Über den Umgang mit Anfragen Dritter nach personenbezogenen Daten an der H-BRS

Handreichung für Beschäftigte in Forschung, Lehre und Verwaltung

1. Zweck der Handreichung

Diese Handreichung regelt den Umgang mit Anfragen Dritter nach personenbezogenen Daten an der Hochschule.
Sie richtet sich an alle Beschäftigten in Forschung, Lehre und Verwaltung, die mit personenbezogenen Daten umgehen und daher für die Sicherstellung des Datenschutzes verantwortlich sind.

Ziel ist es, Datenschutzverstöße zu vermeiden, Handlungssicherheit zu schaffen und ein einheitliches Vorgehen bei internen und externen Anfragen sicherzustellen.

2. Begriffsbestimmungen

2.1 Einfache personenbezogene Daten nach Art. 4 Nr. 1 DSGVO

Einfache personenbezogene Daten (Art. 4 Nr. 1 DSGVO) sind laut DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu zählen insbesondere:

- Name, Adresse, E-Mail-Adresse, Telefonnummer (dienstlich oder privat)
- Personenkennungen wie Matrikelnummer, Bibliotheksnummer, Campus-ID
- Prüfungsleistungen, Noten, Teilnahme- und Anwesenheitsdaten
- Bewerbungs-, Vertrags- und Personalunterlagen
- Fotos, Video- oder Audioaufzeichnungen
- Inhalte dienstlicher Kommunikation

2.2 Sensible personenbezogene Daten nach Art. 9 DSGVO

Sensible personenbezogener Daten (oder auch „personenbezogene Daten besonderer Kategorien“ im Sinne von Art. 9 DSGVO) sind laut DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen **und** aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie:

- Gesundheitsdaten (z. B. Atteste, Behinderungen, Krankheitszeiten),
- Biometrische Daten zur eindeutigen Identifizierung,
- Daten zum Sexualleben oder der sexuellen Orientierung.

Diese Daten unterliegen aufgrund ihrer Sensibilität erhöhten Schutzanforderungen und dürfen nur in begründeten Ausnahmefällen und unter strikter Einhaltung der Datenschutzvorgaben weitergegeben werden. Im Zweifel ist vorab der Datenschutzreferent an der Stabsstelle Recht und Compliance hinzuzuziehen.

Hinweis: Auch Informationen über die Religionszugehörigkeit (z.B. für die Kirchensteuer in Personalakten) fallen unter die sensiblen personenbezogenen Daten.

2.3 Rechtsgrundlage

Eine Rechtsgrundlage ist die rechtliche Erlaubnis, personenbezogene Daten zu verarbeiten. Ohne eine solche Grundlage dürfen personenbezogene Daten grundsätzlich weder erhoben, gespeichert, genutzt noch an Dritte übermittelt werden.
Für öffentliche Hochschulen ergeben sich Rechtsgrundlagen insbesondere aus:

- gesetzlichen Vorschriften (z. B. DSGVO, Hochschulgesetz NRW, Spezialgesetze),
- Rechtsverordnungen oder Satzungen,
- Dienstvereinbarungen,
- Beschlüssen zuständiger Hochschulgremien,
- dienstlichen Weisungen im Rahmen gesetzlicher Aufgaben,
- Einwilligungen der betroffenen Person.

Die Rechtsgrundlage bestimmt zugleich Zweck, Umfang und Grenzen der jeweiligen Datenverarbeitung. Wenn keine klare Rechtsgrundlage für die Verarbeitung oder Nutzung personenbezogener Daten besteht, dürfen diese Daten auch nicht an Dritte weitergegeben werden.

2.4 „Dritte“

Dritte i.S.d. Handreichung sind alle anfragenden Personen, die nicht nach ihren eigenen personenbezogenen Daten fragen, insbesondere:

- Studierende untereinander
- Beschäftigte anderer Gliederungen
- Eltern, Angehörige
- Externe Stellen (z. B. Behörden, Rechtsanwält:innen, Dienstleister)

2.5 Abgrenzung zu Auskunftsersuchen nach Art. 15 DSGVO

Möchte eine Person (z. B. ein:e Studierende:r oder ein:e Kolleg:in) Auskunft über die eigenen, von der H-BRS verarbeiteten personenbezogenen Daten erhalten (Auskunftsrecht der betroffenen Person nach Art. 15 DSGVO), fällt dies in die Zuständigkeit des operativen Datenschutzes (Datenschutzreferent). Bitte leiten Sie solche Anfragen zum operativen Datenschutz weiter und geben Auskunft nicht selbst.

