

Jahrgang **2026**

Nummer **40**

ausgegeben am **14.10.2026**

Verkündungsblatt Hochschule Bielefeld Amtliche Bekanntmachungen

Hinweis für Beschäftigte der Hochschule Bielefeld:
Das gesamte Exemplar finden Sie im Internen Bereich des Webauftritts der Hochschule Bielefeld unter
Amtliche Bekanntmachungen.

Inhalt

Seite

Ausführungsbestimmung für Beschäftigte zum Umgang mit vertraulichen Informationen
an der Hochschule Bielefeld

1239 – 1254

Verteiler:

Präsidentin, Vizepräsident*in I - IV, Vizepräsidentin WP
Dekane der Fachbereiche 1, 2, 3, 4, 5, 6
Büroleiterinnen 1, 2, 3, 4, 5, 6
Hochschulbibliothek
Datenverarbeitungszentrale
Arbeitsstelle für Hochschuldidaktik
Dezernate I, II, III, IV, V, VI
Hochschulkommunikation
Ressort Wissenschaftliche Weiterbildung
Personalrat
Personalrat (wiss.)
Gleichstellungsbeauftragte
Schwerbehindertenvertretung
Datenschutzbeauftragte
Archiv

ASStA (SP und Fachschaftsräte)
Universität Bielefeld
Universität Bielefeld / ZSB – Zentrale Studienberatung

Ausführungsbestimmung für Beschäftigte zum Umgang mit vertraulichen Informationen an der Hochschule Bielefeld

Eigentümer/in	Informationssicherheitsbeauftragte/r
Prüfung durch	IS-Management-Team
Freigabe durch	Präsident/in
Typ	Ausführungsbestimmung
Vertraulichkeitsklasse	Organisationsintern, TLP:GREEN
Status	Zur Freigabe

Inhaltsverzeichnis

1. Einleitung.....	4
2. Geltungsbereich.....	4
3. Bestimmung der Eigentümerschaft.....	4
4. Bestimmung der Vertraulichkeitsklasse	4
5. Kennzeichnung von Informationen	9
6. Übermittlung und Vervielfältigung von Informationen	10
7. Verarbeitung von Informationen auf Datenträgern	13
8. HSBI-Anwendungen und Vertraulichkeitsklassen	14
9. Schlussbemerkung	16
9.1 Behandlung von Ausnahmen	17
9.2 Revision	17
10. Inkrafttreten	17

1. Einleitung

Das Präsidium der Hochschule Bielefeld (HSBI) hat eine „*Richtlinie zum Management der Vertraulichkeit von Informationen*“ verabschiedet. Diese „*Ausführungsbestimmung zum Umgang mit vertraulichen Informationen*“ konkretisiert die Vorgaben der o. g. Richtlinie. Die Konkretisierung erfolgt i. W. durch Praxisbeispiele. Anhand dieser Praxisbeispiele wird aufgezeigt, wie bei typischen Informationen aus dem Arbeitsalltag einer Hochschule die Vertraulichkeitsklasse zu bestimmen ist und welche Implikationen sich daraus für die Kennzeichnung, Übermittlung und Aufbewahrung der klassifizierten Information ergeben.

2. Geltungsbereich

Diese Ausführungsbestimmung ergänzt die *Richtlinie zum Management der Vertraulichkeit von Informationen* und ist für Beschäftigte der HSBI sowie externe Dienstleister/innen verbindlich.

3. Bestimmung der Eigentümerschaft

Die/Der Eigentümer/in ist die Person bzw. Rolle, die für die Steuerung des Lebenszyklus einer Information verantwortlich ist. Üblicherweise ist dies die/der Fach- bzw. Prozessverantwortliche. Folgende Fragen helfen dabei, diese Person/Rolle zu identifizieren:

- Wer entscheidet über Zweck und Mittel der Verarbeitung der Information?
- Wer trägt das fachliche Risiko während der Verarbeitung der Information?
- Wer autorisiert Zugriffe auf die Information?

