

Toolbox zu Wissenssicherheit und Open Science

Anhang zum Bericht [Openness and security: two pillars, one system](#)

Projektpartner:

University of Bern (project leader)

Center for Security Studies (ETH)

University of Applied Sciences and Arts Western Switzerland (HES-SO)

Unterstützt von swissuniversities

Dies ist eine Übersetzung der [englischen Originalversion](#), erstellt mit Unterstützung von DeepL Pro.

Inhalt

1.	Empfehlung 1: Entwicklung umfassender Richtlinien zur Wissenssicherheit _____	5
2.	Empfehlung 2: Einrichtung von “Knowledge Security Officers” oder spezialisierter interner Einheiten _____	5
3.	Empfehlung 3: Durchführung von Schulungs- und Sensibilisierungs-programmen zum Thema Wissenssicherheit _____	8
4.	Empfehlungen 5, 6 und 7: Massnahmen zur Wissenssicherheit in Open Science und Open Science als Massnahme zur Wissenssicherheit _____	9
5.	Anreize und Abstimmung der Bewertung _____	9
1.	Umfassende Leitfäden oder Risikobewertungen _____	11
2.	Inhalt _____	11
2.1	Unterwerfung unter Exportkontrollen	11
2.2	Listen kritischer Technologien.....	12
2.3	Ermittlung des Dual-Use-Potenzials von Forschungsprojekten	12
3.	Partner _____	14
3.1	Umfassende Bewertungsinstrumente	14
3.2	Embargos und Sanktionen	14
3.3	Bewertung der Netzwerke von Institutionen oder Forscher:innen	15
3.4	Listen kritischer Einrichtungen aufgrund militärischer Nähe	16
3.5	Weitere Überlegungen	16
4.	Infrastruktur _____	16
	Anhänge _____	17

Diese Toolbox soll Forscher:innen und Forschungseinrichtungen dabei unterstützen, sich in der sich wandelnden Landschaft der Wissenssicherheit zurechtzufinden, insbesondere im Kontext von Open Science.¹ Sie baut auf dem gemeinsamen Verständnis auf, das in den „Gemeinsamen Werten und Grundsätzen der G7 zu Forschungssicherheit und Forschungsintegrität“ zum Ausdruck kommt, wonach „Offenheit und Sicherheit kein Widerspruch sind, sondern sich ergänzen und gegenseitig verstärken“.

u^b

In ihrem Bericht identifiziert die von swissuniversities geleitete Nationale Arbeitsgruppe für Wissenssicherheit Schwachstellen im Schweizer System zum Umgang mit Wissenssicherheit, insbesondere einen Mangel an „spezifischer Fachkompetenz in den Bereichen Wissenssicherheitsbewertung und Risikomanagement“: „Traditionelle Hochschulverwaltungen verfügen möglicherweise nicht über das erforderliche Fachwissen, um komplexe Sicherheitsauswirkungen von Forschungsprojekten oder internationalen Partnerschaften zu bewerten. Diese Kompetenzlücke stellt eine grundlegende Herausforderung dar, die durch Schulungen, Personalrekrutierung oder externe Unterstützungsmechanismen angegangen werden muss.“²

Der Bericht „*Openness and Security: Two Pillars, One System*“³ ist ein Schritt in Richtung der Schliessung dieser Lücke. Diese Toolbox, die den Bericht ergänzt, bietet praktische Anleitungen, Beispiele und operative Instrumente.

Die Toolbox richtet sich an die Hochschulleitung und nur indirekt an Forschende. Die darin enthaltenen Instrumente können genutzt und an den institutionsspezifischen Kontext sowie den Governance-Rahmen angepasst werden.

Sie zielt darauf ab, potenzielle Risiken zu identifizieren, zu bewerten und zu bewältigen und gleichzeitig die Offenheit, die internationale Zusammenarbeit und die akademische Freiheit zu wahren, die für den wissenschaftlichen Fortschritt von grundlegender Bedeutung sind. Massnahmen sollten in einem angemessenen Verhältnis zu den tatsächlichen Risiken stehen, unnötige Bürokratie vermeiden und diskriminierungsfrei angewendet werden.

Die Toolbox orientiert sich an fünf Grundprinzipien.

1. „So offen wie möglich, so sicher wie nötig“: Forschungsergebnisse, Methoden und Kooperationen sollten standardmässig offen sein, es sei denn, berechnete Risiken erfordern einen kontrollierten Zugang.

¹ Eine Definition des Begriffs „Open Science“ finden Sie in dem Bericht, zu dem diese Toolbox gehört: Universität Bern/Zentrum für Sicherheitsstudien/Fachhochschule Westschweiz: *Openness and Security: Two Pillars, One System*, Bern: 2026. Wir folgen der Definition der UNESCO und konzentrieren uns auf die beiden Dimensionen Open Access und offene Forschungsdaten.

² [Swissuniversities – Wissenssicherheit in der Schweiz: Ein strategischer Rahmen für Hochschulen und Behörden](#), S. 8.

³ Der Bericht legt den regulatorischen Rahmen für Wissenssicherheit und Open Science auf internationaler Ebene und in der Schweiz dar, untersucht und identifiziert, welche Risiken für die Wissenssicherheit im spezifischen Kontext von Open Science tatsächlich bestehen, erläutert, welche Faktoren zu Risiken für die Wissenssicherheit in Open Science führen oder diese verstärken, und beschreibt, wie Institutionen in Europa und der Schweiz derzeit mit Risiken für die Wissenssicherheit in Open Science umgehen. Bevor wir zum Schluss kommen und Empfehlungen aussprechen, wagen wir einen Ausblick auf die Zukunft der Wissenssicherheit und von Open Science.

