

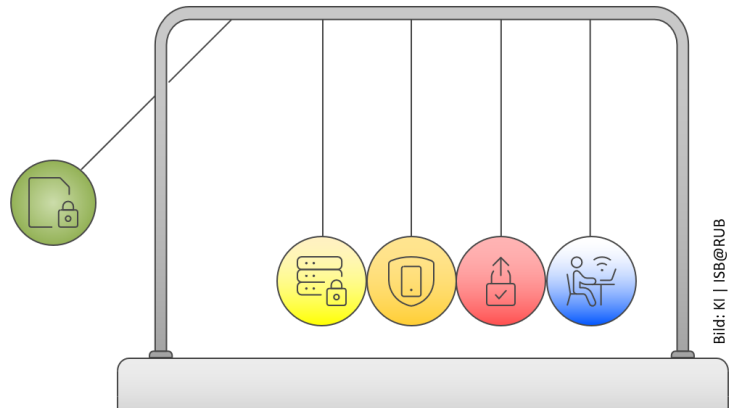
KLASSIFIKATION VON INFORMATIONEN

HANDREICHUNG ZUR INFORMATIONSSICHERHEIT

Diese Handreichung erläutert die Klassifikation von Informationen und benennt exemplarische Einstufungen typischer Informationen aus dem Hochschul-Kontext. Sie unterstützt Nutzende dabei, die Eignung von Informationen für bestimmte Verarbeitungen zu prüfen. Der Schwerpunkt liegt dabei auf der Einstufung in Vertraulichkeitsklassen.

Die Klassifikation von Informationen ist ein strukturierter Prozess, der Informationen nach ihrem Schutzbedarf kategorisiert. Als Schutzbedarf bezeichnet man die Bewertung des notwendigen Schutzniveaus, welches Informationen benötigen. Die Klassifikation bildet die Grundlage für den angemessenen Schutz der Informationen, indem sie die risikogerechte Auswahl technischer und organisatorischer Maßnahmen ermöglicht, ohne Effizienz und Kosten aus dem Blick zu verlieren.

Die Zuordnung von IT-, Cloud- und KI-Systemen zu zulässigen Vertraulichkeitsklassen ist von vielfältigen Parametern abhängig, z.B. Nutzungszweck, Vertragsgestaltung und Sicherheitsmaßnahmen, aber auch Betriebsort und -verantwortlichkeit sowie Prüfungen und Zertifizierungen. Sie wird für jedes System individuell festgelegt und für zentral bereit gestellte Systeme in den Nutzungsbedingungen beschrieben.



GELTUNGSBEREICH UND BEZUG ZUM ISMS

Die Handreichung unterstützt die Klassifikation von Informationen bezüglich der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität. Basis der Klassifikation sind die Regelungen der Informationssicherheitsrichtlinie „Klassifikation von Informationen“ der RUB.

Die Handreichung ist für alle Angehörigen der RUB anwendbar, die damit die Eignung einer Verarbeitung von Informationen in IT-, Cloud- oder KI-Systemen prüfen. Sie wird für zentral bereitgestellte Systeme durch Nutzungsbedingungen ergänzt.

Bei der Einführung oder Änderung von IT- oder Cloud-Systemen sind die Informationssicherheitsrichtlinie „Nutzung von Cloudspeicherdiensten“, die „Rahmen-Dienstvereinbarung über Einführung und Anwendung von Systemen der Informationstechnik (IT)“ und die gesetzlichen Vorgaben und Ziele des Datenschutzes anzuwenden.

ANSPRECHPERSONEN

Ansprechperson in allen Fragen bezüglich dieser Handreichung ist die Informationssicherheitsbeauftragte (CISO) der RUB.

Zur Einschätzung der Risiken von personenbezogenen Daten berät der Datenschutzbeauftragte.

Ansprechpersonen für die zentral bereitgestellten IT-, Cloud- oder KI-Systeme sind die Fachverantwortlichen der jeweiligen Betreiber.