3. Öffentlich zugängliche Dienstdaten

Im Gegensatz zu privaten Daten Dritter gibt es Informationen über Beschäftigte der Hochschule, die im Rahmen der Transparenzpflichten (z.B. nach dem Informationsfreiheitsgesetz NRW) grundsätzlich ohne Einwilligung veröffentlicht und weitergegeben werden dürfen.

Folgende Dienstdaten von Beschäftigten dürfen (und sollen) offen kommuniziert werden:

- Vor- und Zuname sowie Titel und akademische Grade,
- Berufs- und Funktionsbezeichnung und
- dienstliche Kontaktdaten: Büroanschrift, Rufnummer und dienstliche E-Mail-Adresse.

Ausnahmefälle: Bestehen im Einzelfall schwerwiegende Gründe (z. B. eine nachgewiesene Gefährdung für Leben oder Gesundheit einer Person), kann die Veröffentlichung dieser Daten unterbleiben. Solche Ausnahmen sind über das Justiziariat oder den Datenschutz zu klären.

Wichtige Einschränkung: Dies gilt **niemals** für Privatanschriften, private Telefonnummern oder private E-Mail-Adressen.

4. Grundsatz der Datenweitergabe

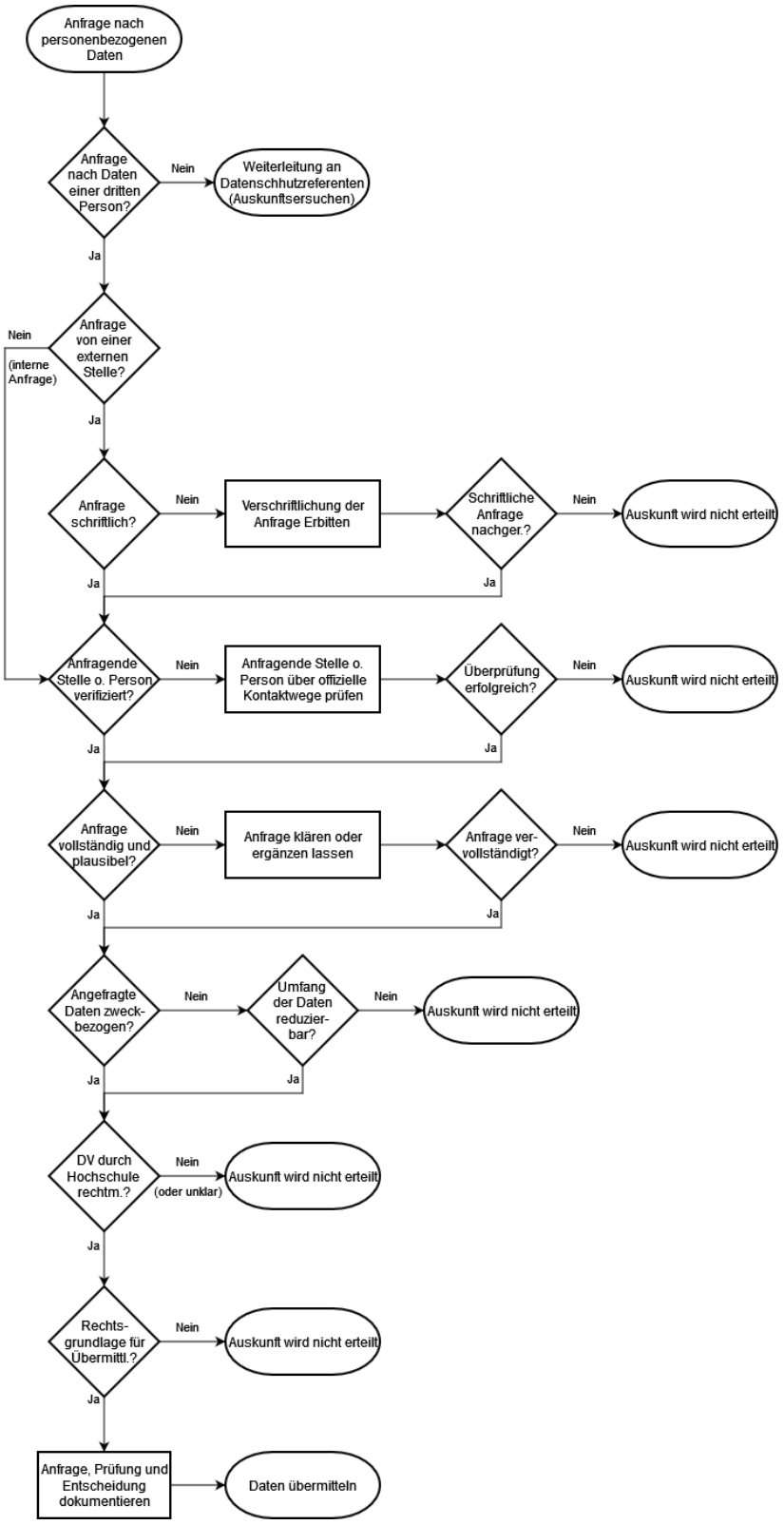
Personenbezogene Daten dürfen an Dritte nur weitergegeben werden, wenn hierfür eine eindeutige datenschutzrechtliche Rechtsgrundlage besteht.