2. Verhältnismässigkeit: Sicherheitsmassnahmen sollten in einem angemessenen Verhältnis zum tatsächlichen Risiko stehen und übermässige Bürokratie vermeiden, die Zusammenarbeit oder Innovation behindert.
3. Unterstützung der Forschenden: Forschende sollten nicht die gesamte Last der «Compliance» tragen müssen. Institutionen müssen Infrastruktur, Schulungen, Beratungsdienste und administrative Unterstützung bereitstellen.
4. Transparenz und Rechenschaftspflicht: Entscheidungen zur Wissenssicherheit sollten dokumentiert, überprüfbar und durch klare institutionelle Verfahren geregelt sein.
5. Erhaltung der internationalen Zusammenarbeit: Das Ziel ist nicht die Deglobalisierung der Wissenschaft, sondern eine widerstandsfähige, ethische und sichere Zusammenarbeit.

Die Toolbox ist in zwei Abschnitte gegliedert: Abschnitt 1 listet Instrumente zur Bewältigung von Wissenssicherheit im spezifischen Kontext von Open Science auf. Abschnitt 2 widmet sich anderen Instrumenten zur Risikobewertung und -klassifizierung sowie Leitlinien, die nicht spezifisch für den Open-Science-Kontext sind, die Institutionen jedoch als nützlich erachten könnten, um Risiken der Wissenssicherheit anzugehen und ihre Risikomanagement-Rahmenwerke zu stärken.

Die meisten, jedoch nicht alle in der Toolbox genannten Instrumente wurden im Rahmen des swissuniversities-Projekts zu Wissenssicherheit und Open Science entwickelt (unten als „Projektergebnis“ gekennzeichnet). Es wurden zudem bestehende Ressourcen zusammengestellt, die als nützlich erachtet werden. Falls Links nicht mehr aktiv sind, wird Nutzenden empfohlen, online nach dem Titel der Publikation zu suchen.

Die folgenden Abschnitte greifen die Empfehlungen aus Kapitel 6 des Berichts „*Openness and Security: Two Pillars, One System*“ auf und schlagen konkrete praktische Instrumente zu deren Umsetzung vor.

u^b

1. Empfehlung 1: Entwicklung umfassender Richtlinien zur Wissenssicherheit

Wissenssicherheit sollte in die institutionelle Strategie, die Forschungssteuerung und die Risikomanagement-Rahmenwerke integriert werden. Institutionen sollten klare Richtlinien zur Wissenssicherheit festlegen, die Schlüsselbereiche wie Sorgfaltspflichten bei internationalen Kooperationen, Protokolle zum Technologietransfer, Massnahmen zur Informationssicherheit und Mechanismen zur Meldung von Bedenken hinsichtlich der Wissenssicherheit abdecken. Diese sollten mit nationalen und institutionellen Vorschriften zu Exportkontrollen, Datenschutz und geistigem Eigentum in Einklang stehen.

Diese Richtlinien sollten in Absprache mit der Forschungsgemeinschaft entwickelt werden, um sicherzustellen, dass sie praxisnah, verhältnismässig und transparent sind. Gleichzeitig sollten sie unnötigen Verwaltungsaufwand minimieren und gleichzeitig ausreichend flexibel bleiben, um auf sich wandelnde Risiken und regulatorische Anforderungen reagieren zu können.

Open Science sollte in dieser Richtlinie und im operativen Geschäft selbstverständlich berücksichtigt werden. Als bewährte Praxis sollten Einrichtungen darüber hinaus eine eigene Richtlinie zur Wissenssicherheit im Rahmen von Open Science verabschieden, die:

- die nationale und die institutionelle Risikobereitschaft hinsichtlich Offenheit versus Einschränkung definiert
- konkrete und institutionenspezifische Leitlinien bereitstellt
- zwischen Disziplinen und Risikostufen unterscheidet (z. B. Geisteswissenschaften vs. MINT-Fächer mit doppeltem Verwendungszweck (Dual-Use)).

In Übereinstimmung mit den Empfehlungen 5, 6 und 7 des Berichts „*Openness and Security: Two Pillars, One System*“ empfehlen wir, dass Open-Science-Praktiken auf operativer Ebene als Massnahmen zur Wissenssicherheit betrachtet und genutzt werden und dass Open-Science-Praktiken durch Massnahmen zur Wissenssicherheit verbessert werden.⁴ Dieser Ansatz stellt sicher, dass sich beide Konzepte gegenseitig verstärken, während gleichzeitig das Risiko vermieden wird, weitere und nicht zwingend notwendige administrative Prozesse zu schaffen.

2. Empfehlung 2: Einrichtung von “Knowledge Security Officers” oder spezialisierter interner Einheiten

Um die oben in Kapitel 1, Abschnitt 1 genannten Richtlinien und Verfahren zu entwickeln und ordnungsgemäss umzusetzen, müssen Institutionen in eine Unterstützungsstruktur investieren, die sowohl rechtliche, Compliance- und Sicherheitsaspekte als auch Open Science abdeckt. Aufgrund

⁴ Ein praktisches Instrument wird in Kapitel 1, Abschnitt 4 dieser Toolbox vorgeschlagen.

der Überschneidungen zwischen Wissenssicherheit und Open Science sollten die jeweiligen Einheiten in dem jeweils anderen Bereich geschult werden.

