safeguarding science
SAFEGUARDING-SCIENCE.EU

ein Angebot vom
DLR Projektträger

Due diligence in science: a closer look at personal background checks

Safeguarding Science team
DLR Projektträger

Imprint

Publisher
DLR Projektträger
Deutsches Zentrum für Luft- und Raumfahrt e.V. (German Aerospace Center)
Heinrich-Konen-Straße 1
53227 Bonn, Germany

DLR-PT.de

Editor
DLR Projektträger
European and International Cooperation
Department *Asia, Oceania*

Bonn, November 2025

ISBN 978-3-949245-35-0

Background

Universities and research institutions are increasingly conducting background checks on individuals, for instance when granting access to sensitive research data or security-relevant technologies. Depending on the institution, such checks may be carried out by different departments (e.g. Human Resources, Export Control, or the International Office) and are integrated into various administrative processes.

In 2024, the DLR Projektträger (DLR-PT) published the "Due Diligence in Science" manual[1], a guideline for developing assessment processes at universities and research institutions. Among other topics, it addresses background checks on individuals, including cooperation partners, invited guest researchers, and international researchers with whom contractual obligations are to be concluded.

At DLR-PT's invitation, a working meeting was held in April 2025 with eight German universities and research institutions that have already established procedures for vetting individuals. The meeting focused on key topics, challenges and processes related to those existing background check procedures. It also resulted in the development of a set of questions that academic institutions should address when developing a systematic background check.

By publishing the discussion results as an addendum to the Due Diligence in Science manual (DDS manual), we aim to provide users with supplementary, in-depth information. As the document is intended as a practical working aid, we have opted for a tabular format that provides an easy overview and allows for quick reference to specific points.

Both the 2024 guidelines nor this addendum are living documents. They do not claim to be exhaustive, nor do they prescribe specific requirements for processes to be established by universities or research institutions. They merely document current practices, which continue to evolve. We therefore welcome feedback from users that can be incorporated into future revisions.

[1] https://www.safeguarding-science.eu/resource/manual-due-diligence-science-assessment-science-cooperation/

Tabular overview of a personal background check process in higher education and research institutions

Categories	Key questions	Proposed approaches / notes
1. Business strategy	1.1 What institutional policy framework guides the implementation of background checks?	Submit a decision paper or strategic policy proposal on the topic to the management and co-determination bodies in order to establish a consistent institutional position and define organisation-specific regulations. This also helps to clarify matters subject to co-determination (e.g. who should be screened, in what manner, and according to which guiding principles).
	1.2 Are there areas within the institution where more extensive background checks may be needed?	Risk profiles or departmental portfolios should be defined as part of the institution's overall strategy, particularly where this is appropriate due to a specific thematic focus, or required by contractual obligations with third parties (for example in the case of U.S. funding or security-related research).
2. (Legal) basics	2.1 Why are background checks conducted, and what is their purpose? Under what circumstances are such checks mandatory? What information may be considered in the background check process? How transparent are the criteria used in decision making? How can organisational liability be prevented?	The process structure, workflow, and responsibilities should be defined in consultation with the legal department in order to ensure legal certainty. Mandatory checks are prescribed in Germany under the Foreign Trade and Payments Act (Außenwirtschaftsrecht). The transfer of knowledge to individuals or institutions, as well as the transmission of technology, may be subject to authorisation requirements or prohibitions. At the same time, it is prohibited to provide any form of economic advantage to listed persons or entities. Consequently, these processes should be reviewed for compliance with the relevant national, European, and where applicable third-country regulations. Further points of reference may include internal institutional rules, management decisions, or strategic policies, direct links to specific

		research projects in sensitive fields, contractual obligations under private law (e.g. purchase agreements for large-scale equipment), or eligibility requirements imposed by funding organisations (for example in the United States). Legal regulations from other jurisdictions may apply both through their extraterritorial reach and through contractual obligations such as nondisclosure agreements or purchase contracts.
	2.2 How are the roles and responsibilities of the responsible unit (i.e. the office or person in charge of background checks) defined and communicated?	The mandate of the responsible unit should be aligned with the relevant legal as well as institution-specific regulations. Within the institution, the mandate needs to be communicated transparently to ensure the responsible unit's authority. The unit's direct reporting lines should likewise be clearly defined and communicated.
	2.3 Which types of background checks or decisions related to conducting background checks require co-determination? Which employment law or other regulations (e.g. anti-discrimination rules) must be taken into account?	See also section 1. The types of background checks that require co-determination should be defined at the institutional level. For instance, pre-employment screenings are typically not subject to such requirements.
	2.4 How is compliance with the General Data Protection Regulation (GDPR) ensured?	Since background checks involve the processing of personal data, data protection requirements, especially those set out in the GDPR, must be ensured throughout the process. All handling of personal data, including access, processing, storage, and deletion, should be carried out in close consultation with the data protection officers.

