Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

74/2022
Mitteilungsblatt / Bulletin
16. August 2022

Richtlinie
zur Organisation des Datenschutzes und der Informationssicherheit an der Hochschule für Wirtschaft und Recht Berlin
vom 10.08.2022

Editor
Der Präsident der Hochschule für Wirtschaft und Recht Berlin /
The President of the Berlin School of Economics and Law
Badensche Straße 52 • 10825 Berlin
T +49 (0)30 30877-1393 • F +49 (0)30 30877-1319

Inhalt

Richtlinie
zur Organisation des Datenschutzes und der Informationssicherheit an der Hochschule für Wirtschaft und Recht Berlin vom 10.08.2022

Präambel und Ziele der Richtlinie

Im Jahr 2016 wurde durch den europäischen Gesetzgeber die Datenschutz Grundverordnung (DSGVO) erlassen und entfaltete 2018 Rechtsverbindlichkeit. Die DSGVO regelt die Grundsätze, die bei der Verarbeitung personenbezogener Daten zu beachten sind. Daneben unterliegt die Hochschule u.a. noch folgenden weiteren relevanten gesetzlichen Regelwerken:

- E-Government-Gesetz Berlin § 23 - Verpflichtung zum Aufbau eines Informations-Sicherheits-Management-Systems (ISMS) gemäß den Standards des Bundesamtes für die Sicherheit in der Informationstechnik
- Bundesdatenschutzgesetz
- Telekommunikations-Telemedien-Datenschutz-Gesetz
- Landesdatenschutzgesetz Berlin
- Berliner Hochschulgesetz
- Studierendendatenverordnung Berlin

Zur Umsetzung dieser gesetzlichen Anforderungen und den Erfordernissen an eine sichere Verarbeitung von Informationen (im Sinne der Informationssicherheit), wird diese Richtlinie erlassen.

§ 1 Geltungs-/ Anwendungsbereich

Der Geltungsbereich dieser Richtlinie erstreckt sich auf alle digital und analog verarbeiteten Informationen sowie auf jegliche verarbeiteten personenbezogenen Daten innerhalb der Verfahren und Geschäftsprozesse der HWR Berlin, auf alle Einrichtungen der Hochschule, auf die gesamte IT-Infrastruktur der Hochschule, einschließlich der betriebenen IT-Systeme sowie auf die Gesamtheit der Mitglieder der HWR Berlin.

§ 2 Bedeutung des Datenschutzes und der Informationssicherheit

Vor dem Hintergrund der gesetzlichen Anforderungen sowie der Ziele der Richtlinie muss Datenschutz und Informationssicherheit ein integraler Bestandteil der Hochschulkultur sein.
Die Hochschulleitung trägt die Verantwortung in Fragen des Datenschutzes. Demgegenüber muss sich jedes Mitglied der HWR Berlin der Notwendigkeit und Beachtung datenschutzrechtlicher Vorgaben bzw. Informationssicherheitsmaßnahmen bewusst sein.

§ 3 Hierarchie der Richtlinien / Dokumente zum Datenschutz und zur Informationssicherheit

Die Richtlinie zum Datenschutz und für Informationssicherheit definiert die Rollen, Zuständigkeiten und Verantwortlichkeiten, die für die Organisation der Informationssicherheit und des Datenschutzes maßgeblich sind.

Die Richtlinie wird durch Handbücher, Leitfäden, Handlungsanweisungen und Benutzungsordnungen ergänzt, die im Rahmen der jeweiligen Zuständigkeiten erstellt und erlassen werden. Diese Dokumente dienen der Festsetzung und Kommunikation von verbindlichen Regeln, technischen Vorgaben und Prozessen, die im Rahmen der Informations-Sicherheits- und Datenschutzorganisation anzuwenden und einzuhalten sind. Sofern keine anderen Zuständigkeiten geregelt sind, werden sie von der oder dem Chief Information Officer in Abstimmung mit der IT-Leitung und der Stabsfunktion Datenschutz und Informationssicherheit erlassen.