DEFINITIONEN

Schutzziele sind grundlegende Sicherheitsprinzipien, die den angestrebten Schutzzustand von Informationen beschreiben. In der Informationssicherheit lauten die wichtigsten Schutzziele:

- **Vertraulichkeit:** Zugriff nur für Berechtigte; Schutz vor unbefugter Offenlegung.
- **Verfügbarkeit:** Daten und Dienste sind bei Bedarf für Berechtigte nutzbar.
- **Integrität:** Daten und Systeme bleiben korrekt und vollständig; Schutz vor unbefugten/ungewollten Änderungen.

Als **personenbezogene Daten** werden alle Informationen bezeichnet, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Als **sensible Daten** werden Informationen mit erhöhtem Schutzbedarf bezeichnet, weil ihre unbefugte Offenlegung, Veränderung oder ihr Verlust erhebliche Risiken oder Nachteile für betroffene Personen oder die Ruhr-Universität verursachen kann. Im Datenschutz meint „sensibel“ in der Regel die besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO (u. a. Gesundheits-, genetische und biometrische Daten, politische Meinungen, religiöse/ philosophische Überzeugungen, Gewerkschaftszugehörigkeit, sexuelle Orientierung). In der Informationssicherheit umfasst der Begriff darüber hinaus alle nichtöffentlichen Informationen mit hohem Schutzbedarf (z. B. Zugangsdaten und Kryptomaterial, Geschäfts- und Betriebsgeheimnisse, unveröffentlichte Forschungsdaten, Prüfungsaufgaben, Sicherheitsarchitekturen), die typischerweise als vertraulich/streng vertraulich klassifiziert und entsprechend besonders geschützt werden.

Als **hochsensible Daten** werden Informationen mit sehr hohem Schutzbedarf bezeichnet, z.B. Gesundheitsdaten, aus deren Verarbeitung sich unmittelbare Folgen für Freiheit, Leib und Leben ergeben können – z.B. prädiktive Gendiagnose/Huntington, Daten zu strafrechtlichen Verurteilungen und Straftaten nach Art. 10 DSGVO, (negative) dienstliche Beurteilungen und Arbeitszeugnisse, sowie Informationen zu Personen, die besonderen Gefahren oder Bedrohungen ausgesetzt sind.

PRINZIPIEN DER KLASSIFIKATION VON INFORMATIONEN

Die Klassifikation erfolgt anhand definierter Prüfszenarien für jedes Schutzziel (Vertraulichkeit, Verfügbarkeit und Integrität). Ausgehend von einem angenommenen Verlust der Schutzziele werden die Folgen für Personenrechte, Lehre, Forschung und Betrieb, Finanzen, Reputation und Rechtskonformität eingeschätzt und in Klassen eingeordnet. Der Gesamtschutzbedarf richtet sich nach dem höchsten Einzelbedarf (Maximalprinzip).

Die Einstufung von Informationstypen (z.B. personenbezogene Daten, Daten Beschäftigter oder Studierender, Forschungsdaten) ist abhängig von Art und Umfang recht unterschiedlich. Sie richtet sich nach dem jeweils höchsten Schutzbedarf von Teilinformationen und der Anzahl von Datensätzen. Auch der Lebenszyklus von Daten bestimmt die Einstufung.

Beispiele:

Personenbezogene Daten Dritter, Beschäftigter oder Studierender

allgemeine Daten, z.B. Namen, Anschrift, Telefon: *normaler Schutzbedarf* (V2), bei großen Umfängen *hoher Schutzbedarf* (V3)

besondere Kategorien, z.B. einfache Gesundheitsdaten: *normaler bis hoher Schutzbedarf* (V2/V3)

Disziplinar-/Genom-/Straftaten-Daten und umfassende Gesundheitsdaten: mindestens *hoher*, regelmäßig *sehr hoher Schutzbedarf* (V4)

Prüfungsdaten

Einzelprüfungsleistung: *normaler Schutzbedarf* (V2)

Gesamtzugriff auf Prüfungsleistungen einzelner Personen: *hoher Schutzbedarf* (V3)

bei sehr großem Umfang oder besonderer Sensitivität: *sehr hoher Schutzbedarf* (V4)