4. Bestimmung der Vertraulichkeitsklasse

Die HSBI unterscheidet vier Vertraulichkeitsklassen:

- Öffentliche Informationen
- Organisationsinterne Informationen
- Vertrauliche Informationen
- Streng vertrauliche Informationen

Die Zuordnung einer Information zu einer Vertraulichkeitsklasse ist grundsätzlich eine (kontextabhängige) Einzelfallentscheidung und sollte auf Basis einer Schutzbedarfsanalyse getroffen werden (Tritt ein Schaden bei Offenlegung der Information ein? Wenn ja, in welcher Kategorie¹ und in welchem Ausmaß?). Die Verantwortung für die Einstufung liegt bei der Eigentümerin/dem Eigentümer der

¹ Die Gefährdungskategorien finden sich in der Richtlinie zur Durchführung von Risikoanalysen und werden auch in der zu dieser Ausführungsbestimmung zugehörigen Richtlinie aufgegriffen.

Information und der zuständigen Einrichtungs-, Verwaltungs-, Fachbereichs- oder Institutsleitung.

Im Folgenden werden typische HSBI-Datentypen mit ihrer standardmäßigen Zuordnung zu Vertraulichkeitsklassen auf Basis einer generischen Schutzbedarfsanalyse aufgeführt. Abweichungen von diesen Vorgaben sind im Einzelfall zu begründen und zu dokumentieren.

Tab. 4.1: Vertraulichkeitsklassen von typischen „Allgemeinen Organisationsdaten“

Allgemeine Organisationsdaten	Öffentlich	Organisations-intern	Vertraulich	Streng vertraulich
<i>Allgemeine Berichte</i>	Abhängig von konkreten Inhalten			
<i>Allgemeine Servicebeschreibungen (Studienberatung, IT-Services, Bibliotheksangebote etc.)</i>	X			
<i>Aktenplan</i>		X		
<i>Aussonderungslisten</i>		X		
<i>Archivische Bewertungsentscheidungen</i>		X		
<i>Newsletter</i>	Abhängig von konkreten Inhalten			
<i>Öffentliches Vorlesungsverzeichnis</i>	X			
<i>Öffentlicher Veranstaltungskalender</i>	X			
<i>Organigramme</i>	Abhängig von konkreten Inhalten			
<i>Pressemeldungen</i>	X			
<i>Stellenangebote</i>	X			
<i>Studienganginformationen</i>	X			
<i>Werbematerialien (z.B. Flyer)</i>	X			
<i>Zentrale Ansprechpartner/innen</i>	X			

Tab. 4.2: Vertraulichkeitsklassen von typischen „Governance-Daten“

Governance-Daten	Öffentlich	Organisations- intern	Vertraulich	Streng vertraulich
<i>Strategiepläne/ Entwicklungspläne</i>		Abhängig von konkreten Inhalten		
<i>Leitlinien, Leitbilder</i>	X			
<i>Satzungen, Ordnungen</i>	Abhängig von konkreten Inhalten			
<i>Richtlinien</i>		X		
<i>Ausführungsbestimmungen</i>		Abhängig von konkreten Inhalten		
<i>Sitzungsprotokolle</i>		Abhängig von konkreten Inhalten		
<i>Dienstanweisungen</i>		X		
<i>Notfallhandbücher</i>			X	
<i>Geschäftsverteilungspläne</i>		X		
<i>Wahlunterlagen</i>			X	

Tab. 4.3: Vertraulichkeitsklassen von typischen „Personaldaten“

Personaldaten	Öffentlich	Organisations- intern	Vertraulich	Streng vertraulich
<i>Dienstliche Kontaktdaten von Beschäftigten (Telefonnummer, E-Mail, Anschrift)</i>	Je nach Freigabe/Position			
<i>Private Kontaktdaten von Beschäftigten (Telefonnummer E-Mail, Anschrift)</i>			X	
<i>Personalakten</i>			Abhängig von den konkreten Inhalten	
<i>Bewerbungs- und Berufungsunterlagen (Externe Gutachten, Berufungslisten etc.)</i>			X	
<i>Personalratsunterlagen</i>			Abhängig von den konkreten Inhalten	