Den Einrichtungen wird folgendes Leistungsportfolio empfohlen:

1. Open-Science-Helpdesk: Unterstützung bei Veröffentlichungen und Repositorien

Dieser Service ist die Anlaufstelle für Forschende, die ihre Ergebnisse offen veröffentlichen und dabei die Anforderungen von Förderern oder der Einrichtung erfüllen möchten.

Kernfunktionen

- Unterstützung bei Open-Access-Veröffentlichungen: Beratung zu Verlagsrichtlinien, APC-Finanzierung, transformativen Vereinbarungen und Rechtebeibehaltung
- Unterstützung bei Repositorien: Hinterlegung von Artikeln, Datensätzen, Software, Dissertationen und anderen Forschungsergebnissen in institutionellen oder fachspezifischen Repositorien
- Metadaten und Auffindbarkeit: Sicherstellung, dass Forschungsergebnisse korrekt beschrieben, verknüpft (ORCID, DOI, Förderkennzahlen) und indexiert werden
- Beratung zu Lizenzen: Unterstützung von Forschenden bei der Auswahl geeigneter Lizenzen (z. B. Creative Commons)
- Überwachung der Einhaltung von Vorgaben: Überprüfung der Einhaltung von Förderervorgaben und institutionellen Open-Science-Richtlinien

2. Data Stewardship : FAIR-konformes und sicheres Datenmanagement, einschliesslich Wissenssicherheitsrisiken im Bereich Open Science

Dieser Service stellt sicher, dass Forschungsdaten sowohl wiederverwendbar als auch angemessen geschützt sind.

FAIR-Datenmanagement

- Findable: persistente Identifikatoren und aussagekräftige Metadaten
- Accessible: kontrollierte oder offene Zugangsmechanismen
- Interoperable: Verwendung von Standards und gängigen Formaten
- Reusable: Dokumentation, Provenienz und Lizenzierung

Sicherheits- und Governance-Funktionen

- Datenklassifizierung (öffentlich/intern/vertraulich/eingeschränkt oder: offen/eingeschränkt/geheim/exportkontrolliert usw.)
- Sichere Speicherung und Zugriffskontrollen
- Verschlüsselung, Datensicherung und Aufbewahrungsrichtlinien
- Unterstützung für Datenmanagementpläne (DMPs)

Die Rolle der Wissenssicherheit für Open Science

Eine moderne Datenverwaltungsstelle prüft zudem, ob die offene Bereitstellung von Daten Risiken für die Wissenssicherheit mit sich bringen könnte. Beispiele hierfür sind Forschungsdaten mit doppeltem Verwendungszweck, sensible Infrastrukturinformationen, strategische Technologien oder Daten, die vertraglichen oder nationalen Beschränkungen unterliegen.

Data Stewards führen daher in Zusammenarbeit mit den Compliance-Beauftragten für Wissenssicherheit (siehe unten) folgende Aufgaben durch oder koordiniert diese:

- Risikoidentifizierung
- Risikobewertung (Eintrittswahrscheinlichkeit und Auswirkungen)
- Risikominderung (teilweise Freigabe, Sperrfristen, kontrollierter Zugriff, Anonymisierung)
- Dokumentation von Entscheidungen

3. Knowledge Security Compliance Officer

Institutionen sollten Beauftragte für Wissenssicherheit (Knowledge Security Compliance Officer) ernennen und/oder einen Ausschuss für Wissenssicherheit einrichten, um die Umsetzung und Entscheidungsfindung zu unterstützen.⁵ Sie beraten Forschende und Führungskräfte, koordinieren Risikobewertungen, prüfen komplexe oder risikoreiche Fälle, stellen klare Eskalationswege für schwierige Entscheidungen bereit und gewährleisten eine einheitliche und verhältnismässige Anwendung der Richtlinien in der gesamten Institution sowie die effektive und harmonisierte Integration der Wissenssicherheit in andere Einheiten innerhalb der Institution (z. B. Open-Science- oder Auslandsbüros usw.).

Hauptaufgaben⁶

- Bewertung internationaler Kooperationen: Identifizierung von Partnern, Finanzierungsquellen, Rechtsordnungen und strategischen Technologiebereichen; Bewertung der Risiken eines ungewollten Transfers von Wissen, Technologie, Daten oder Fachwissen
- Überprüfung bei der Personalrekrutierung: Überprüfung von Ernennungen in sensiblen Forschungsbereichen; Identifizierung von Interessenkonflikten, nicht offengelegten Verbindungen oder Sanktionsbedenken
- Überprüfung von Studierenden (sofern gesetzlich zulässig und von der Einrichtung beschlossen): Bewertung des Zugangs zu hochsensiblen Einrichtungen, Datensätzen oder Technologien; Anwendung verhältnismässiger, risikobasierter Massnahmen
- Risikomanagement im Bereich Open Science: Prüfung, ob geplante Veröffentlichungen, Preprints, Software-Veröffentlichungen oder der Datenaustausch Bedenken hinsichtlich der Wissenssicherheit hervorrufen könnten; Koordinierung von Abhilfemassnahmen vor der Veröffentlichung
- Schulung und Sensibilisierung: Bereitstellung von Leitlinien für Forschende, Betreuende, Verwaltungsmitarbeiter:innen und Führungskräfte

Diese Funktion sollte nicht als pauschaler „Gatekeeper“ für die internationale Zusammenarbeit dienen. Bewährte Praktiken sind risikobasiert, verhältnismässig und transparent und schaffen ein Gleichgewicht zwischen akademischer Freiheit und Sicherheitsverpflichtungen.

4. Rechts- und Exportkontrollstelle: Unterstützung bei regulatorischen Fragen

Diese Stelle liefert die formelle rechtliche und regulatorische Auslegung, auf der die anderen Funktionen basieren.