Eine Datenweitergabe ist insbesondere dann nicht zulässig, wenn sie allein aus Zeitdruck, bloßem dienstlichem oder gar privatem Interesse, langjähriger Praxis oder informellen Absprachen erfolgt.

Es gilt stets: keine Herausgabe ohne Prüfung.

5. Prüfung von Anfragen

Der folgende Entscheidungsbaum dient als erste Orientierung, ob personenbezogene Daten an Dritte herausgegeben werden dürfen. Er fasst die wichtigsten Prüfschritte dieser Handreichung in vereinfachter Form zusammen.



Für eine vollständige und dokumentierte Prüfung empfiehlt sich die Nutzung der Checkliste in Anhang II, die alle Prüfschritte dieser Handreichung systematisch zusammenfasst.

Schritt 1: Einordnung der Anfrage
Zunächst ist zu klären:

- Handelt es sich um eine interne oder externe Anfrage?
- Wer stellt die Anfrage (Organisationseinheit, Behörde, Privatperson)?
- Welche personenbezogenen Daten sind konkret betroffen?
- Erfolgt die Anfrage nach personenbezogenen Daten durch die betroffene Person selbst? (Auskunftsersuchen nach Art. 15 DSGVO)

Schritt 2: Form und Kommunikationsweg der Anfrage
In diesem Schritt geht es ausschließlich darum, auf welchem Weg eine Anfrage die Hochschule erreichen muss, um geprüft werden zu können. Die Wahl des sicheren **Antwortweges** erfolgt erst nach positiver Prüfung (siehe Punkt 6).

Externe Anfragen
Anfragen externer Stellen (z. B. Behörden, Rechtsanwält:innen, Privatpersonen) müssen grundsätzlich schriftlich bzw. in Textform erfolgen, z. B. per Brief, per Fax oder per E-Mail. Telefonische Auskunftsersuchen externer Stellen werden nicht beantwortet.

Zielen Anfragen erkennbar auf besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) ab, ist bei der Bearbeitung besondere Vorsicht geboten. Sollten solche Anfragen über unsichere Kanäle (z. B. unverschlüsselte E-Mail) eingehen, ist dies intern zu dokumentieren. Die Rückmeldung oder Datenherausgabe durch die Hochschule darf in diesen Fällen keinesfalls über den unsicheren Eingangskanal erfolgen, sondern muss über besonders sichere Wege (z. B. Briefpost oder beBPo) abgewickelt werden.

Interne Anfragen
Telefonische Anfragen zwischen Beschäftigten der Hochschule können zulässig sein, sofern

- die Identität der anfragenden Person zweifelsfrei feststeht,
- die Auskunft für die dienstliche Aufgabenerfüllung erforderlich ist,
- keine besonderen Kategorien personenbezogener Daten betroffen sind und
- der Umfang der Auskunft auf das notwendige Minimum beschränkt bleibt.

