichkeiten werden in Abstimmung mit der Hochschulleitung in den der Leitlinie folgenden Richtlinien und Ordnungen festgelegt.

## § 4 Informationssicherheitsmanagement

(1) Mit Informationssicherheitsmanagement wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen.
(2) Grundlage des Informationssicherheitsprozesses ist eine Strukturanalyse zur Ermittlung des Schutzbedarfes der einzelnen Geschäftsprozesse der Hochschule, welche an IT-Systeme und −Anwendungen gekoppelt sind, um einen entsprechenden Schutz zu bestimmen. Daraus wird für die Hochschule Bochum entsprechend den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein allgemeines Informationssicherheitskonzept erstellt.
(3) Das Informationssicherheitskonzept wird regelmäßig auf seine Aktualität, Angemessenheit und Wirksamkeit geprüft. Das Präsidium unterstützt die ständige Verbesserung und Einhaltung des Sicherheitsniveaus durch eine kontinuierliche Revision der Regelungen bzw. Richtlinien.
(4) Das diese Leitlinie ergänzende Informationssicherheitskonzept beinhaltet die allgemeinen Regeln und Hinweise zur Informationssicherheit. Es wird durch weiterführende detaillierte Maßnahmenbeschreibungen ergänzt.

## § 5 In-Kraft-Treten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Hochschule Bochum in Kraft.

Ausgefertigt aufgrund des Beschlusses des Präsidiums der Hochschule Bochum vom 23.01.2023.

Bochum, 13.02.2023
Der Präsident

gez. *Wytzisk-Arens*

(Prof. Dr. Andreas Wytzisk-Arens)

Bochum, 10.02.2023
Der Kanzler

gez. *Hinsenkamp*

(Dipl.-Ök. Markus Hinsenkamp)