<i>Schulungsdaten/- ergebnisse</i>			X	
<i>Arbeitszeitchweise</i>			X	

Tab. 4.4: Vertraulichkeitsklassen von typischen „Studierendendaten“

Studierendendaten	Öffentlich	Organisations- intern	Vertraulich	Streng vertraulich
<i>Studierendenstammdaten</i>			Abhängig von den konkreten Inhalten	
<i>E-Mail-Adresse an der Hochschule</i>		X		
<i>Korrigierte Klausuren</i>			X	
<i>Prüfungsprotokolle</i>			X	
<i>Haus-/Seminararbeiten</i>	Je nach Freigabe			
<i>Abschlussarbeiten</i>	Je nach Freigabe			
<i>Ergebnisse von Lernstandkontrollen</i>			X	
<i>Gutachten</i>			X	
<i>Noten(-Übersicht)</i>			X	
<i>Zeugnisse</i>			X	

Tab. 4.5: Vertraulichkeitsklassen von typischen „Finanzdaten“

Finanzdaten	Öffentlich	Organisations- intern	Vertraulich	Streng vertraulich
<i>Angebote</i>			X	
<i>Auftragsbestätigungen</i>			X	
<i>Vertragsentwürfe und Verträge</i>		Abhängig von den konkreten Verträgen		
<i>Haushaltsdaten</i>			X	
<i>Gehaltsdaten</i>			X	
<i>Abrechnungsunterlagen</i>			X	

<i>Drittmittel- und Fördermitteldaten</i>			X	
---	--	--	---	--

Tab. 4.6: Vertraulichkeitsklassen von typischen „Forschungsdaten“

Forschungsdaten	Öffentlich	Organisations-intern	Vertraulich	Streng vertraulich
<i>Forschungsanträge (im Antragsstatus)</i>			Abhängig von konkreten Inhalten	
<i>Forschungsdaten</i>	Abhängig von den konkreten Daten			
<i>Informationen zu unveröffentlichten Patenten</i>				X
<i>Berichte an Fördermittelgeber</i>			X	
<i>Publikationen</i>	Je nach Lizenz			
<i>Gutachten (Peer-Review)</i>			X	
<i>Exportkontrollrelevante Forschungsunterlagen</i>			Abhängig von konkreten Inhalten	
<i>Unterlagen zu Industriekooperationen</i>			X	

Tab. 4.7: Vertraulichkeitsklassen von typischen „Gesundheitsdaten“

Gesundheitsdaten	Öffentlich	Organisations-intern	Vertraulich	Streng vertrauliche
<i>Allgemeine Gesundheitsdaten ohne Detailangaben (Krankmeldungen, Schwerbehinderung, Nachteilsausgleich etc.)</i>			X	
<i>Gesundheitsdaten mit stigmatisierenden Befunden</i>				X
<i>Berufsgenossenschaftliche Verletzungsverfahren</i>			X	
<i>Forschungsdaten aus Studien mit Gesundheitsbezug (nicht anonymisiert)</i>			Abhängig von den konkreten Inhalten	
<i>Ergebnisse arbeitsmedizinischer Untersuchungen</i>			Abhängig von den konkreten Inhalten	

Tab. 4.8: Vertraulichkeitsklassen von typischen „IT- und Infrastrukturdaten“

IT- und Infrastrukturdaten	Öffentlich	Organisations-intern	Vertraulich	Streng vertraulich
Anleitungen	Abhängig von den konkreten Inhalten			
Systemdokumentation/ Betriebshandbücher			X	
Logdaten			X	
Wiederanlaufpläne			X	
Netzwerkpläne			X	
Zugangsdaten (Passwörter, Token, Zertifikate etc.)				X
Gebäude- und Raumpläne	Abhängig von den konkreten Inhalten			
Baupläne			X	
Brandschutzpläne		X		
Flucht- und Rettungspläne	X			
Inventarlisten		Abhängig von den konkreten Inhalten		

5. Kennzeichnung von Informationen

Zur Kennzeichnung der Klassifizierung von Vertraulichkeitsklassen nutzt die HSBI die Symbolik des Traffic Light Protocol 2.0 (TLP) wie folgt:

Tab. 5.1: Kennzeichnung von Informationen nach TLP-Protokoll

Vertraulichkeitsklasse	TLP-Klassifizierung
Öffentlich	TLP:CLEAR
Organisationsintern	TLP:GREEN
Vertraulich	TLP:AMBER

Streng vertraulich

TLP:RED

Alternativ können auch die entsprechenden Bezeichnungen („Öffentlich“, „Organisationsintern“, „Vertraulich“, „Streng vertraulich“) verwendet werden.