3. Responsible unit *(refers to the office, department, or designated staff member within a higher education or research institution that is responsible for conducting background checks)*	3.1 Where within the institution is the responsible unit based, and who is responsible for conducting background checks in which cases? Should the process be managed centrally or through a decentralized structure? If decentralised, how can consistency be ensured in terms of mandate and specific background check steps?	Each institution should determine individually where the unit is situated within its organisational structure. Experience shows that assigning the overall responsibility to the export control office can be particularly effective, as legally required checks are already carried out there under foreign trade law. Export control and due diligence are best addressed together, for example by establishing a team or committee for export control, research security, and due diligence in science (DDS). Where appropriate, this team should work closely with a Risk Assessment Committee, the Commission for Research Involving Significant Security Risks (FEG) and/or the Ethics Commission for Security-Relevant Research (KEF), as well as other relevant bodies.
	3.2 How can the responsible unit build and strengthen the expertise required to carry out background checks?	The expertise of the responsible unit can be strengthened and further developed through targeted qualification and training measures, as well as through exchange with comparable universities and research institutions. Participation in relevant networks is also recommended, for example at the state level or through existing associations or initiatives such as the BundesArbeitsKreis Exportkontrolle Academia (BAKEA) or the European Export Control Association for Research Organisations (EECARO). Where necessary, external support or advisory services may also be involved.
	3.3 What level of effort and resources can be estimated for the responsible unit and for the overall process? Are internal resources sufficient, or is external support required?	Experience to date indicates that resource requirements vary significantly depending on the scope of the unit's responsibilities. A general standard or benchmark therefore cannot be currently defined.

4. Involvement of third parties	4.1 How are disputed cases and those requiring a careful weighing of risks and opportunities addressed?	In cases of disagreement, mediation or escalation mechanisms should be established between applicants and the responsible unit. Depending on the nature and complexity of the case, decisions may be taken at different institutional levels, for example by a Due Diligence in Science (DDS) committee, a risk assessment committee, the Ethics Commission for Security-Relevant Research (KEF) or the Commission for Research Involving Significant Security Risks (FEG).
	4.2 Which external bodies can be involved in cases requiring further clarification or review?	Depending on the area of responsibility and the nature and complexity of the case, external bodies such as the Federal Office for the Protection of the Constitution (BfV) or the respective State Office for the Protection of the Constitution (LfV), the Federal Office of Economics and Export Control (BAFA), the Federal Intelligence Service (BND) or the Federal Foreign Office (AA) may be consulted.
	4.3 Which external bodies can be involved when specific scientific or technical expertise is needed?	Depending on the field of research, each institution should determine which external bodies can be involved to provide expert advice. Examples include the Friedrich Loeffler Institute for research on zoonotic pathogens and the Robert Koch Institute (RKI) for research involving viruses and other infectious agents.
5. Review process	5.1 How should the background check process be set up?	The process should be established as a standardised, preferably digital workflow with clearly defined responsibilities and, where possible, timelines.
	5.2 How are the background check procedures received and evaluated?	The process should be clearly communicated within the institution to ensure transparency and raise awareness. Regular monitoring and evaluations are necessary to assess the effectiveness of the procedures. Potential workarounds may indicate that the procedures are not fully supported or perceived

		as too burdensome. Monitoring should therefore also take into account the acceptance among those involved.
	5.3 At what stage and in which department is the background check process initiated?	The background check process should be triggered automatically as part of a standardized procedure that applies to all individuals subject to review within the institution. It should not occur on a random or case-by-case basis. Ideally, the process should be initiated as early as possible, for example before issuing an invitation letter or hosting agreement, or upon receipt of an application. Possible triggers include the processing of an application by the HR department, activation in the Identity Management (IdM) system or the granting of IT access rights, as well as the issuance of campus access permissions.
	5.4 Which documents must be submitted for the background check, and in what format?	The responsible unit or management should develop standardized, digitally fillable questionnaires and checklists. Examples and suggestions can be found in the annex of the DDS manual. All information should be collected in German or English and, where applicable, additionally in the person's native language using non-Latin script. Required documentation may include a CV, the certificate of the most recent academic degree, a residence permit (including any supplementary conditions, where relevant), a self-disclosure form (as defined by the institutions, for example concerning criminal records or memberships), lists of publications and patents, and a project description including all equipment and goods.
	5.5 Which software, databases or legal sources are used for the background checks?	The responsible unit should regularly assess which sources and tools are relevant to the institution and, where necessary, obtain

