

*u<sup>b</sup>*

---

*b*

**UNIVERSITÄT  
BERN**

*u<sup>b</sup>*

# Knowledge Security and Open Science

## Knowledge without borders – but with locks?

**Kei Hannah Brodersen, Wissenschaftliche Mitarbeiterin Compliance und Forschungsförderung**  
Lunch & Learn Open Science, 24 April 2026

# Contents

1. Background
2. Context: Geopolitics and universities/HEIs
3. What is Knowledge Security?
4. Open Science
5. What are risks to Knowledge Security in Open Science?
6. What are Knowledge Security risks in Open Science?
7. How to detect Knowledge Security risks in Open Science?
8. Knowledge Security Management Plan
9. Knowledge Security in Open Science
10. Institutional risk management context

# Background

- SWU mandate on «Knowledge Security and Open Science»
  - Operationalise «as open as possible, as closed as necessary»
  - Report and toolbox for institutional management
- Collaboration between UniBE, Center for Security Studies (CSS) of ETHZ, University of Applied Sciences and Arts Western Switzerland (HES-SO)
- End of project: July 2026

# Context: Geopolitics and universities

- Geopolitics
  - Return of great-power rivalry
  - Wars and rising geopolitical instability
  - Technology becoming a strategic asset
  - Interdependence as leverage
  - Cyber and intelligence competition

# Context: Geopolitics and universities

- Characteristics of universities/research institutions
  - Sit at the intersection of knowledge production, technology development, talent mobility, and political influence (= strategic assets)
  - Openness of research sector (Open Science, exchange of information, collaboration with diverse partners, physical access to buildings, international research groups, etc)
  - Switzerland: high scientific standards
- → institutions strengthen governance and security frameworks

*u*<sup>b</sup>

# What is Knowledge Security?

- Strategic approach in science, technology, and innovation that democratic states use to address risks emerging from a globalised and highly interconnected research environment
- Aims:
  - Safeguard national/institutional interests (esp. national security) and competitiveness
  - Protect scientific integrity and values
  - Ensure responsible international cooperation
  - → make science possible, but safe