Als „Öffentlich“ eingestufte Informationen müssen nur dann gekennzeichnet werden, wenn aus dem Inhalt und/oder dem Ablageort nicht unmittelbar ersichtlich ist, dass es sich um eine öffentliche Information handelt.

Bei „vertraulichen“ und „streng vertraulichen“ Informationen kann eine zeitliche Beschränkung der Vertraulichkeitsklasse vermerkt werden, wobei in diesem Fall anzugeben ist, auf welche Vertraulichkeitsklasse die Information zurückfällt.

Zusätzlich können bei „vertraulichen“ und „streng vertraulichen“ Informationen (z. B. auf der Titelseite) die Hinweise „COPY FORBIDDEN/KOPIEREN VERBOTEN“ und „COPYING WILL LEAD AUTOMATICALLY TO LEGAL CONSEQUENCES AND IS FORMALLY FORBIDDEN“ bzw. „KOPIEREN FÜHRT AUTOMATISCH ZU RECHTLICHEN KONSEQUENZEN UND IST AUSDRÜCKLICH VERBOTEN“ vermerkt werden.

Je nach Speicher-/Übermittlungsmedium und Vertraulichkeitsklasse gelten folgende Vorgaben für die Kennzeichnung.

Tab. 5.2: Anforderungen an die Kennzeichnung von Informationen nach Medium

	Öffentlich	Organisations- intern	Vertraulich	Streng vertraulich
<i>Dokumente (analog/ digitalisiert)</i>	Titelseite, alle folgenden Seiten Fußzeile	Titelseite, alle folgenden Seiten Fußzeile	Titelseite, alle folgenden Seiten Fußzeile	Titelseite, alle folgenden Seiten Fußzeile
<i>E-Mail</i>	keine Kennzeichnung erforderlich	Funktion des E-Mail- Programms oder in Klammern im Betreff	Sofern zulässig die Funktion des E-Mail-Programms oder in Klammern im Betreff	Sofern zulässig die Funktion des E-Mail-Programms oder in Klammern im Betreff
<i>Messenger</i>	keine Kennzeichnung erforderlich	Hinweis bei externen Empfängern erforderlich	Hinweis erforderlich	Sofern zulässig ist ein Hinweis erforderlich
<i>Verbal</i>	kein Hinweis erforderlich	Hinweis bei externen Empfängern erforderlich	Hinweis erforderlich	Hinweis erforderlich

6. Übermittlung und Vervielfältigung von Informationen

Grundsätzlich ist bei der Übermittlung von Informationen zwischen interner und externer Übermittlung zu unterscheiden. Um eine interne Übermittlung handelt es sich, wenn Absender/in und Empfänger/in beide Hochschulangehörige der HSBI sind. Um

eine externe Übermittlung handelt es sich, wenn Absender/in oder Empfänger/in nicht Hochschulangehörige der HSBI sind.

Die Übermittlung öffentlicher Informationen ist prinzipiell zulässig und unterliegt keinen spezifischen Anforderungen. Für nicht-öffentliche Informationen gelten in Bezug auf die Übermittlung folgende Grundprinzipien:

Tab. 6.1: Grundprinzipien der Übermittlung von nicht-öffentlichen Informationen

	Organisationsintern	Vertraulich	Streng vertraulich
<i>Interne Übermittlung</i>	in notwendigem Umfang	Kenntnis nur, wenn im Rahmen der Tätigkeit erforderlich Andernfalls nur mit Zustimmung durch den/die Eigentümer/in	Nur mit Zustimmung durch die/den Eigentümer/in an einen vorab definierten, stark eingeschränkten Personenkreis
<i>Externe Übermittlung</i>	Kenntnis nur, wenn im Rahmen der Tätigkeit erforderlich	Kenntnis nur, wenn im Rahmen der Tätigkeit erforderlich	Nur mit Zustimmung durch die/den Eigentümer/in

Bei streng vertraulichen Informationen ist die persönliche Überbringung immer vorzuziehen.