Typische Aufgaben

- Einstufung nach Exportkontrollbestimmungen und Überprüfung auf Sanktionen
- Vertragsprüfung
- Beratung zum geistigen Eigentum

⁵ Siehe auch die Empfehlung der Nationalen Arbeitsgruppe hier: [Swissuniversities – Wissenssicherheit in der Schweiz: Ein strategischer Rahmen für Hochschulen und Behörden](#) , Abschnitt 4.1, sowie Empfehlung 2 des Berichts „Openness and Security: Two Pillars, One System“.

⁶ Siehe auch die Empfehlung der Nationalen Arbeitsgruppe hier: [Swissuniversities – Wissenssicherheit in der Schweiz: Ein strategischer Rahmen für Hochschulen und Behörden](#) , Abschnitt 4.2 und Anhang 3.

- Einhaltung von Datenschutz- und Privatsphäre Vorschriften
- Unterstützung bei der Dokumentation und bei Audits
- Zusammenarbeit mit nationalen Behörden

5. Wie die vier Dienstleistungen zusammenpassen

Open-Science-Helpdesk → Data Stewardship → Beauftragte für Wissenssicherheit → Rechts- und Exportkontrollen

u^b

Beispiel:

- Ein/e Forscher:in möchte einen Artikel veröffentlichen und einen Datensatz freigeben
- Der Open-Science-Helpdesk unterstützt bei der Hinterlegung im Repository und der Lizenzierung
- Die Data-Stewardship-Stelle prüft die FAIR-Kriterien, die Vertraulichkeit und mögliche Sicherheitsrisiken
- Wenn das Projekt sensible Daten umfasst, wird der/die Beauftragte für Wissenssicherheit in die Risikobewertung und das Risikomanagement einbezogen
- Treten Fragen zu kontrollierten Technologien oder Sanktionen auf, ermittelt die Rechtsabteilung bzw. die Stelle für Exportkontrollen die geltenden rechtlichen Anforderungen.
- Der/die Forscher:in erhält einen koordinierten Entscheidungsweg anstelle widersprüchlicher Empfehlungen verschiedener Stellen.

3. Empfehlung 3: Durchführung von Schulungs- und Sensibilisierungsprogrammen zum Thema Wissenssicherheit

Voraussetzung für die erfolgreiche Umsetzung von Massnahmen zur Wissenssicherheit in den institutionellen Abläufen ist das Bewusstsein und die Akzeptanz innerhalb der Forschungsgemeinschaft. Die Initiierung einer Bottom-up-Bewegung ist effektiver und nachhaltiger als das Auferlegen von Top-down-Anforderungen. Die folgenden Instrumente sollen Institutionen dabei unterstützen, das Bewusstsein zu schärfen und über Wissenssicherheit (in Open Science) zu informieren.

- **Projektergebnis:** „Do’s and Don’ts“ für Wissenssicherheit in Open Science (Anhang 1)

Was: Kompaktes Reflexions- und Leitfadensinstrument zur allgemeinen Sensibilisierung

Für wen: Forschende

Zeitpunkt: Zeitloses Instrument

- **Projektergebnis:** Folien zum Thema „Einführung in die Wissenssicherheit in Open Science“ (Anhang 2)

Was: Folien zur Einführung in die Wissenssicherheit in Open Science, die an die Bedürfnisse und Prioritäten der jeweiligen Einrichtung angepasst werden können.

Für wen: Universitätsverwaltung, die mit der Sensibilisierung der Forschenden beauftragt ist.

Wann: Zeitloses Instrument; kann bei der Einarbeitung neuer Mitarbeiter:innen und/oder im Rahmen regelmässiger Schulungen eingesetzt werden.

4. Empfehlungen 5, 6 und 7: Massnahmen zur Wissenssicherheit in Open Science und Open Science als Massnahme zur Wissenssicherheit

Die folgenden Instrumente sollen Einrichtungen dabei unterstützen, Wissenssicherheit in Open-Science-Praktiken zu integrieren und Open-Science-Praktiken als Instrumente der Wissenssicherheit zu nutzen.

u^b

- **Projektergebnis:** Knowledge Security Management Plan (für Open Science, KSMP) (Anhang 3)

Was: Vorschlag für einen umfassenden Fragebogen, der als Instrument zur Risikobewertung eingesetzt werden kann, um Risiken für die Wissenssicherheit bei der Umsetzung von Open Science zu ermitteln. Es handelt sich um ein Instrument, um auf bestimmte Risiken hinzuweisen und das Bewusstsein dafür zu schärfen.

Für wen: Ist von Forschenden in Zusammenarbeit mit Data Stewards und Beauftragten für Wissenssicherheit auszufüllen.

Wann: So früh wie möglich im Forschungsprozess, spätestens jedoch vor der Veröffentlichung der Daten.

- **Projektergebnis:** Entscheidungsbaum zur Datenfreigabe (Wissenssicherheit in Open Science) (Anhang 4)

Was: Ein praktischer Entscheidungsbaum, der den Knowledge Security Management Plan, KSMP, (für Open Science) ergänzt und operationalisiert. Der KSMP kann Klarheit schaffen oder Hinweise geben, wie die im Entscheidungsbaum gestellten Fragen zu beantworten sind.

Für wen: Forschende, möglicherweise in Zusammenarbeit mit Data Stewards und Beauftragten für Wissenssicherheit.

Wann: So früh wie möglich im Forschungsprozess, spätestens jedoch vor der Veröffentlichung der Daten.