Bei sensiblen Sachverhalten (private Kontaktdaten von Betroffenen oder gar personenbezogene Daten nach Art. 9 DSGVO, s.o.) ist die Anfrage auf einen schriftlichen Kommunikationsweg zu verlagern.

Schritt 3: Verifikation der anfragenden Stelle oder Person
Es ist sicherzustellen, dass die anfragende Stelle oder Person tatsächlich diejenige ist, für die sie sich ausgibt. Dabei ist insbesondere zu prüfen:

- Ist die anfragende Organisationseinheit, Behörde oder Institution bekannt und existent?
- Ist die anfragende Person dort tatsächlich tätig bzw. zur Anfrage befugt?
- Stimmen die verwendeten Kontaktinformationen mit offiziellen Quellen überein?

Bei internen Anfragen ist sicherzustellen, dass die Identität der anfragenden Person zweifelsfrei feststeht (z. B. bekannte dienstliche Telefonnummer, bekannte E-Mail-Adresse).

Bei externen Anfragen ist im Zweifel eine Verifikation über offizielle Kontaktwege vorzunehmen. Die in der Anfrage angegebenen Kontaktdaten dürfen hierfür nicht ungeprüft verwendet werden.

Wenn die Identität oder Berechtigung der anfragenden Person nicht eindeutig festgestellt werden kann, dürfen keine personenbezogenen Daten herausgegeben werden.

Schritt 4: Plausibilität prüfen

Im Anschluss ist zu prüfen, ob die Anfrage inhaltlich nachvollziehbar und schlüssig ist. Dabei ist insbesondere zu prüfen:

- Ist der Zweck der Anfrage plausibel?
- Passt die Art der angefragten Daten zum Zweck?
- Besteht ein sachlicher Zusammenhang zwischen Anfrage und Aufgabe?

Im Zweifel gilt stets: Lieber eine Anfrage hinterfragen, als personenbezogene Daten unrechtmäßig weitergeben.

Schritt 5: Vollständigkeit der Anfrage prüfen

Eine prüffähige Anfrage muss mindestens folgende Angaben enthalten:

- Name und Kontaktdaten der anfragenden Person
- Organisation / Behörde / Organisationseinheit
- ggf. Aktenzeichen oder Referenznummer
- konkrete Beschreibung der angeforderten Daten
- Zweck der Datenverwendung
- Angabe der geltend gemachten Rechtsgrundlage
  (z. B. gesetzliche Befugnis, behördliche Anordnung, Einwilligung, dienstliche Aufgabenerfüllung)

Fehlen diese Angaben, ist eine rechtliche Bewertung nicht möglich. Die Anfrage ist zu klären oder zu ergänzen.

Schritt 6: Art und Umfang der Daten prüfen

- Welche Daten sollen konkret herausgegeben werden?
- Handelt es sich um einfache personenbezogene Daten oder besondere Kategorien?
- Stehen die angeforderten Daten in einem sachlichen Zusammenhang mit dem angegebenen Zweck?
- Ist der Umfang erforderlich oder unverhältnismäßig?

Es gilt stets der Grundsatz der Datenminimierung.

Schritt 7: Zulässigkeit der Datenverarbeitung durch die Hochschule prüfen
Vor einer Weitergabe personenbezogener Daten ist zu prüfen, ob deren Erhebung und Verarbeitung durch die Hochschule selbst rechtmäßig erfolgt.

Die Hochschule darf nur solche Daten übermitteln, die sie auf einer zulässigen Rechtsgrundlage im Sinne von Abschnitt 2.3 verarbeitet.

Dabei sollte insbesondere Klarheit über folgende Punkte bestehen:

- **Rechtsgrundlage der Verarbeitung**
  Auf welcher Grundlage werden die Daten erhoben und verarbeitet? (z. B. gesetzliche Vorschriften, hochschulrechtliche Regelungen, Dienstvereinbarungen, Satzungen, Beschlüsse von Hochschulgremien oder Einwilligungen)
- **Zweckbindung der Datenverarbeitung**
  Erfolgt die Verarbeitung der Daten zu dem Zweck, für den sie ursprünglich erhoben wurden?
- **Umfang und Nutzung der Daten**
  Ist die konkrete Verarbeitung innerhalb der Organisationseinheit (Art und Umfang der Daten sowie deren Speicherdauer) von der jeweiligen Rechtsgrundlage gedeckt?