Je nach Medium gelten für die Übermittlung und Vervielfältigung von nicht-öffentlichen Informationen folgende Vorgaben:

Tab. 6.2: Anforderungen an die Übermittlung/Vervielfältigung von nicht-öffentlichen Informationen nach Medium

	Organisationsintern	Vertraulich	Streng vertraulich
<i>mündlich</i>	Nur zulässig, wenn keine Unberechtigten mithören können	Nur zulässig, wenn keine Unberechtigten mithören können	Nur zulässig, wenn keine Unberechtigten mithören können
<i>fernmündlich (Telefon, Videokonferenz)</i>	Nur zulässig, wenn keine Unberechtigten mithören können.	Nur zulässig, wenn keine Unberechtigten mithören können. Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln und die Identität des Empfängers ist sicherzustellen. Informationen nicht auf Anrufbeantworter oder Voicemailbox hinterlassen sowie keine	Nur zulässig, wenn keine Unberechtigten zuhören können. Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln und die Identität des Empfängers ist sicherzustellen. Informationen nicht auf Anrufbeantworter oder Voicemailbox hinterlassen sowie keine

		Sprachnachrichten versenden	Sprachnachrichten versenden
<i>E-Mail (intern)</i>	Ohne Einschränkungen zulässig	Der Inhalt ist zu verschlüsseln.	Der Inhalt ist zu verschlüsseln.
<i>E-Mail (extern)</i>	An berechnigte Empfänger unter Hinweis auf Regeln der Weitergabe für die Information zulässig	Der Inhalt ist zu verschlüsseln.	Der Inhalt zu verschlüsseln
<i>E-Mail-Verteiler (intern)</i>	Ohne Einschränkungen zulässig	Nicht zulässig	Nicht zulässig
<i>Postweg (intern)</i>	Ohne Einschränkungen zulässig	Mit verschlossenem und undurchsichtigem Umschlag zulässig	Mit verschlossenem und undurchsichtigem Umschlag mit Versiegelung (z.B. Stempel) zulässig Zusatz „persönlich“ bei Anschrift hinzufügen
<i>Postweg (extern)</i>	Als normaler Brief zulässig	Als normaler Brief mit dem Zusatz „persönlich“ bei Empfänger zulässig	Als Einschreiben oder Kuriersendung mit dem Hinweis „nur persönliche Übergabe“ zulässig
<i>Messenger (intern)</i>	Der Inhalt der Nachricht ist Ende-zu- Ende zu verschlüsseln.	Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln. Die Identität des Empfängers ist sicherzustellen.	Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln und die Identität des Empfängers ist sicherzustellen
<i>Messenger (extern)</i>	Der Inhalt der Nachricht ist Ende-zu- Ende zu verschlüsseln und die Identität des Empfängers ist sicherzustellen	Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln und die Identität des Empfängers ist sicherzustellen	Nicht zulässig
<i>Ausdruck</i>	Ohne Einschränkungen zulässig	Nur unter Beaufsichtigung des Vervielfältigungsvorgangs zulässig	Nur nach Freigabe durch die/den Informationseigentümer/in und unter Beaufsichtigung des Vervielfältigungsvorgangs zulässig

<i>Fax (intern)</i>	Ohne Einschränkungen zulässig	Nicht zulässig	Nicht zulässig
<i>Fax (extern)</i>	Nur nach Vorankündigung beim Empfänger zulässig Deckblatt mit Anzahl der Seiten mitversenden	Nicht zulässig	Nicht zulässig
<i>Transport (Dokumente, Datenträger, Dienstgeräte)</i>	in verschlossener Tasche	in verschlossener Tasche	in abgeschlossener Tasche

7. Verarbeitung von Informationen auf Datenträgern

Für die Ablage bzw. Speicherung öffentlicher Informationen auf Datenträgern bestehen keine Vorgaben. In Bezug auf nicht-öffentliche Informationen gelten je nach Vertraulichkeitsklasse und unter Beachtung der Berechtigungseinstellungen folgende Vorgaben.