Forschungsdaten

unveröffentlichte Forschungsdaten: *hoher Schutzbedarf* (V3)

Erfindungen/Patente vor Offenlegung, NDA gebundene Geschäftsgeheimnisse: *sehr hoher Schutzbedarf* (V4)

Sicherheits- und Infrastrukturinformationen

Übersichtsinformationen: *hoher Schutzbedarf* (V3)

detaillierte Konfigurationen, Schwachstellen: *sehr hoher Schutzbedarf* (V4)

Zugangsdaten

Personen ohne besondere Berechtigungen: *hoher Schutzbedarf* (V3)

Personen mit umfangreichen oder besonderen Berechtigungen, Administrative Accounts: *sehr hoher Schutzbedarf* (V4)

Achtung: Der Gesamtschutzbedarf von Informationen und Prozessen kann durch besonders hohe Anforderungen an Verfügbarkeit oder Integrität höher ausfallen als die Vertraulichkeitsklasse (z.B. bei Prüfungsverwaltung, Gerätesteuerung, zu installierender Software). Die Klassifikation ist daher nach dem höchsten Schutzbedarf über alle Schutzziele festzulegen.

BEISPIELKLASSIFIKATION IN VERTRAULICHKEITSKLASSEN

Öffentliche Informationen

(Klasse V1 / Daten ohne Schutzbedarf bzgl. Vertraulichkeit)

Es handelt sich um Informationen, die ausdrücklich zur uneingeschränkten Veröffentlichung bestimmt und rechtlich freigegeben sind. Ihre Bekanntgabe hat keinen negativen Einfluss. Es bestehen keine Vertraulichkeitsanforderungen. **Personenbezogene Inhalte fallen nur dann in diese Vertraulichkeitsklasse, wenn die Veröffentlichung rechtmäßig ist - z.B. durch wirksame, dokumentierte Einwilligung und mit angemessener Rechtsgrundlage - und zweckgebunden freigegeben ist.**

Beispiele:

- Web, Social Media, Downloads: öffentliche Inhalte auf der Hochschul-/Universitätswebseite, Portalen, Social-Media-Kanälen, frei verfügbare Downloads
- Marketing & PR: Pressemitteilungen, Flyer, Broschüren, Hochschul-/Unizeitung
- Studium & Lehre (öffentlich): Vorlesungsverzeichnis, öffentlich bereitgestellte Lehr-/Lernmaterialien¹ (z. B. OER), Programme öffentlicher Lehr-/Info-Veranstaltungen
- Publikationen: öffentlich zugängliche Publikationen, Abstracts, Vorträge, Konferenzbeiträge
- Veranstaltungen & Medien nach Freigabe: Ankündigungen/Programme öffentlicher Veranstaltungen, Fotos/Videos nach rechtlicher Prüfung (keine sensiblen Inhalte; keine hervorgehobene Darstellung einzelner identifizierbarer Personen ohne Einwilligung)
- Öffentlich zugängliche Quellen: Informationen aus offen verfügbaren und rechtmäßig nutzbaren Quellen (z. B. Literatur, Dokumente, öffentlich bekannte dienstliche Kontaktdaten)
- Pflichtveröffentlichungen wie bspw. Geschäftsverteilungspläne

¹ nicht jedoch Inhalte aus zugangsbeschränkten Lehr-/Lernplattformen, z.B. Moodle, und nicht urheberrechtlich geschützte Inhalte

Informationen für internen Gebrauch und berechnigte Dritte (Klasse V2 / Daten mit normalem Schutzbedarf bzgl. Vertraulichkeit)

Es handelt sich um interne Informationen für Angehörige der Ruhr-Universität, die für den täglichen Betrieb benötigt werden und nicht für die Öffentlichkeit bestimmt sind, aber bei dienstlicher Notwendigkeit auch externen Stellen übermittelt werden dürfen. Ein unbefugtes Bekanntwerden könnte einen geringen bis mittleren Schaden verursachen.