Wenn die Rechtmäßigkeit der Datenverarbeitung unklar ist, dürfen die Daten nicht herausgegeben werden, bis die Zulässigkeit geklärt wurde.

Schritt 8: Rechtsgrundlage der Übermittlung bewerten
Auch die Übermittlung personenbezogener Daten an Dritte stellt eine eigene Verarbeitung dar und erfordert daher eine gesonderte Rechtsgrundlage.

Eine Herausgabe personenbezogener Daten kommt insbesondere in Betracht bei:

- Gesetzlicher Verpflichtung oder behördlicher bzw. gerichtlicher Anordnung (Art. 6 Abs. 1 lit. c DSGVO)
- Wirksamer Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a DSGVO)
- Erforderlichkeit zur Wahrnehmung einer Aufgabe der Hochschule im öffentlichen Interesse (Art. 6 Abs. 1 lit. e DSGVO)

Bestehen Zweifel an der Rechtmäßigkeit der Anfrage, ist keine Herausgabe vorzunehmen. Die bloße Behauptung eines Dritten, ein Recht auf die Daten zu haben, genügt nicht als Rechtsgrundlage.

Personenbezogene Daten dürfen nur dann an Dritte weitergegeben werden, wenn **alle Prüfschritte dieser Handreichung positiv** abgeschlossen wurden.

Sollte einer der Prüfschritte negativ ausfallen oder bestehen **Zweifel**, insbesondere an der Identität der anfragestellenden Person, der Zulässigkeit oder dem Umfang einer Anfrage, dürfen **keine personenbezogenen Daten herausgegeben** werden.

Bei Unsicherheiten kann jederzeit der Datenschutzreferent an der Stabsstelle Recht und Compliance (siehe Punkt 8) hinzugezogen werden.

6. Herausgabe und Übermittlung der Daten

Die Wahl des Übermittlungsweges orientiert sich am Risiko für die betroffene Person. Ziel ist es, den Verwaltungsaufwand gering zu halten, ohne die Datensicherheit zu gefährden.

6.1 Grundsatz der Datensparsamkeit

Geben Sie nur die Daten heraus, die zur Erfüllung des angegebene Zwecks zwingend erforderlich sind.

Einfache Bestätigungen (z. B. Studienzeiten) an verifizierte Empfänger (z. B. Behörden, nachgewiesene Betreuer) können per einfacher E-Mail erfolgen, sofern keine schutzwürdigen Interessen der betroffenen Person entgegenstehen.

In Dokumenten sind alle Informationen, die nicht Gegenstand der Anfrage sind (z. B. Noten der Studierenden auf einer Liste), vor Herausgabe zu schwärzen.

6.2 Wahl des Übermittlungsweges

Je nach Sensibilität der Daten und Vertrauenswürdigkeit des Empfängers kommen unterschiedliche Wege in Betracht:

- **Einfache Bestätigungen an verifizierte Empfänger:**
  Handelt es sich um unkritische Daten (z. B. bloße Bestätigung von Studienzeiten oder Immatrikulationsstatus) und ist die Identität sowie Legitimation des Empfängers (z. B. Behörde, gerichtlich bestellte Betreuer) bereits zweifelsfrei nachgewiesen, kann die Antwort per einfacher E-Mail erfolgen.
- **Interne Übermittlung:**
  Innerhalb der Hochschule ist der Versand per E-Mail zulässig, sofern die Auskunft für die dienstliche Aufgabenerfüllung erforderlich ist.
- **Sensible Daten & Besondere Kategorien (Art. 9 DSGVO):**
  Daten mit hohem Schutzbedarf (z. B. Gesundheitsdaten, Notenübersichten, Anschriften bei Gefahr im Verzug) dürfen nicht unverschlüsselt per E-Mail versendet werden. Hier ist zwingend der Postweg, eine verschlüsselte Datei (z. B. passwortgeschütztes ZIP) oder ein gesicherter Behördenzugang (beBPo) zu nutzen.