Tab. 7: Anforderungen für die Speicherung von nicht-öffentlichen Informationen auf Datenträgern

	Organisationsintern	Vertraulich	Streng vertraulich
Papierdokumente	für Unbefugte nicht einsehbar in Schränken und Regalen	für Unbefugte unzugänglich in abschließbaren Schränken zugangsbeschränkte Lagerräume	Dauerhaft unter Verschluss in abschließbaren Schränken oder Tresoren zugangsbeschränkte Lagerräume
Private Endgeräte	außer im Rahmen von Ausnahmeregelungen nicht auf Privatgeräten speichern		
Dienstgeräte	Nur bei Verschlüsselung des Datenträgers zulässig	Nur bei Verschlüsselung des Datenträgers zulässig	Nur bei Verschlüsselung des Datenträgers sowie zusätzlicher Verschlüsselung der Inhalte zulässig
Mobile Datenträger	Nur bei Verschlüsselung des Datenträgers zulässig	Nur bei Verschlüsselung des Datenträgers zulässig	Nur bei Verschlüsselung des Datenträgers sowie zusätzlicher

			Verschlüsselung der Inhalte zulässig
--	--	--	--------------------------------------

8. HSBI-Anwendungen und Vertraulichkeitsklassen

Dienstlich bzw. studienbezogen verarbeitete Hochschuldaten dürfen ausschließlich in von der DVZ freigegebenen Anwendungen verarbeitet werden.

Die folgende Tabelle bietet einen Überblick über zentrale Anwendungen der HSBI und gibt an, welche Vertraulichkeitsklassen von Informationen auf diesen Systemen verarbeitet werden dürfen, sofern die Zugriffsrechte jeweils so eingestellt sind, dass nur autorisierte Personen Zugriff erhalten.

Für einige Anwendungen ist vor der Verarbeitung bestimmter Informationen die Umsetzung zusätzlicher Sicherheitsmaßnahmen erforderlich (z. B. die Verschlüsselung von E-Mails in Exchange Online beim Versand vertraulicher oder streng vertraulicher Inhalte).

Wichtig:

Bei der Verarbeitung personenbezogener Daten muss stets ein konkreter Verarbeitungszweck vorliegen. Dass eine Anwendung für die Verarbeitung vertraulicher Informationen zugelassen ist, bedeutet nicht automatisch, dass dort alle Arten vertraulicher personenbezogener Daten verarbeitet werden dürfen.

Dies wird etwa am Beispiel der E-Learning-Plattform ILIAS deutlich: Dort ist die Verarbeitung vertraulicher Informationen grundsätzlich zulässig. Vertrauliche Finanzdaten, Bewerbungsdaten, Gesundheitsdaten dürfen beispielsweise auf ILIAS jedoch nicht verarbeitet werden, da es nicht dem Verarbeitungszweck der Plattform entspricht, entsprechende Daten zu verarbeiten.

Tab. 8: Zulässige Vertraulichkeitsklassen nach zentralen Anwendungen

	Organisationsintern	Vertraulich	Streng vertraulich
Adobe Creative Cloud	Zulässig	Zulässig (Inhalt verschlüsseln)	Nicht zulässig
CAT	Zulässig	Zulässig	Zulässig
Cisco Webex (Meeting)	Zulässig	Zulässig	Zulässig (Verwendung der Secured Pro Meeting Vorlage erforderlich)
Cisco Webex (Softphone)	Zulässig	Zulässig	Nur interne Anrufe zulässig