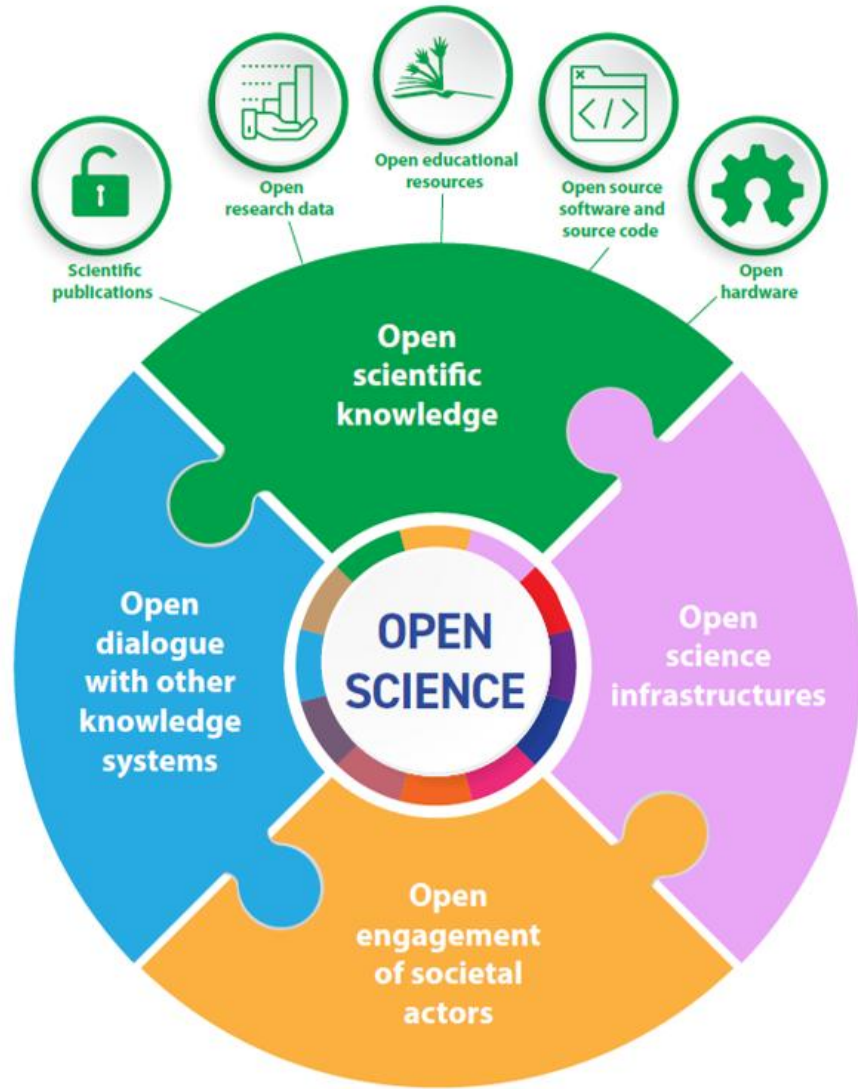
$u^b$

# What is Knowledge Security?

## Core elements

- Preventing the unwanted transfer of sensitive knowledge, data, or technology
  - Espionage or hacking/theft
- Limiting foreign interference or influence in research
  - Swiss researchers put under pressure abroad
  - Foreign researchers in Switzerland put under pressure by home country (to influence research, to exert pressure on compatriots)
  - Otherwise influencing the research agenda or outputs in Switzerland
- Reducing strategic dependencies that may pose security or economic risks
  - Too close collaborations with competitors
- Considering ethical dimensions to ensure research is not used for harmful or authoritarian purposes
  - Decontextualising knowledge, for instance for military purposes

# Open Science



- Swiss National Open Access Strategy
- Swiss National Open Research Data Strategy

# What are risks to Knowledge Security in Open Science?

## Our categorisation

<p><b>Unwanted knowledge transfer</b></p>	<p>Regulatory non-compliance in knowledge disclosure (= knowledge sharing is regulatory infringement) <i>E.g. publication violates export controls, data protection or IP laws</i></p>	<p>Misappropriation or unauthorised exfiltration of knowledge (= knowledge gets stolen) <i>E.g. closed data employed in an OS project are stolen via a cyberattack</i></p>
<p><b>Foreign interference</b></p>	<p>Undue influence, manipulation or corruption of knowledge (= knowledge gets altered or influenced) <i>E.g. published data is altered to fit a political narrative; open data erased because of political censorship</i></p>	
<p><b>Strategic dependencies</b></p>		
<p><b>Misuse</b></p>	<p>Misuse of scientific knowledge (= knowledge gets misused) <i>E.g. data is decontextualised and misused for human rights violations</i></p>	

*u*<sup>b</sup>

# How to detect risks to Knowledge Security in Open Science?

## Knowledge Security Management Plan

### Categories

- a) General legal, regulatory, and contractual constraints
- b) Data sensitivity and misuse
- c) Foreign dependencies and influence
- d) Data management
- e) Infrastructure
- f) Access controls

# Knowledge Security Management Plan

## A comprehensive questionnaire



### Knowledge Security Management Plan (for Open Science)

#### A) General legal, regulatory, and contractual constraints

- 1) What is the applicable legal regime for the publication of this data (e.g. Swiss law only, or additional foreign laws)?
- 2) Could publication of this data (or parts of it) be restricted by:
  - a) Data protection laws?
  - b) Intellectual property laws?
  - c) Export control or sanctions regimes?
- 3) Could publication conflict with contracts or agreements with third parties?
- 4) Are there foreseeable legal or policy risks that could force data removal or restriction in the future?

#### B) Data sensitivity and misuse

- 5) Does the data concern a sensitive research area under national security considerations:
  - a) Dual-use research?
  - b) Emerging technologies?
  - c) AI and IT technologies?
  - d) Geopolitics?
  - e) Economics?
- 6) Could the data be used to target individuals, groups, institutions, ecosystems, or states?
- 7) Is the data politically, socially, or ethically sensitive because it includes:
  - a) Personal data?
  - b) Political affiliation?
  - c) Religion?
  - d) Gender identity?
  - e) Criminal records?
  - f) Health?
  - g) Financial data?
  - h) Business secrets?
  - i) Security data?
- 8) Could the dataset be re-identified using external data sources?
- 9) Could the dataset be combined with other datasets to enable harmful insights or unintended capabilities?
- 10) Is the data produced or managed by individuals under political pressure?
- 11) Are there undisclosed affiliations or advisory roles with external entities?