6.3 Verbot privater Kommunikationsmittel

Die Nutzung privater E-Mail-Accounts, privater Messenger-Dienste oder privater Cloud-Speicher für die Übermittlung dienstlicher Daten ist strikt untersagt.

7. Dokumentation

Jede Anfrage und deren Bearbeitung sind nachvollziehbar zu dokumentieren.
Mindestens festzuhalten sind:

- Datum der Anfrage
- anfragende Stelle und Ansprechpartner:in
- Zweck und Rechtsgrundlage

- Umfang der herausgegebenen oder verweigerten Daten
- Art der Übermittlung

8. Unterstützung und Beratung

Bei Unsicherheiten oder komplexen Sachverhalten wenden Sie sich bitte an die **Stabstelle Recht und Compliance:** Manfred Höffken (Datenschutzreferent).

9. Abschließender Hinweis

Im Zweifel keine Daten herausgeben, sondern Unterstützung oder Beratung einholen.

Diese Handreichung soll Beschäftigte unterstützen, nicht ersetzen.
Sorgfalt, Nachfragen und Dokumentation sind ausdrücklich erwünscht.

Anhang I: Typische Anfragesituationen und Entscheidungshilfen

Praxisbeispiele für häufige Anfragen nach personenbezogenen Daten und deren datenschutzrechtliche Bewertung.

Szenario A: Die besorgten Eltern

- **Situation:** Ein Vater ruft an und möchte wissen, ob seine Tochter zur Prüfung erschienen ist, da er die Studiengebühren zahlt.
- **Entscheidung:** Ablehnung. Auch die Zahlung von Gebühren begründet kein Auskunftsrecht. Volljährige Studierende verwalten ihre Daten selbst.
- **Vorgehen:** Verweisen Sie den Vater direkt an seine Tochter.

Szenario B: Amtshilfe durch die Polizei

- **Situation:** Die Polizei bittet telefonisch um die Privatadresse eines Dozenten wegen einer Zeugenbefragung.
- **Entscheidung:** Hinterfragen. Am Telefon erfolgt keine Auskunft.
- **Vorgehen:** Bitten Sie um eine schriftliche Anfrage mit Angabe des Aktenzeichens und der Rechtsgrundlage (Amtshilfe).

Szenario C: Interne Recherche

- **Situation:** Eine Kollegin aus einer anderen Gliederung benötigt Daten für eine statistische Auswertung der Hochschule.
- **Entscheidung:** Prüfung der Erforderlichkeit. Besteht ein dienstlicher Auftrag für diese Statistik?
- **Vorgehen:** Geben Sie Daten nur im notwendigen Umfang weiter – idealerweise anonymisiert oder pseudonymisiert, sofern dies für den Zweck ausreicht.

Szenario D: Gesetzliche Betreuer (z. B. für Rentenversicherungszwecke)

- **Anfrage:** Ein Betreuer benötigt Studienzeiträume zur Meldung an die Rentenversicherung.
- **Entscheidung:** Eine Auskunft ist zulässig, sofern die Legitimation zweifelsfrei nachgewiesen ist.

- **Voraussetzung:** Der Betreuer muss seine Bestellungsurkunde (vom Betreuungsgericht) im Original oder als beglaubigte Kopie nachweisen. Achten Sie auf Plausibilität und Anzeichen für Fälschungen.

Szenario E: Verdacht auf Urkundenfälschung (z. B. durch das Studierendenwerk)

- **Anfrage:** Das Studierendenwerk bittet um Bestätigung, ob eine eingereichte Studienbescheinigung echt ist.

- **Entscheidung:** Restriktive Auskunft. Der Schutz personenbezogener Daten geht vor.

- **Vorgehen:** Bestätigen Sie keine konkreten persönlichen Details der betroffenen Person. Zulässig ist allenfalls der allgemeine Hinweis, dass eine Matrikelnummer nicht zum offiziellen Nummernkreis der Hochschule gehört oder das Dokument formale Fehler aufweist.

Szenario F: Interne Ermittlung durch Lehrende (z. B. bei Plagiatsverdacht)

- **Anfrage:** Ein Professor fordert Anschrift und Nationalität einer Studentin an, um Urheberrechtsverstöße auf Online-Plattformen zu verfolgen.