		(keine Sprachnachrichten auf Anrufbeantworter)	(keine Sprachnachrichten auf Anrufbeantworter)
Cisco Webex (Messenger)	Zulässig	Zulässig	Nur interne Übermittlung zulässig
Conceptboard	Zulässig (Beim Teilen bzw. Freigeben von Boards über einen Link muss ein Passwort gesetzt werden.)	Nicht zulässig	Nicht zulässig
Dokumentenmanagementsystem (DMS)	Zulässig	Zulässig	Zulässig
DVZ-Survey	Zulässig	Nicht zulässig bei Erstellung der Umfrage. Bei personenbezogenen Daten nur pseudonymisiert in Antworten der Befragten zulässig.	Nicht zulässig bei Erstellung der Umfrage. Bei personenbezogenen Daten nur anonymisiert in Antworten der Befragten zulässig.
Exchange Online	Zulässig	Zulässig (Verschlüsselung der Inhalte erforderlich)	Zulässig (Verschlüsselung der Inhalte erforderlich)
F4transkript (Online-Transkription)	Zulässig	Bei personenbezogenen Daten nur pseudonymisiert zulässig.	Nicht zulässig
HSBI-Intranet	Zulässig	Mit Ausnahmeregelungen möglich	Nicht zulässig
HSBIKI Chat	Zulässig	Nicht zulässig	Nicht zulässig
HSBI-Netzlaufwerk	Zulässig	Zulässig	Zulässig (Verschlüsselung der Inhalte erforderlich)
ILIAS (E-Assessment)	Zulässig	Zulässig	Nicht zulässig
ILIAS (E-Learning)	Zulässig	Zulässig	Nicht zulässig
KI-Connect	Zulässig	Nicht zulässig	Nicht zulässig
LSF	Zulässig	Zulässig	Nicht zulässig
MACH	Zulässig	Zulässig	Nicht zulässig

MAXQDA (Online-Version)	Zulässig	Bei personenbezogenen Daten nur pseudonymisiert zulässig	Nicht zulässig
Medienportal	Zulässig	Zulässig bei Einschränkung auf autorisierten Personenkreis	Nicht zulässig
Sciebo-Cloud	Zulässig Beim Teilen bzw. Freigeben von Dateien und Ordern über einen Link muss ein Passwort gesetzt werden.	Zulässig 2FA muss aktiviert sein und Freigabe nur direkt an autorisierte Personen	Nicht zulässig
SVA	Zulässig	Zulässig	Zulässig
Zoom X (Meeting)	Zulässig	Zulässig	Zulässig (Aktivierung von E2E mit lokal gespeichertem privatem Schlüssel erforderlich)
Zoom X (Messenger)	Zulässig	Zulässig	Nur interne Übermittlung zulässig

9. Entsorgung und Vernichtung von Informationen

Für die Vernichtung und Entsorgung öffentlicher Informationen bestehen keine Vorgaben. In Bezug auf nicht-öffentliche Informationen gelten nach erfolgter archivischer Vernichtungsfreigabe je nach Vertraulichkeitsklasse folgende Vorgaben.

Tab. 9: Vernichtung von Unterlagen und Datenträgern nach Vertraulichkeitsklasse

	Organisationsintern	Vertraulich	Streng vertraulich
Vernichtung von Unterlagen	Aktenvernichter (P2) ² oder Datenschutzbehälter	Aktenvernichter (P3) oder Datenschutzbehälter	Aktenvernichter (P3) oder Datenschutzbehälter
Rücksendung von Datenträgern an Lieferanten	nur nach zertifizierter Löschung		
Entsorgung von HSBI-Datenträgern	Entsorgung ausschließlich über die DVZ		

² Hierbei handelt es sich um Schutzklassen nach ISO/IEC 21964.

10. Schlussbemerkung

10.1 Behandlung von Ausnahmen

Ausnahmen von den Vorgaben dieser Ausführungsbestimmung müssen durch einen begründeten Ausnahmeantrag bei der/dem Eigentümer/in gestellt werden.

10.2 Revision

Diese Ausführungsbestimmung wird regelmäßig, jedoch mindestens einmal pro Jahr, durch die/den Eigentümer/in auf Aktualität und Konformität geprüft und bei Bedarf angepasst.

11. Inkrafttreten

Diese Ausführungsbestimmung tritt zum 10.09.2026 in Kraft.

Bielefeld, den 10.09.2026

gez. I. Schramm-Wölk

Prof. Dr. Ingeborg Schramm-Wölk