- 12) Is there a risk of coercion, conflicts of interest, or undue external influence on key personnel?
- 13) Are conflicts of interest formally declared and reviewed?

#### C) Foreign dependencies and influence

- 14) Is long-term project funding secured?
- 15) Is your project funded by:
  - a) Your institution?
  - b) Swiss institutions?
  - c) EU institutions?
  - d) US institutions?
  - e) Other countries (e.g. China, Russia, Iran)?
- 16) Is data publishing funded by:
  - a) Your institution?
  - b) Swiss institutions?
  - c) EU institutions?
  - d) US institutions?
  - e) Other countries (e.g. China, Russia, Iran)?
- 17) Is data storage funded by:
  - a) Your institution?
  - b) Swiss institutions?
  - c) EU institutions?
  - d) US institutions?
  - e) Other countries (e.g. China, Russia, Iran)?
- 18) Is data stored in a repository or platform owned by:
  - a) Your institution?
  - b) Swiss institutions?
  - c) EU institutions?
  - d) US institutions?
  - e) Other countries (e.g. China, Russia, Iran)?

- 19) Do key researchers depend on continued funding from a single external actor?
- 20) Is there a risk of coercion, conflicts of interest, or undue external influence on key personnel?
- 21) Are early-career researchers particularly exposed to funding or career pressure?
- 22) Are you responsible for defining research questions, scope, and methodology?
- 23) Can funders or partners veto publications or results?
- 24) Do funders or partners have formal or informal influence over research design, interpretation, or publication?
- 25) Are there contractual clauses allowing review, delay, or modification of outputs?
- 26) Is academic independence explicitly guaranteed in funding agreements?
- 27) Are results subject to pre-publication review by external actors?
- 28) Is selective reporting or suppression of unfavorable results possible?
- 29) Could foreign laws or regulations compel data alteration, disclosure, or censorship?
- 30) Does the host jurisdiction allow government intervention in research activities?
- 31) What is the likelihood of undue influence (low / medium / high)?
- 32) What is the impact if results were altered or biased?
- 33) Is the influence risk systemic (structural dependency) or situational (individual case)?

#### D) Data management

- 34) Is the data stored in open or widely supported formats?

- 35) Do you have a plan to prevent data obsolescence (e.g. format migration)?
- 36) Does the data include hidden or embedded metadata?
- 37) Do you need to upload or manage large corpora of data (>100 GB)?
- 38) Are metadata and documentation preserved together with the data?
- 39) Are previous versions of your data:
  - a) Preserved and restorable?
  - b) Overwritten or deleted?
- 40) Is there a defined process for updating datasets without losing history?
- 41) Is there a clear provenance trail for data and metadata?
- 42) Are analysis pipelines reproducible and documented?
- 43) Are data integrity checks in place?
- 44) Is documentation sufficient to ensure long-term interpretability?
- 45) Is data and metadata discoverable via persistent identifiers?
- 46) Is there a designated entity responsible for long-term stewardship?
- 47) Are responsibilities over data documented and resilient to personnel changes?
- 48) Are ownership and custodianship clearly defined?
- 49) Are staff and collaborators trained in data security?
- 50) Is data sharing conducted via institutional infrastructure?
- 51) Is data shared or managed via non-institutional tools (e.g. personal cloud services)?
- 52) Is data transfer encrypted (secure APIs, encrypted channels)?
- 53) Is data ever downloaded locally by users?
- 54) Are exports logged and monitored?
- 55) Are derivative datasets or subsets shared externally?
- 56) Is data management and sharing governed by written contracts or agreements?

#### E) Infrastructure

- 57) Is the repository designed for long-term preservation?
- 58) Are backups performed regularly and stored redundantly?
- 59) Are external mirrors or secondary archives available?
- 60) Is there a plan for rehosting if the repository becomes unavailable?
- 61) Could access restrictions, policy changes, or platform shutdowns impair future retrieval?
- 62) Does the hosting platform provide documented reliability and disaster-recovery measures?
- 63) Is the platform regularly audited for security and resilience?
- 64) Does the repository comply with recognised archiving or trust standards?
- 65) Are controls in place to prevent or recover from cyber incidents?