Diese Vertraulichkeitsklasse ist die Standard-Einstufung für nicht gekennzeichnete, nicht öffentliche Inhalte, sofern Art und Umfang der Daten keinen höheren Schutzbedarf erfordern.

Sie enthält ggf. personenbezogene Daten ohne besondere Sensitivität, die nicht öffentlich zugänglich gemacht wurden und für die keine speziellen Geheimhaltungsverpflichtungen bestehen.

Beispiele:

- Intranet & interne Kommunikation: Inhalte aus dem Hochschul-/Universitätsintranet, interne Richtlinien/Regelwerke, Dienst- und Arbeitsanweisungen, interne Rundschreiben und Berichte, interner Schriftverkehr (E-Mail/Chat), interne Veranstaltungen, interne Telefonverzeichnisse
- Teile der Studierendenakte (intern): Teilnehmerlisten zu Lehrveranstaltungen (auch mit Matrikelnummern), Notenlisten in geringem Umfang (bei großem Umfang höherer Schutzbedarf), nicht-öffentliche Lehr-/Lernunterlagen ohne sensible Personendaten; prüfungsbezogene Unterlagen in begrenztem Umfang (z. B. Gutachten, Notenlisten) – typischerweise normal, bei größerem Umfang oder erhöhtem Risiko höher einstufen
- Forschung & Projekte (intern): Projektakten ohne vertrauliche/streng vertrauliche Inhalte (z. B. Arbeitspaketbeschreibungen, Abschlussberichte, Abrechnungen), unveröffentlichte oder für Dritte nicht interpretierbare Forschungsdaten ohne NDA, erste konzeptionelle Forschungsansätze ohne sensible Details
- Wissenschaftlich-empirisches Material (Interviews, Befragungsdaten) wenn der Inhalt des Materials nicht durch Sensibilität einen höheren Schutzbedarf erforderlich macht, z.B. Experten-Interviews gegenüber Interviews zu Diskriminierung/Gesundheitsdaten (höherer Schutzbedarf).
- Medienaufnahmen & Interviews (abhängig vom Inhalt): Fotos und Videos von Veranstaltungen nach interner Nutzung bzw. begrenzter Verbreitung ohne sensible Inhalte; Audio-/Videoaufnahmen von Interviews – typischerweise normal, je nach Inhalt/Beteiligten ggf. hoch bis sehr hoch
- Personal- und Organisationsdaten (geringe Sensitivität): ausgewählte Beschäftigtendaten mit geringer Sensitivität im internen Kontext (z. B. interne organisatorische Zuordnungen, Gehaltsinformationen) – bei detaillierten Personaldaten ggf. hoch
- Urheberrechtlich geschützte, nicht öffentlich freigegebene Materialien: intern geteilte Dokumente/Unterlagen, die dem Copyright unterliegen, ohne besondere Geheimhaltungsanforderungen.

Achtung: Umfang, Detailtiefe, Personenbezug, vertragliche Verpflichtungen (z. B. NDA) und Inhalte, die kurz vor einer Veröffentlichung stehen, können eine Höherstufung auf „hoch“/„sehr hoch“ erforderlich machen.

Informationen für vertraulichen Gebrauch und berechtigte Dritte (Klasse V3 / Daten mit hohem Schutzbedarf bzgl. Vertraulichkeit)

Es handelt sich um vertrauliche interne Informationen, deren unbefugte Offenlegung, Verlust oder Einsichtnahme einen großen Schaden oder erheblichen Imageverlust für die Ruhr-Universität verursachen kann. Eine unbefugte Verarbeitung kann darüber hinaus Betroffene in ihrer gesellschaftlichen oder wirtschaftlichen Stellung sowie in ihren Rechten erheblich beeinträchtigen.

Diese Vertraulichkeitsklasse umfasst insbesondere personenbezogene Daten mit erhöhter Schutzbedürftigkeit (einschließlich besonderer Kategorien nach DSGVO) sowie prüfungs-, forschungs-, finanz- und sicherheitsrelevante Inhalte.