- **Projektergebnis:** Risiken für die Wissenssicherheit in Open Science: Massnahmen zur Risikominderung (Anhang 5)

Was: Zusammenstellung von Massnahmen zur Minderung der im Knowledge Security Management Plan identifizierten Risiken. Kann als Folgeinstrument zum KSMP oder zum Entscheidungsbaum verwendet werden, sobald Risiken identifiziert wurden und/oder eine Entscheidung über den Grad der Beschränkung eines Datensatzes getroffen wurde.

Für wen: Forschende in Zusammenarbeit mit Data Stewards und Beauftragten für Wissenssicherheit.

Wann: Sobald Risiken identifiziert wurden, spätestens jedoch vor der Veröffentlichung der Daten.

5. Anreize und Abstimmung der Bewertung

Wissenssicherheit und Open Science lassen sich beide durch Anreize und die Ausrichtung des Bewertungssystems einer Einrichtung stärken, ergänzend zu möglichen CoARA-Standards. Ziel ist es, Forschende für verantwortungsbewusste Offenheit und sicheres Forschungsverhalten zu belohnen.

Beispielsweise können die folgenden Elemente in einen bestehenden Rahmen für Beförderungskriterien aufgenommen werden:

Bereich	Beispielindikator
Open Access	Prozentualer Anteil offen zugänglicher Publikationen

Offene Daten	Hinterlegte FAIR-konforme Datensätze
Reproduzierbarkeit	FAIR-Kodex, Arbeitsabläufe, Protokolle
Public engagement	Citizen Science und gesellschaftliche Auswirkungen
Verantwortungsvolle Zusammenarbeit	Abschluss von Sorgfaltsprüfungsverfahren (due diligence procedures)
Sichere Datenpraktiken	Angemessener Umgang mit sensiblen Daten

u^b

In ähnlicher Weise könnten institutionelle Auszeichnungen für dieselben Aktivitäten vergeben werden, und interne Fördermittel könnten Kriterien von Open Science und der Wissenssicherheit berücksichtigen.

u^b

In Kapitel 3 des Berichts „Openness and Security: Two Pillars, One System“ analysieren wir die Faktoren, die Risiken für die Wissenssicherheit verursachen oder verstärken. Die folgenden Instrumente unterstützen Einrichtungen dabei, die Wahrscheinlichkeit von rechtlichen und sicherheitsrelevanten Risiken losgelöst vom bisherigen Fokus auf Open Science anhand dieser Faktoren (Forschungsinhalte, Partner und Infrastruktur) zu bewerten.

1. Umfassende Leitfäden oder Risikobewertungen

Die folgenden beiden Instrumente decken mehrere rechtliche und sicherheitsrelevante Risiken ab und lassen sich daher keiner der Kategorien (Inhalt, Partner, Infrastruktur) zuordnen.

- Regierung der Niederlande (2022): [Nationale Leitlinien zur Wissenssicherheit](#)
Was: Leitlinien zu Bedrohungsanalyse, rechtlichem Rahmen, Risikobewertung, Risikomanagement, internationalen Partnerschaften, Personalrekrutierung und Cybersicherheit
Für wen: Hochschuleinrichtungen und deren Leitung
Wann: Vor oder während der Umsetzung institutioneller Governance-Strukturen
- DLR-Projektträger/Safeguarding Science (2024): [Sorgfaltspflicht in der Wissenschaft](#)
Was: Leitlinien vor allem zu Risiken im Zusammenhang mit Personalrekrutierung und internationalen Kooperationen
Für wen: Hochschulen und deren Leitung
Wann: Vor oder während der Umsetzung institutioneller Governance-Strukturen

2. Inhalt

2.1 Unterwerfung unter Exportkontrollen

- Schweizer Exportkontrolllisten
 - [Güterkontrollgesetz](#)
 - [Verordnung über die Güterkontrolle](#)
 - [Kriegsmaterialgesetz](#)
 - [Kriegsmaterialverordnung](#)
 - Chemikalienkontrollverordnung (auf [Deutsch](#), [Französisch](#) oder [Italienisch](#))
 - Verordnung über die Ausfuhr und Vermittlung von Gütern für die Internet- und Mobilfunküberwachung (auf [Deutsch](#), [Französisch](#) oder [Italienisch](#))
 - Anhänge mit den Listen der Güter, die der Ausfuhrkontrolle unterliegen (auf [Deutsch](#), [Französisch](#) oder [Italienisch](#))
- Ausländische Vorschriften mit extraterritorialer Geltung
 - Die US-amerikanischen Vorschriften zu Sanktionen, Embargos und Exportkontrollen sind extraterritorialer Natur. Sie finden weltweit Anwendung, wenn bestimmte Anknüpfungskriterien erfüllt sind:

- US-Personen: alle US-Bürger:innen, alle in den USA ansässigen Personen und Personen mit einer US-Aufenthaltsgenehmigung (z. B. Green Card), unabhängig von ihrem Aufenthaltsort; alle natürlichen und juristischen Personen, die in den USA ansässig oder dort domiziliert sind; sowie alle in den USA domizilierten Unternehmen und deren ausländische Niederlassungen.
 - US-Produkte, einschliesslich Produkte, die zu mindestens 10 % oder 25 % auf Produkten US-amerikanischen Ursprungs basieren (z. B. eine Drohne, die zur Steuerung US-Software verwendet).
- US-Exportkontrollregelungen:
 - Export Administration Regulation (EAR): Güter mit doppeltem Verwendungszweck ([Commerce Control List](#))
 - [International Traffic in Arms Regulations \(ITAR\)](#): Militärgüter
- Hilfe zur Suche in den Güterlisten:
 - Die Güterlisten sind nur auf Deutsch, Französisch oder Italienisch verfügbar. Wenn Sie die Güterlisten in einer anderen Sprache benötigen, können Sie die EU-Liste der Güter mit doppeltem Verwendungszweck (Anhang 1 der [Verordnung \(EU\) 2021/821](#)) konsultieren, die in allen EU-Sprachen verfügbar ist. Sie ist nicht zu 100 % identisch mit der Schweizer Liste, überprüfen Sie daher unbedingt, ob der von Ihnen gefundene Eintrag auch in der Schweizer Liste enthalten ist.
 - Stichwortverzeichnisse zur Feststellung, ob eine bestimmte Ware, Technologie oder Software den Ausfuhrkontrollen unterliegt
 - Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA): [Gemeinsames, unverbindliches Glossar für Teil I der Ausfuhrliste und Anhang I der EU-Dual-Use-Verordnung](#) (auf Deutsch). Dieser Stichwortindex basiert auf der EU-Liste der Güter mit doppeltem Verwendungszweck; Sie müssen daher überprüfen, ob der von Ihnen gefundene Eintrag auch in der Schweizer Liste enthalten ist.
 - Bureau of Industry and Security (BIS): [Interactive Commerce Control List](#). Hierbei handelt es sich um die US-amerikanische Liste für Güter mit doppeltem Verwendungszweck, die nach Stichwörtern durchsucht werden kann. Da die Schweizer Liste nicht zu 100 % mit der US-amerikanischen Liste übereinstimmt, müssen Sie erneut überprüfen, ob der von Ihnen gefundene Eintrag auch in der Schweizer Liste enthalten ist.

2.2 Listen kritischer Technologien

- DLR Projektträger/Safeguarding Science (2026): [Listen kritischer und sensibler Technologien – Geltungsbereich, Zweck und Zielgruppe](#) (diese Publikation erläutert die von verschiedenen Akteuren und Ländern erstellten Listen)
- [EU-Liste kritischer Technologien](#)
- US-Liste kritischer und aufstrebender Technologien ([Januar 2026](#))
- Kanadische [Liste sensibler Technologien](#)
- ETH-Liste kritischer Technologien (aufgeführt in diesem Artikel: [Dual-Use und Sanktionen: Diese Anwendungen erfordern eine Sicherheitsüberprüfung – Staffnet | ETH Zürich](#))

2.3 Ermittlung des Dual-Use-Potenzials von Forschungsprojekten

- **Projektergebnis:** Fragebogen zum Dual-Use-Potenzial (Anhang 6)

Was: Ein umfassender Fragebogen zur Ermittlung des Dual-Use-Potenzials eines bestimmten Forschungsprojekts in den Bereichen Künstliche Intelligenz/Maschinelles Lernen, Biotechnologie, Chemie, Robotik, Cybersicherheit, Materialwissenschaften, Energiesysteme, Quantentechnologien,

Luft- und Raumfahrt, Synthetische Biologie oder Neurowissenschaften. Ein Instrument zur Sensibilisierung und zur Ermittlung von Risiken, Risikominderungsstrategien sowie institutioneller oder staatlicher Aufsicht.

Für wen: Richtet sich an Forschende.

Wann: Während des gesamten Forschungszyklus: bei der Projektplanung, immer dann, wenn ein Projekt in eine neue Phase eintritt oder unerwartete Ergebnisse liefert, vor der Weitergabe von Ergebnissen oder Materialien an Kooperationspartner sowie vor der Veröffentlichung oder anderweitigen Verbreitung von Forschungsergebnissen.

- Robert-Koch-Institut (2013): [Dual-Use-Potenzial der Lebenswissenschaften](#) (Abschnitt 3)

Was: Der Verhaltenskodex des Robert-Koch-Instituts zur Risikobewertung und Risikominderung legt Grundsätze und Verfahren zur Identifizierung, Bewertung und Minderung des Dual-Use-Potenzials von Forschung in den Lebens-, Gesundheits- und Medizinwissenschaften fest.

Für wen: In erster Linie für Forschende, Projektleitende und Management, insbesondere für diejenigen, die in den Lebenswissenschaften mit Krankheitserregern oder Toxinen forschen oder andere Forschungsarbeiten mit potenziellen Dual-Use-Implicationen durchführen.

Wann: Während des gesamten Forschungszyklus: bei der Projektplanung, immer dann, wenn ein Projekt in eine neue Phase eintritt oder unerwartete Ergebnisse liefert, vor der Weitergabe von Ergebnissen oder Materialien an Kooperationspartner sowie vor der Veröffentlichung oder anderweitigen Verbreitung von Forschungsergebnissen.

- Niederländisches Amt für Biosicherheit (2021): [Dual-Use-Quickscan](#)

Was: Der Dual-Use-Quickscan ist ein Online-Tool zur Selbsteinschätzung, das Forschenden in den Biowissenschaften hilft, potenzielle Dual-Use-Aspekte ihrer Forschung anhand eines strukturierten Fragebogens zu identifizieren und das Bewusstsein für Biosicherheitsrisiken zu schärfen.

Für wen: Forschende, die mit Mikroorganismen oder damit verbundenen biologischen Erkenntnissen und Technologien arbeiten.

Wann: In jeder Phase des Forschungszyklus, von der Projektkonzeption bis zur Veröffentlichung.