§ 4 Organisation des Managementsystems für Datenschutz bzw. Informationssicherheit

Der folgende Abschnitt gibt Auskunft darüber, welche Rollen innerhalb der Datenschutz- bzw. Informationssicherheitsorganisation definiert sind. Daneben sind die Verantwortlichkeiten und Aufgaben beschrieben.

1. Hochschulleitung (HL)

Die Hochschulleitung ist das oberste Entscheidungsgremium. Sie verabschiedet auf Vorschlag der oder des Chief Information Officer und der oder dem Datenschutzbeauftragten diese Richtlinie.
Die Hochschulleitung ist dafür verantwortlich, sicherzustellen, dass das Informationssicherheits- bzw. Datenschutzmanagementsystem entsprechend dieser Richtlinie umgesetzt, aktualisiert und die notwendigen Ressourcen zur Verfügung gestellt werden. Der IT-Leitung, der oder dem Datenschutzbeauftragten und der Stabsfunktion "Datenschutz und Informationssicherheit" werden von der Hochschulleitung ausreichende finanzielle, personelle und zeitliche Ressourcen zur Verfügung gestellt, um die durch diese Richtlinie definierten Ziele zu erreichen. Die Hochschulleitung erhält von der IT-Leitung, der Stabsfunktion "Datenschutz und Informationssicherheit" und der oder dem Datenschutzbeauftragten jährlich eine Stellungnahme hinsichtlich der zur Verfügung gestellten Ressourcen.

Die Gesamtverantwortung für Datenschutz und Informationssicherheit verbleibt bei der Hochschulleitung.

2. Chief Information Officer (CIO)

Die Kanzlerin oder der Kanzler ist Chief Information Officer (CIO) der HWR Berlin. Diese Funktion umfasst die Ressortverantwortung über die an der HWR Berlin verarbeiteten Informationen und personenbezogenen Daten sowie den Betrieb und die Weiterentwicklung der Informations- und Kommunikationstechnik (IuK). Dies schließt die Ressortverantwortung für Datenschutz, Informations- und IT-Sicherheit mit ein. Die Funktion der oder des Chief Information Officer ist mit der erforderlichen Entscheidungskompetenz und damit der Entscheidungsverbindlichkeit für alle Belange ausgestattet, die hinsichtlich der genannten Verantwortlichkeiten von Bedeutung sind.
Die Aufgaben der oder des Chief Information Officer bestehen aus:

- Generalverantwortung für Informations- und Kommunikationstechnologie
- Aufbau einer geeigneten Informationssicherheits- und Datenschutzorganisation bzw. Initiierung und Fortschreibung eines Informationssicherheits- und Datenschutzmanagementsystems
- Bestimmung von Datenschutz- und Informationssicherheitszielen
- Aussprache von Empfehlungen zur Fortschreibung der Datenschutz- und Informationssicherheitsrichtlinie
- Überprüfung der Umsetzung dieser Richtlinie

- Analyse aller Informations- und Kommunikations-Leistungen der Hochschule nach innen und außen, die sowohl die technische Infrastruktur als auch die IuK-Services betreffen
- Vorbereitung aller Entscheidungen auf dem Informations- und Kommunikations-Gebiet der Hochschule und der Ausarbeitung von Entscheidungshilfen für die Hochschulleitung
- Interessenvertretung der Hochschule nach außen auf dem Informations- und Kommunikations-Gebiet in grundsätzlichen Koordinierungsaufgaben (Ministerium, Deutsches Forschungsnetz, Senat, etc.).

Die oder der Chief Information Officer wird bei der Wahrnehmung der Aufgaben von der IT-Leitung und der Stabsfunktion Datenschutz und Informationssicherheit unterstützt.