#### F) Access controls

- 66) Is data classified by sensitivity and access control level?
- 67) Is sensitive access concentrated in a small number of individuals?
- 68) Is the data protected by digital access controls?
- 69) Is the data protected by physical access controls (where applicable)?
- 70) Are access rights:
  - a) Role-based and least-privilege?
  - b) Time-limited and regularly reviewed?
- 71) Are accounts promptly revoked when personnel leave?
- 72) Is multi-factor authentication required?
- 73) Is access logged and monitored?
- 74) Are alerts in place for unusual access patterns or bulk downloads?

*u<sup>b</sup>*

# Knowledge Security Management Plan

## A comprehensive questionnaire

- Purpose
  - Detect possible Knowledge Security risks in Open Science
  - Basis for decision-making on risk-taking
  - Identify mitigation measures to counter risks
- Audience: researchers, in collaboration with Knowledge Security- and Open Science officers (possibility to segment the questionnaire and assign roles to fill it in)

# Knowledge Security in Open Science

## Risk mitigation measures

### Knowledge Security risks in Open Science: Risk mitigation measures

#### A) General legal, regulatory, and contractual constraints

- a. Legal mapping and clearance
  - Perform an upfront legal regime mapping (Swiss, EU, US, third-country laws).
- b. Data protection compliance
  - Apply privacy-by-design and privacy-by-default principles.
  - Conduct a Data Protection Impact Assessment (DPIA) where personal data is involved.
  - Anonymise or pseudonymise data; publish only aggregated or derived datasets where possible.
  - Negotiate Non-disclosure agreements, data processing agreements or data protection and confidentiality clauses.
  - Consider restricting access from certain countries (e.g. countries with questionable data protection regimes).
- c. IP and licensing safeguards
  - Conduct IP ownership audits before publication.
  - Use clear open licenses (e.g. CC-BY, CC-BY-NC) consistent with IP constraints.
  - Exclude or embargo IP-sensitive components.
- d. Export control and sanctions screening
  - Screen datasets against export control lists and sanctions regimes.
  - Obtain relevant licences for publication or sharing, if applicable.
  - Segment or restrict access to controlled elements if necessary.
  - Consider restricting access from certain countries (e.g. embargo countries or countries with a low human rights index, depending on the technology).
- e. Contractual risk management
  - Review all third-party agreements for publication restrictions.
  - Renegotiate or document explicit publication rights where unclear.
  - Maintain a contract registry linked to datasets.
- f. Future risk preparedness
  - Define responsibilities and governance for responding to legal or policy changes.

#### B) Data sensitivity and misuse

- a. Sensitivity classification
  - Classify datasets by misuse potential (low / medium / high).
  - Consult with an (ethics) committee on the potential for data misuse.
  - Apply stricter controls to dual-use, emerging technology, AI, geopolitical, or economic data.
- b. Misuse and threat modeling
  - Conduct misuse scenario analysis (who could misuse, how, and with what impact).

- Restrict access that pose elevated misuse risk. Identify users before granting access.
  - Consider licensing or data-use restrictions with terms that prohibit harmful or unethical use.
  - Consider obliging users to accept conditions before accessing restricted data. Provide responsible use guidelines.
- c. Risk-minimised publication
    - Release reduced-resolution, delayed, or synthetic datasets where risks are high.
    - Use controlled-access repositories for sensitive components.
  - d. Re-identification risk reduction
    - Test re-identification risks using external datasets.
  - e. Combination risk controls
    - Provide contextual documentation warning against harmful recombination.
  - f. Researcher protection
    - Provide institutional backing and legal support for researchers under political pressure.
    - Avoid single-person control over sensitive datasets.

#### C) Foreign dependencies and influence

- a. Funding diversification
  - Avoid reliance on a single external funder, especially foreign state-linked entities.
  - Document contingency plans for funding withdrawal.
- b. Transparency of funding sources
  - Publicly disclose all funding sources linked to data creation, storage, and publication.
  - Label datasets with funding provenance metadata.
- c. Independence safeguards
  - Ensure funding contracts explicitly guarantee academic freedom.
  - Prohibit funder veto rights over results or publications.
- d. Governance firewalls
  - Use independent steering or ethics committees for oversight.
- e. Early-career researcher protection
  - Assign senior mentors to shield early-career researchers from undue pressure.
  - Ensure employment and authorship decisions are insulated from funder influence.
- f. Foreign legal exposure management
  - Avoid storing or processing sensitive data under jurisdictions with coercive disclosure laws.
  - Use legal entities and hosting locations with strong research autonomy protections.
- g. Influence risk monitoring
  - Periodically reassess influence likelihood and impact.
  - Document whether risks are structural or situational and adjust controls accordingly.