- Gemeinsame Forschungsstelle & Universität Lüttich: [TIM Dual-Use-Webplattform](#) (STRIKE-Projekt, Referate G.II.7 und T.5)

Was: TIM Dual-Use ist eine webbasierte Text-Mining-Plattform, die wissenschaftliche Publikationen, Patente und EU-finanzierte Forschungsprojekte abbildet, um auf der Grundlage der EU-Dual-Use-Kontrollliste und neuer Technologien Forschungsarbeiten mit potenzieller Dual-Use-Relevanz zu identifizieren. Sie unterstützt die Sensibilisierung, Trendanalyse und institutionelle Compliance, indem sie Nutzern hilft, potenziell sensible Forschungsergebnisse zu identifizieren. Kann genutzt werden, um Dual-Use-Forschung oder Forschung mit exportkontrollierten Gütern rückwirkend (d. h. nach der Veröffentlichung) zu erkennen.

Für wen: Forschungseinrichtungen, Universitäten, politische Entscheidungsträger:innen und Fachleute im Bereich der Exportkontrolle.

Wann: Zur Überprüfung bestehender Forschungsergebnisse und zur Überwachung von Dual-Use-Technologien im Hinblick auf Sensibilisierung, Compliance und strategische Analyse.

3. Partner

3.1 Umfassende Bewertungsinstrumente

- **Projektergebnis:** Selbstbewertung zur Wissenssicherheit für Forschende und Bewertungsmatrix für die Hochschulleitung (Anhang 7)

Was: Selbstbewertung für Forschende, die internationale Kooperationen eingehen möchten, zur Analyse und Sensibilisierung für Risiken im Bereich der Wissenssicherheit. Die (optionale) begleitende Matrix ermöglicht es der Hochschulleitung, die Selbstbewertung anhand eines Ampelsystems zu bewerten.

Für wen: Die Selbstbewertung richtet sich an Forschende, die eine neue internationale Zusammenarbeit beginnen. Die Bewertungsmatrix ist ein Instrument für die Hochschulleitung, das die Entscheidungsfindung unterstützt.

Wann: Vor Abschluss einer internationalen Zusammenarbeit.

- Deutscher Akademischer Austauschdienst/Kiwi (2025): [Die KIWi-Checkliste Wissenssicherheit](#) (auf Deutsch)

Was: Die KIWi-Checkliste Wissenssicherheit ist ein praktisches Instrument zur Selbsteinschätzung, das dabei hilft, Risiken der Wissenssicherheit in internationalen Forschungskooperationen zu identifizieren und zu reflektieren. Dies geschieht anhand eines strukturierten Fragenkatalogs, der die Bereiche Partner, Finanzierung, Exportkontrollen, geistiges Eigentum und Forschungsethik abdeckt.

Für wen: Einzelne Forschende oder die Leitung bzw. Verwaltung einer Einrichtung bei der Umsetzung institutioneller Prozesse.

Wann: Vor oder während des Aufbaus internationaler Forschungskooperationen, als erste Risikobewertung.

- Europäische Kommission (2024): [Forschungssicherheit – Bausteine für die Risikobewertung](#)

Was: Die „Bausteine für die Risikobewertung“ der Europäischen Kommission bieten einen Rahmen für die Bewertung von Forschungssicherheitsrisiken in internationalen Forschungs- und Innovationskooperationen. Sie schlagen eine strukturierte, kontextbezogene Bewertung vor, die das Forschungsgebiet, die Partner, den Länderkontext und projektspezifische Faktoren abdeckt, um eine fundierte Entscheidungsfindung zu unterstützen, anstatt die Zusammenarbeit einzuschränken.

Für wen: Forschungseinrichtungen, Forschungsförderer und Hochschulen.

Wann: Vor dem Aufbau internationaler Forschungspartnerschaften oder der Vergabe von Forschungsmitteln.

3.2 Embargos und Sanktionen

- Schweiz:
 - CH-SECO: [«Suchmaschine» zur Ermittlung von Sanktionsobjekten](#) (Personen/Organisationen)
 - CH-SECO: [Schweizer Sanktionsmassnahmen](#) (Inhalte verfügbar auf Deutsch, Französisch oder Italienisch)
- Ausländische Bestimmungen mit extraterritorialer Geltung
(US-Sanktionen und Embargos müssen von allen US-Bürger:innen und Inhaber:innen einer Green Card angewendet werden, unabhängig von ihrem Wohnsitz. EU-Sanktionen müssen von allen EU-Bürger:innen und juristischen Personen, die nach dem Recht eines EU-Mitgliedstaats gegründet oder registriert sind, eingehalten werden – unabhängig von ihrem Wohnsitz oder Sitz. Gleiches gilt für britische Staatsbürger:innen und juristische Personen in Bezug auf britische Sanktionen)
 - US-Office of Foreign Asset Control (OFAC): [Sanktionsprogramme und Länderinformationen](#)

- US-OFAC: [Suche in der Sanktionsliste](#)
- EU-Sanktionen und Embargos: [Sanktionskarte](#)
- Britische Sanktionen und Embargos: [Handelssanktionen, Waffenembargos und andere Handelsbeschränkungen – GOV.UK](#)

3.3 Bewertung der Netzwerke von Institutionen oder Forscher:innen

Bei den folgenden Tools handelt es sich um kommerzielle Lösungen, die relativ kostspielig sind und deren Integration in die Sorgfaltsprüfungsprozesse einer Institution zu Abhängigkeiten führen kann. Die meisten der vorgestellten Tools konzentrieren sich auf die Aufdeckung von Netzwerken, an denen sanktionierte oder militärische Partner beteiligt sind.

Die Europäische Kommission arbeitet derzeit (2026) an der Entwicklung einer eigenen, öffentlichen Sorgfaltspflicht-Plattform.