		the corresponding licenses. Joint procurement with other institutions or through federal states may also be considered. Examples for commonly used resources include sanction list software such as ZERBERUS and financial sanctions lists (FiSaLis) as well as the Dual-Use Regulation (EU) 2021/821, the Foreign Trade and Payments Ordinance (AWV) and the Foreign Trade and Payments Act (AWG). In addition, bibliometric analysis tools such as Science OS, Dimensions, Scopus, Web of Science, and Open Alex, as well as specialized risk assessment software such as the ASPI Defence Universities Tracker, Datenna, Strider, Kharon, and IranWatch may be used. The Academic Freedom Index can also serve as a supplementary information source.
6. Assessment criteria	6.1 Should red lines be defined?	Clear exclusion criteria should be established that prevent access to the institution, for example in cases involving visiting researchers affiliated with military institutes.
	6.2 Which groups of individuals are subject to review?	The law does not define the categories of persons to be reviewed but refers to the transfer of specific knowledge that may require assessment. Each institution should individually determine the scope of individuals to be reviewed, which also defines the resources required. Typical groups of people subject to review include individuals in pre-employment or pre-boarding processes, guest researchers, doctoral candidates, interns, student or research assistants, and staff working in critical infrastructure.
	6.3 Are persons of certain nationalities subject to review?	Institutions may decide to conduct reviews for individuals from specific countries, for example all non-EU states or those listed under EU001 in accordance with the Foreign Trade and Payments Ordinance (AWV).

	6.4 Are individuals affiliated with certain institutes reviewed?	
	6.5 What role do previous affiliations play in the review?	Previous career steps and institutional affiliations may be a relevant criterion.
	6.6 Are individuals with dual affiliations reviewed?	
	6.7 Are non-academic career steps, such as military service, taken into account?	
	6.8 Is an individual's source of funding taken into account?	If applicants bring their own funding, the funding source may justify further examination. Institutions may decide that specific funding sources automatically trigger a review, regardless of research topic or duration of stay.
	6.9 Does the planned duration of stay influence who is reviewed?	Some institutions conduct reviews only after a defined minimum stay, for example four months.
	6.10 Are individuals reviewed based on their research topics or application areas?	Depending on the institution's profile, certain research areas may require particular attention. Some institutions use internal risk profiles or lists of sensitive research areas issued by the EU or national authorities. Research projects or proposals should include thematic keywords and short subject descriptions.
	6.11 Which research infrastructure will be used?	Certain equipment or technologies may be access-restricted, for instance devices from US manufacturers under specific contract terms. Project descriptions should specify any intended use of such equipment.

	6.12 Are individuals reviewed based on specific methodological expertise?	Depending on the institution's profile, certain methodological skills may require review. Project descriptions should indicate which methods are applied or to be learned.
	6.13 Are ethical criteria defined for review?	Ethical considerations should be included where relevant to the research field. The project or proposal should address any ethical aspects. For security-relevant research, the Commission for Ethics in Security Relevant Research (KEF) should be consulted.
	6.14 Is ownership of research results considered?	Regulations on intellectual property should take into account dual affiliations, funding arrangements, and contractual obligations.
	6.15 Are US, UK, or other foreign regulations taken into account?	Where cooperation with partners in third countries exists, institutions should consider whether foreign regulations need to be observed to avoid jeopardizing ongoing collaborations. Checklists may include questions such as whether US citizens are involved, US goods are used, or US research funding is provided.
	6.16 Does a person's involvement in a project have implications for others?	Possible overlaps with third-country regulations affecting other researchers should be considered – for example, if collaboration with individuals from sanctioned states could have consequences for project partners.
7. Decision-making process and documentation	7.1 How is the outcome of the review determined, and what are the consequences?	The outcome of the background check, including any conditions or restrictions, must be clearly documented and communicated transparently. Where a high number of background checks is conducted, standardising review protocols is essential to ensure consistency and transparency.

	7.2 How are decisions made, and who makes them?	See also point 3.1. Depending on the complexity of the case, decisions may be taken at different levels. Simple, clear-cut cases are usually decided directly by the responsible unit. Disputed cases should involve the risk assessment committee, where available, institutional leadership and, if necessary, the legal department. Special or exceptional cases may require separate procedures.
	7.3 How is the outcome of the review documented and communicated?	The outcome of the review should be recorded within a digital workflow. In straightforward cases, decisions can be communicated digitally.