- **Entscheidung:** Ablehnung der Herausgabe der Privatanschrift/Nationalität.

- **Vorgehen:** Während Kurs- und Leistungsdaten für die Lehre zulässig sind, ist die Herausgabe privater Kontaktdaten für die Verfolgung von Urheberrechtsverstößen (Privatrecht) in der Regel nicht durch die dienstliche Aufgabenerfüllung gedeckt.

Anhang II: Checkliste zur Prüfung von Anfragen nach personenbezogenen Daten Dritter

Die folgende Checkliste dient der systematischen Prüfung und Dokumentation von Anfragen nach personenbezogenen Daten Dritter.

Eine vereinfachte Übersicht der Prüfschritte bietet der Entscheidungsbaum in Kapitel 5 dieser Handreichung.

Einordnung der Anfrage – Ist klar, wer die Anfrage stellt und in welchem Kontext?
- ☐ interne Anfrage (andere Gliederung der Hochschule)
- ☐ externe Anfrage (z. B. Behörde, Rechtsanwält:innen, Privatpersonen)

Form der Anfrage
- ☐ schriftlich (Fax, E-Mail)
- ☐ gesichert schriftlich (verschlüsselte E-Mail, beBPo, Briefpost)
- ☐ telefonisch (Achtung: zulässig nur für bestimmte, interne Anfragen)

Verifikation der anfragenden Stelle
- ☐ Ist die anfragende Stelle / Organisation bekannt und existent?
- ☐ Ist die anfragende Person dort tatsächlich tätig bzw. berechtigt?
- ☐ Stimmen die verwendeten Kontaktdaten mit offiziellen Quellen überein?

Bei Zweifeln ist eine Verifikation über **offizielle Kontaktwege** vorzunehmen. Die in der Anfrage angegebenen Kontaktdaten dürfen hierfür nicht ungeprüft verwendet werden.

Plausibilität der Anfrage – Ist die Anfrage inhaltlich nachvollziehbar?
- ☐ Ist der Zweck der Anfrage plausibel?
- ☐ Passt die Art der angefragten Daten zum Zweck?
- ☐ Besteht ein sachlicher Zusammenhang zwischen Anfrage und Aufgabe?

Vollständigkeit der Anfrage – Enthält die Anfrage alle notwendigen Angaben?
- ☐ Name und Kontaktdaten der anfragenden Stelle, Behörde, Abteilung, ggf. Aktenzeichen
- ☐ konkrete Beschreibung der angeforderten Daten
- ☐ Zweck der Datenverwendung und geltend gemachte Rechtsgrundlage

Fehlen Angaben, ist die Anfrage **zu klären oder zu ergänzen**.

Art und Umfang der Daten – Welche personenbezogenen Daten sind betroffen?
- ☐ Einfache Personenbezogene Daten (Art. 4 Nr. 1 DSGVO)
- ☐ Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)
- ☐ Sonstige Daten mit erhöhtem Schutzbedarf (Private Kontaktdaten)
- ☐ Stehen die angefragten Daten in einem sachlichen Zusammenhang mit dem Zweck?

Zulässigkeit der Datenverarbeitung durch die Hochschule – Darf die Hochschule die betreffenden Daten selbst rechtmäßig verarbeiten?
- ☐ Liegt eine zulässige Rechtsgrundlage der Verarbeitung vor?
- ☐ Erfolgt die Nutzung im Rahmen des ursprünglichen Verarbeitungszwecks?
- ☐ Sind Umfang und Speicherdauer von der Rechtsgrundlage gedeckt?

Rechtsgrundlage der Übermittlung – Eine Herausgabe kommt insbes. in Betracht bei:
- ☐ gesetzlicher Verpflichtung oder behördlicher bzw. gerichtlicher Anordnung
- ☐ wirksamer Einwilligung der betroffenen Person
- ☐ Erforderlichkeit zur Wahrnehmung einer Aufgabe der Hochschule

Dokumentation – Die Anfrage und ihre Bearbeitung sind zu dokumentieren:
- ☐ Datum der Anfrage
- ☐ anfragende Stelle und Ansprechpartner:in
- ☐ Zweck und Rechtsgrundlage
- ☐ Umfang der herausgegebenen oder verweigerten Daten
- ☐ Art der Übermittlung