3. Behördliche Datenschutzbeauftragte oder Behördlicher Datenschutzbeauftragter (bDSB)

Die Hochschulleitung benennt eine Behördliche Datenschutzbeauftragte oder einen Behördlichen Datenschutzbeauftragten. Die Benennung ist zu dokumentieren und gegenüber der Hochschule sowie der Aufsichtsbehörde bekannt zu geben. Die oder der Behördliche Datenschutzbeauftragte ist frei von Weisungen und trägt direkt der oder dem Chief Information Officer als Teil der Hochschulleitung vor.
Die Aufgaben der oder des Behördlichen Datenschutzbeauftragten ergeben sich aus den gesetzlichen Bestimmungen. Daneben berichtet die oder der Behördliche Datenschutzbeauftragte jährlich über den Stand in Sachen Datenschutz an den Akademischen Senat und die Hochschulleitung

4. IT-Leitung

Die zentrale Instanz für operative IT-Sicherheit ist die IT-Leitung. Sie ist für den sicheren Betrieb der IT und die Einbringung bzw. Umsetzung geeigneter IT-Sicherheitsmechanismen verantwortlich.
Die IT-Leitung sorgt u.a. für die technische Umsetzung und Einhaltung von Maßnahmen und Regelungen, die dem Schutz personenbezogener Daten, Informationen oder der IT-Systeme dienen (u.a. durch Bereitstellung aktueller Software-Versionen, sowie auf regelmäßiges Einspielen von Updates und eine in Hinblick auf die IT-Sicherheit angemessene Konfiguration).
Die IT-Leitung stellt sicher, dass die oder der Behördliche Datenschutzbeauftragte frühzeitig in alle IT-Projekte eingebunden wird.

5 Beratungskreis für IuK, Datenschutz und Informationssicherheit (BIDI)

Der Beratungskreis für Datenschutz und Informationssicherheit setzt sich aus der IT-Leitung, der oder dem Behördlichen Datenschutzbeauftragten, einer Professorin oder einem Professor mit einem Arbeitsschwerpunkt in fachlicher Nähe zum Handlungsfeld IT-Sicherheit und Datenschutz sowie der Stabsfunktion Datenschutz und Informationssicherheit zusammen. Die Professorin oder der Professor wird von der Hochschulleitung jeweils für die Dauer einer Wahlperiode der Hochschulleitung benannt. Der BIDI berät die oder den Chief Information Officer in Fragen IuK, Datenschutz und Informationssicherheit. Die Sitzungen finden statt, sooft es die Geschäftslage erfordert, mindestens jedoch einmal pro Semester. Die Sitzungen werden durch die oder den Chief Information Officer einberufen.

6. Stabsfunktion Datenschutz und Informationssicherheit

Die Stabsstelle Datenschutz und Informationssicherheit unterstützt die Hochschule bei der Sicherstellung von Datenschutz- und Informationssicherheitsanforderungen und wirkt auf die Einhaltung datenschutzrechtlicher Vorschriften hin. Die Mitarbeitenden der Stabsstelle sind zugleich Ansprechpersonen der Hochschulmitglieder in Belangen des Datenschutzes und der Informationssicherheit.
Die Aufgaben der Stabsstelle umfassen ferner:

- Initiierung, Aufbau und Betrieb eines Informations-Sicherheits-Management-Systems nach BSI IT-Grundschutz
- Führung des Registers zur Datenschutzdokumentation (Datenschutzvorfälle, Verarbeitungsverzeichnis, Einwilligungen, etc.)
- Erstellung eines jährlichen Berichtes über den Stand in Sachen Datenschutz und Informationssicherheit an den Akademischen Senat und die Hochschulleitung
- Erarbeitung von Empfehlungen zur Änderung dieser Richtlinien und übergreifender Informationssicherheits- und Datenschutzkonzepte
- Koordination bzw. Umsetzung von Informationssicherheitstrainings und -programmen zur Bewusstseinsbildung (Awareness) für Mitglieder der HWR Berlin
- Koordination, Beratung, Information und Weiterbildung der Koordinatoren für Datenschutz und Informationssicherheit
- Erstellung von Notfallplänen in Zusammenarbeit mit der IT-Abteilung, die Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse beinhalten, mit dem Ziel, die Wahrscheinlichkeit und/oder die Auswirkungen solcher Ereignisse auf ein akzeptables Niveau zu verringern sowie eine möglichst schnelle Wiederherstellung der Verfügbarkeit der informationstechnischen Ressourcen zu erreichen (Business Continuity Management)
- Sicherheitsvorfälle analysieren und deren Behebung koordinieren