- [China Defence Universities Tracker](#)

Ein abonnementbasiertes Tool, das mehr als 180 chinesische Einrichtungen mit Verbindungen zu den Bereichen Verteidigung, Nachrichtendienste und Technologieforschung überwacht. Es ermöglicht Nutzern, potenzielle Dual-Use-Fähigkeiten zu untersuchen, relevante Sanktionslisten einzusehen und Risiken globaler Zusammenarbeit zu bewerten. Der Tracker ist als gezielte analytische Ressource zum Verständnis institutioneller Beziehungen konzipiert. Er ist weder ein Tool zur Profilerstellung von Einzelpersonen noch eine Grundlage für pauschale Beschränkungen und sollte nicht als schwarze Liste interpretiert werden. Vielmehr dient er dazu, fundierte und verhältnismässige Entscheidungen zu unterstützen. Der Tracker ist zwar umfangreich, aber nicht vollständig. Nicht erfasste Institutionen können dennoch Risiken darstellen, und die Einträge in der Datenbank geben möglicherweise nicht den vollen Umfang oder die Art der Verbindungen einer Institution zum Verteidigungs- und Sicherheitssektor wieder.

- [Strider Technologies](#)

Strider ist ein abonnementbasiertes Tool, das einen externen, auf Open-Source-Informationen basierenden Überblick über die globale Forschungslandschaft bietet. Es identifiziert Diskrepanzen zwischen den von einer Person angegebenen Erfahrungen und öffentlich zugänglichen Daten, die auf frühere Forschungsleistungen, institutionelles Engagement und langjährige berufliche Präsenz zurückzuführen sind. Darüber hinaus bietet es einen einheitlichen Überblick über Organisationen, Mitarbeiter:innen und Forschungseinheiten sowie eine kontinuierliche Überwachung von Risiken durch Nationalstaaten.

- [Kharon](#)

Kharon ist eine Risikoinformationsplattform, die die Einhaltung von Sanktionen, die Sorgfaltspflicht bei der Exportkontrolle, das Risikomanagement in der Lieferkette und die Überprüfung von Drittparteien unterstützt. Sie nutzt Open-Source-Informationen, Netzwerkanalysen und Datenanalysen, um verborgene Beziehungen zwischen Personen, Organisationen, Eigentumsverhältnissen sowie sanktionierten oder risikoreichen Akteuren aufzudecken.

- [Xapien](#)

Xapien ist eine KI-gestützte Plattform für Due-Diligence-Prüfungen und die Risikobewertung von Dritten. Sie automatisiert Hintergrundrecherchen zu Personen und Organisationen, indem sie Informationen aus dem offenen Internet, Nachrichtenquellen, Unternehmensregistern, Sanktions-

und Beobachtungslisten sowie anderen kommerziellen Datensätzen zu einem einzigen, quellenbelegten Bericht zusammenführt.

- [Dimensions Research Security](#)

Dieses abonnementbasierte Tool bildet internationale Verbindungen, Kooperationen und Finanzierungsströme ab. Es unterstützt die Identifizierung von Doppelmandaten, der Teilnahme an ausländischen Talentprogrammen und potenzieller Verbindungen zu sanktionierten Einrichtungen und hilft Institutionen so, Kooperationsrisiken besser einzuschätzen und zu steuern.

u^b

3.4 Listen kritischer Einrichtungen aufgrund militärischer Nähe

- Regierung von Kanada: [Liste namentlich genannter Forschungseinrichtungen](#)
- [Einrichtungen, die als chinesische Militärunternehmen identifiziert wurden, die in den USA tätig sind](#)
- [Japanische Endnutzerliste](#)
- Australian Strategic Policy Institute: [China Defence Universities Tracker](#)

3.5 Weitere Überlegungen

- [Rechtsstaatlichkeitsindex des World Justice Project](#)
- [Demokratieindex](#)
- [Menschenrechtsindex 2025: Rangliste der besten und schlechtesten Länder](#)
- [Index der menschlichen Freiheit](#)
- [Index von Freedom House](#)
- [Index der akademischen Freiheit](#)
- [Korruptionswahrnehmungsindex](#)

4. Infrastruktur

Risiken für die Wissenssicherheit im Zusammenhang mit der Infrastruktur können mithilfe des in Kapitel 1, Abschnitt 4 vorgeschlagenen Wissenssicherheitsmanagementplans bewertet werden.

Anhänge

Download über den Link

Englisch (Original)

1. [Do's and Don'ts for Knowledge Security in Open Science](#)
2. [Slides on "Introduction to Knowledge Security in Open Science"](#)
3. [Knowledge Security Management Plan \(for Open Science\)](#)
4. [Decision tree on data sharing \(Knowledge Security in Open Science\)](#)
5. [Knowledge Security risks in Open Science: mitigation measures](#)
6. [Questionnaire on Dual-use potential](#)
7. [Checklist for researchers and evaluation matrix for institutional management for international collaborations](#)

Übersetzungen in Deutsch

1. [«Do's and Don'ts» für Wissenssicherheit in Open Science](#)
2. [Folien zum Thema «Einführung in die Wissenssicherheit in Open Science»](#)
3. [Plan zum Wissenssicherheitsmanagement \(für Open Science\)](#)
4. [Entscheidungsbaum zum Datenaustausch \(Wissenssicherheit in Open Science\)](#)
5. [Risiken für die Wissenssicherheit in Open Science: Massnahmen zur Risikominderung](#)
6. [Fragebogen zum Dual-Use-Potenzial](#)
7. [Checkliste für Forschende und Bewertungsmatrix für das institutionelle Management bei internationalen Kooperationen](#)

u^b