Beispiele:

- Personen- und Gesundheitsdaten:
 - umfassende Personal- und Studierendendaten (z. B. Bewerbungen, Leistungsnachweise, vollständige Studierendendaten)
 - Details mit Gesundheitsbezug (z. B. Arbeitsunfähigkeitsbescheinigungen)
 - Umfassendere Dateien mit besonderen Kategorien (z. B. rassische/ethnische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, sexuelle Orientierung), soziale Verhältnisse
 - Biometrische Daten (z. B. Fingerabdrücke, spezifisch auswertbare Gesichts-/Augenbilder) – hoch bis sehr hoch
 - Scans von Identitätsdokumenten
- Prüfungswesen und Studium:
 - Prüfungsdaten (z. B. Klausuraufgaben, Prüfungsprotokolle)
 - Geschützte Studien- und Abschlussarbeiten (nicht veröffentlichte / vertrauliche Inhalte)
 - Notenlisten, prüfungsbezogene Unterlagen, z.B. Prüfungs- und Leistungsdokumentation in größerem Umfang
- Forschung und geistiges Eigentum:
 - Vertrauliche/unveröffentlichte Forschungsrohdaten
 - Auswertungen von Forschungsdaten (vor Veröffentlichung)
 - Forschungsverträge, vertrauliche Projektdaten, Metadaten und eigenentwickelte Software aus Projekten
- Finanzen, Verträge und Organisation:
 - Gehalts-, Reisekostenabrechnungen mit Kontodaten, vertrauliche Finanz-/Budgetdaten
 - Kalkulationen wirtschaftlicher Drittmittelprojekte
 - Vertragsentwürfe und Verträge (z. B. Rahmen- und Forschungsverträge)
 - Abschluss-/Revisions-/Auditberichte
 - Interne Protokolle von Gremien/Ausschüssen
- Technik und Sicherheit:
 - Technische/infrastrukturelle Informationen und Sicherheitskonzepte (z. B. Baupläne sensibler Bereiche, Standortangaben, Netzwerk-/Sicherheitspläne)
 - Passwortlisten, Zugangsdaten, Authentisierungs-/Schlüsselmaterial – hoch bis sehr hoch

Achtung: Umfang, Detailtiefe, Anzahl Betroffener, rechtliche/vertragliche Vorgaben (z. B. NDAs) und die Kritikalität (z. B. Zugangsdaten zu Kernsystemen, detaillierte Sicherheitspläne, große Datenmengen besonderer Kategorien) können eine Einstufung auf „sehr hoch“ erforderlich machen.

Informationen für streng vertraulichen oder geheimen Gebrauch und berechnigte Dritte (Klasse V4 / Daten mit besonders hohem Schutzbedarf bzgl. Vertraulichkeit)

Es handelt sich um Informationen mit höchstem Vertraulichkeitsbedarf, bei denen unberechtigte Einsichtnahme unter allen Umständen zu verhindern ist. Eine Offenlegung, ein Verlust oder eine unbefugte Verarbeitung kann schweren bis existenzgefährdenden Schaden, erheblichen Imageverlust oder Gefahren für Leib und Leben verursachen.

Dazu zählen insbesondere vertraglich oder berufsrechtlich geheim zu haltende Inhalte (z. B. NDAs, Geschäfts- und Berufsgeheimnisse) sowie hochsensible personenbezogene Daten (u. a. besondere Kategorien nach DSGVO, Daten zu Straftaten).

Beispiele:

- Hochsensible personenbezogene Daten:
 - Tiefe Gesundheits-/Patienten- und psychologische Daten zu Einzelpersonen im Sinne eines Profils, genetische/Genomdaten, die Identifizierungen ermöglichen; Gesundheitsinformationen mit potenziell stigmatisierenden Befunden
 - Besondere Kategorien nach DSGVO (z. B. Religionszugehörigkeit zu potentiell diskriminierten Gemeinschaften, Gewerkschaftszugehörigkeit, sexuelle Orientierung), Sozialdaten, hoch aussagekräftige Persönlichkeitsprofile (z. B. Bewegungsprofile)
 - Daten zu Straftaten oder Disziplinarverfahren; (umfassende) Personalakten und Nebenakten, dienstliche Beurteilungen, Arbeitszeugnisse
 - Studierendenakten mit besonders sensiblen Inhalten (z. B. Disziplinarvorgänge, Nachteilsausgleiche, Beratungs-/Gesundheitsbezug)
 - Adressen/Angaben zu Personen, die im dienstlichen Kontext erheblichen Bedrohungen ausgesetzt sind; Schuldeninformationen
- Zugangsdaten und Schlüsselmaterial:
 - Passwörter, kryptographische Schlüssel, Schlüsselverteilungspläne
 - Forschung, IP und Geschäftsgeheimnisse:
 - Erfindungsmeldungen und Patentunterlagen vor Offenlegung/Anmeldung
 - Vertrauliche F&E-Unterlagen, Prototypen, geheime technische Daten und neue Verfahren
 - Projektinformationen aus Kooperationen mit Dritten (Wirtschaft, Forschung, ggf. Militär), die unter strengen Verschwiegenheitsverpflichtungen stehen oder mit hohem Patent-/Reputationsrisiko verbunden sind; Geschäftsgeheimnisse von Partnern
- Sicherheit & Verwundbarkeiten:
 - Informationen über bestehende Sicherheitsmaßnahmen (z. B. Konfiguration von Sicherheitseinrichtungen), detaillierte Netz-/Sicherheitskonfigurationen
 - Details zu schwerwiegenden Schwachstellen (Software, Zutrittssteuerung etc.) und mögliche Angriffspfade
 - Sicherheitskritische Forschung
- Strategie & Steuerung (vor Veröffentlichung):
 - Strategiepapiere und sensible Planungsdokumente, deren vorzeitige Offenlegung erheblichen Schaden verursachen könnte.

Achtung: Große Datenumfänge, hohe Personenanzahl, besondere rechtliche/vertragliche Bindungen oder unmittelbare Gefährdungen für Personen sind Indikatoren für die Einstufung „sehr hoch“.

ZULÄSSIGE IT-, CLOUD- UND KI-SYSTEME

Den Rahmen für die Beurteilung der Zulässigkeit von Cloud- und KI-Systemen setzt die Informationssicherheitsrichtlinie „Nutzung von Cloudspeicherdiensten“, Die konkrete Einordnung, welche Systeme zur Verarbeitung oder Speicherung von Informationen spezifischer Vertraulichkeitsklassen zulässig sind, erfordert in der Regel eine individuelle Analyse von Nutzungszwecken, umgesetzten Sicherheitsmaßnahmen, Verträgen mit Betreibern, Betriebsort und -verantwortlichkeit sowie vorhandenen Prüfungen und Zertifizierungen von Betreibern oder Anbietern. Je nach Nutzungszweck sind auch die Anforderungen an die Schutzziele Verfügbarkeit und Integrität zu berücksichtigen.

Die Verarbeitung von Daten einer höheren Vertraulichkeitsklasse auf für niedrigere Klassen zugelassenen Systemen ist nur zulässig, wenn geeignete, dokumentierte und freigegebene kompensierende Maßnahmen ein gleichwertiges Schutzniveau sicherstellen, etwa Anonymisierung, Pseudonymisierung oder starke Ende-zu-Ende-Verschlüsselung.

Die Eignung zentral bereit gestellter Systeme für spezifische Vertraulichkeitsklassen wird in den jeweiligen Nutzungsbedingungen beschrieben. Eine Übersicht zulässiger Cloud- und KI-Systeme ist in Erstellung. Ansprechpersonen sind die Informationssicherheitsbeauftragte (CISO) und der Datenschutzbeauftragte der RUB.

WEITERFÜHRENDE INFORMATIONEN

Regelwerk zur Informationssicherheit an der RUB:

<https://isms.ruhr-uni-bochum.de/>

Webseite der Stabsstelle für Informationssicherheit:

<https://informationssicherheit.ruhr-uni-bochum.de/>