#### D) Data management

- a. Standards-based data formats
  - Use open, non-proprietary, community-supported formats.
  - Maintain documented format migration plans.
- b. Metadata hygiene
  - Strip hidden or embedded metadata before publication.
  - Preserve essential provenance and context metadata explicitly.
- c. Versioning and provenance
  - Implement robust version control with immutable records.
  - Preserve previous versions with clear change logs.
- d. Reproducibility and integrity
  - Document analysis pipelines, software versions, and dependencies.
  - Use checksums, hashes, and integrity verification tools.
- e. Long-term interpretability
  - Provide rich documentation, codebooks, and readme files.
  - Assign persistent identifiers (DOIs) to datasets and versions.
- f. Stewardship and responsibility
  - Designate a long-term data steward or institutional unit.
  - Document roles, ownership, and custodianship.
- g. Training and awareness
  - Provide mandatory training on data security and responsible sharing.
  - Update training to reflect evolving threats.
- h. Secure sharing practices
  - Use institutional infrastructure for sharing and storage.
  - Prohibit or strictly regulate use of personal cloud services.
  - Encrypt data at rest.
- i. Controlled data flows
  - Encrypt data transfers.
  - Log, monitor, and audit data exports.
  - Govern derivative dataset sharing via agreements.

#### E) Infrastructure

- a. Trusted repositories
  - Use repositories designed for long-term preservation.
  - Prefer platforms certified under recognised trust standards.
- b. Resilience and continuity
  - Implement redundant backups in geographically separate locations.
  - Maintain mirror sites or secondary archives.
- c. Exit and rehosting planning
  - Develop a rehosting and migration plan if platforms fail or policies change.
  - Ensure data portability and contractual exit rights.
- d. Security and disaster recovery
  - Require documented disaster recovery plans.

#### F) Access controls

- a. Data classification and access tiers
  - Define access levels (open, registered, restricted, controlled).
  - Apply stricter controls to higher-risk data.
- b. Least-privilege access

- Regularly review and time-limit permissions.
  - c. Strong authentication
    - Choose repositories using multi-factor authentication for sensitive systems and that prohibit shared or generic accounts.
  - d. Monitoring and logging
    - Choose repositories that log all access and downloads.
    - Choose repositories that monitor for anomalous patterns (e.g. bulk downloads) and that alert in case of suspicious behavior.
- #### G) General
- a. Training and awareness raising
    - Inform and train all researchers involved in your project on risks of unwanted knowledge transfer, foreign interference and influence, dependencies and misuse in relation to Open Science.
    - Refresh training in case of policy changes.

*u*<sup>b</sup>

# Knowledge Security in Open Science

Two sides of the same coin

Main take-aways:

- As open as possible, as closed as necessary.

$u^b$

# Knowledge Security in Open Science

Two sides of the same coin

Main take-aways:

- ~~• As open as possible, as closed as necessary.~~

$u^b$

# Knowledge Security in Open Science

## Two sides of the same coin

Main take-aways:

- ~~As open as possible, as closed as necessary.~~
- Openness and security are complementary and mutually reinforcing.
  - → if Open Science is done well, there are little risks to knowledge security
  - → Open Science as a chance

*u<sup>b</sup>*

# Institutional risk management context

## Integration into existing processes

- Options (among others):
  - Integrate into Data Management Plans (DMP), integrate DMP into Knowledge Security Management Plan, or additional to DMPs
  - Integrate into research project risk assessment
  - Integrate into research project ethics assessment
- Responsibilities
  - Risk assessment
  - Risk mitigation
  - Decision making
- Roles
  - Researchers
  - Research management/administration
  - Commissions
  - University board

*u*<sup>b</sup>

# Institutional risk management context

## Integration into wider institutional risk analysis

- Questions
  - What do we want to protect? (national security («sensitive technologies») + x (e.g. «crown jewels»))
  - Where/who is what we want to protect? (break it down to institutes/research groups)
  - Where does the danger come from? («risky countries»; to narrow down the workload)

# $u^b$ Questions?

## **Kei Hannah Brodersen**

Wissenschaftliche Mitarbeiterin Compliance und Forschungsförderung

[hannah.brodersen@unibe.ch](mailto:hannah.brodersen@unibe.ch)

+41 31 684 84 91