7. Verfahrensverantwortliche

Verfahrensverantwortliche sind jene Personen, die über die Verarbeitung von personenbezogenen Daten und / oder Informationen entscheiden. Verfahrensverantwortliche sind in der Regel diejenigen Personen, die aus ihrer Leitungsaufgabe heraus Fachprozesse oder Forschungsaufgaben und in Verbindung damit auch den diesbezüglichen Einsatz der unterstützenden IT-Werkzeuge verantworten.
Die Verantwortung für Datenschutz und Informationssicherheit für die jeweiligen Fachverfahren liegt bei den Verfahrensverantwortlichen. Diese sind vor Inbetriebnahme eines neuen Fachverfahrens (insbesondere auch IT-Verfahren) gegenüber der Stabsfunktion Datenschutz und Informationssicherheit zu benennen. Die Verfahrensverantwortlichen sind Dateneigner für die von ihnen verantworteten Fachprozesse, Informationen, personenbezogenen Daten und dafür eingesetzten IT-Verfahren. Sie sind verantwortlich für die Erstellung der Verfahrensbeschreibungen wie auch der verfahrensspezifischen Datenschutzdokumentation. Sie erhalten in dieser Rolle Unterstützung durch die Stabsfunktion Datenschutz und Informationssicherheit.
Die Verfahrensverantwortlichen stellen sicher, dass die oder der Behördliche Datenschutzbeauftragte frühzeitig in alle datenschutzrelevanten Projekte eingebunden wird.

8. Koordinatorinnen und Koordinatoren für Datenschutz und Informationssicherheit (KoDI)

Die Leitung einer Organisationseinheit ist verantwortlich für die Koordination von Datenschutz und Informationssicherheit (KoDI) im jeweiligen Zuständigkeitsbereich. Die Leitung der Organisationseinheit kann diese Aufgabe delegieren und eine entsprechend qualifizierte Person (sowie ggf. eine Vertretung) gegenüber der Stabsfunktion Datenschutz und Informationssicherheit benennen. Den Koordinatorinnen und Koordinatoren für Datenschutz und Informationssicherheit muss ausreichend Gelegenheit gegeben werden, damit diese ihren Aufgaben fachgerecht nachkommen können. Bei der Benennung ist besonders auf eine personelle Kontinuität zu achten.
Die Aufgaben der Koordinatorinnen und Koordinatoren für Datenschutz und Informationssicherheit bestehen aus folgenden Elementen:

- Erster Ansprechpartner für alle Mitglieder der Organisationseinheit in Fragen des Datenschutzes und der Informationssicherheit
- Unterstützung und Beratung der Leitung der Organisationseinheit in Fragen des Datenschutzes und der Informationssicherheit wie auch über getroffene oder zu treffende Maßnahmen zur Datensicherheit und sicherheitsrelevante Vorfälle
- Hinwirken auf die Einhaltung von Maßnahmen und Regelungen, die dem Schutz personenbezogener Daten, Informationen oder der IT-Systeme dienen
- Meldung von sicherheits- und datenschutzrelevanten Vorfällen in Absprache mit der Leitung der Organisationseinheit
- Teilnahme an regelmäßiger Weiterbildung zu aktuellen Themen des Datenschutzes und der Informationssicherheit
- Mitwirkung bei der Einschätzung von Risiken, sowie Beurteilungen und Umsetzung von Informationssicherheits- und Datenschutzkonzepten

§ 5 Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung im Mitteilungsblatt / Bulletin der HWR Berlin in Kraft.