Handling Security-Relevant Aspects in DFG Funding Activities

Preliminary note

Freedom of research is a central concern of the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation). At the same time, it entails a responsibility to reflect on the potential ethical and security-relevant implications of research projects. In March 2018, the DFG added guidance on handling security-relevant aspects of research projects to its guidelines. Since 2024, the guidelines have also explicitly addressed risks arising in connection with international cooperation.

The aim of including these issues in proposals is to raise awareness among applicants and institutions at an early stage and encourage them to carefully weigh the potential knowledge gain and potential uses against security-relevant considerations. This includes identifying and assessing potential scenarios involving misuse and risks arising from international cooperation and where necessary limiting these by adopting appropriate measures.

1. Information on security-relevant aspects

Applicants are asked to consciously assess and responsibly weigh issues that may arise from the research content, research cooperation or potential use of the research results. Relevant information must be provided if there are indications for concern about security-relevant aspects, particularly where:

- there are indications that the research results could potentially generate knowledge, products or technologies that might be directly misused for significantly harmful purposes (dual-use research of concern, DURC);
- cooperation with international partners is planned and the research topic, the partner institution, the research conditions or the political and legal context of the cooperation give rise to indications of security-relevant risks.

In these cases, the proposal must explain:

- how the balance of risks and benefits is assessed and
- what measures are planned to minimise risks.

In order to enable a transparent assessment, it is necessary to specify the relevant indications, any remaining uncertainties, responsibilities within the project and possible alternative approaches. If the rules of the higher education institution or research institution require the involvement of a committee for ethics in security-relevant research or a comparable body, the latter's statement must be enclosed with the proposal.

> ***Assessment under foreign trade law***
> *Irrespective of the ethical assessment of risks and benefits, the applicable provisions of foreign trade law must be observed. Responsibility for this lies with the individuals and research institutions involved; the decision as to whether authorisation is required is made by the competent authorities, in particular the German Federal Office for Economic Affairs and Export Control (BAFA). The DFG funding procedure is not a substitute for this legal assessment.*

2. Principles and roles in connection with DFG funding

Consideration of security-relevant aspects is integrated in the DFG's regular funding procedure. Primary responsibility for identifying, reflecting on and presenting potential risks in a transparent manner lies with applicants and their institutions. The latter assess the balance of risks and benefits and set out appropriate measures to minimise risks. Where required by their institution's rules, they also enclose a statement by the committee for ethics in security-relevant research or a comparable body. The following provide the basis for this:

- the DFG Code of Conduct "Guidelines for Safeguarding Good Research Practice",
- the Recommendations for Handling of Security-Relevant Research, issued by the DFG and Leopoldina and
- the DFG's recommendations on Dealing with Risks in International Research Cooperation.

Once a proposal has been received, the DFG Head Office examines whether security-relevant aspects have been adequately addressed and plausibly assessed in the proposal; additional information is requested where necessary. Based on the recommendations above, reviewers contribute to this assessment within the scope of their subject-specific expertise. The responsible evaluation and decision-making bodies take the available information into account when making the funding decision. Responsibility for addressing security-relevant aspects also continues throughout the project.

3. Stages of the research funding procedure

► Proposal submission

Reflection on security-relevant aspects begins at the project planning stage and must be taken into account both in individual proposals and in proposals under the coordinated programmes. Applicants assess whether the research topic, the proposed methods, the anticipated results, transfer of data and knowledge or international cooperation give rise to security-relevant issues. Where there are indications for concern about security-relevant aspects, these must be set out in the proposal or supplementary information.

The assessment of risks and benefits and the proposed measures to minimise risks must be explained in specific and transparent terms. Where required by the institution's rules, a statement by a committee for ethics in security-relevant research or a comparable body must be enclosed with the proposal.

When preparing their proposal, applicants are asked to familiarise themselves with the recommendations issued by the DFG and Leopoldina on handling security-relevant research and, where relevant, to observe the recommendations on dealing with risks in international research cooperation.

▶ Check by the DFG Head Office

When processing a proposal, the DFG Head Office checks whether security-relevant aspects arising from the research topic, the proposed methods, the anticipated results, transfer of data and knowledge or international cooperation have been addressed and plausibly assessed. The depth of this check depends on the individual case. Under the regular funding procedure, all relevant proposals are checked to ensure that security-relevant aspects have been presented in a transparent manner. If specific indications emerge or questions remain following an initial assessment, a more detailed check may be carried out. For this purpose, additional information and statements may be obtained, supplementary sources of information consulted and further subject-specific or institutional assessments taken into account.

> *Where clarification is required, the applicants and the research institution involved may be asked to provide a supplementary assessment. Depending on the issue concerned, this may involve those with subject-specific responsibility, a committee for ethics in security-relevant research or comparable body and the responsible compliance or export control offices. All relevant aspects and any outstanding issues are presented transparently for consideration during the review, evaluation and decision-making stages.*

▶ Review and evaluation

Where necessary, the DFG Head Office draws reviewers' attention to security-relevant aspects and asks them to assess these within the scope of their subject-specific expertise and based on the above recommendations. Their assessment supports the plausibility check and the subsequent deliberations by the responsible bodies.

During the subsequent evaluation by the responsible review boards, security-relevant aspects are considered alongside the academic quality of the proposal by evaluating whether the risk assessment is transparent and plausible. In the case of on-site reviews under the coordinated programmes, these aspects are included in the reviewers' discussions.

Information that only becomes known during the review or evaluation may require a renewed or supplementary assessment.

▶ Funding decision

The decision is taken by the Joint Committee or the Grants Committees appointed by it. The academic quality of the project is the primary basis for the funding decision. Where indications for concern about security-relevant aspects are apparent, consideration is also given to whether the risks have been assessed in a transparent manner and whether the proposed measures indicate that they will be handled responsibly. In exceptional cases, funding may be declined if it does not appear sufficiently plausible that the project can be carried out responsibly. Where a decision to reject a proposal is based to a significant extent on security-related considerations, these considerations are communicated to the applicant in advance and the applicant is given an opportunity to submit a statement.

The decision is taken with due regard for academic freedom protected under the Basic Law and the principle of proportionality.

▶ Funding and subsequent course of the project

Research objectives, methods, cooperation arrangements and the technical, political or legal framework conditions may change over the course of the project. Project leaders and institutions are therefore expected to continually examine whether the original assessment of risks and benefits remains valid and whether existing measures need to be adapted. Material changes must be clarified with the DFG Head Office in accordance with the funding conditions.

4. Handling nominations for academic prizes

Since the award of an academic prize gives particular visibility to the prizewinner and their institutional environment – as well as to the DFG – security-relevant aspects must be handled with particular care and sensitivity in this context.

Nominees generally cannot be involved in the award selection process, or can only be involved to a limited extent. Relevant information should be available for the selection meeting at the earliest possible stage, since recommendations made by selection committees can only be amended to a limited extent during the subsequent procedure.

The invitation letters accordingly emphasise the need to take safety-related aspects into due account. In order to provide the selection committee with as much of the necessary information as possible for its discussions, the nominator – or the applicant in the case of a self-nomination – may be asked to comment. Reviewers (including review board members where relevant) may also be explicitly asked to provide an assessment of the matter.

All information concerning security-relevant aspects is made transparently available to the selection committees so that it can be assessed during their discussions and taken into account in the selection decision.

5. Funding and procurement of instrumentation and software

Security-relevant aspects may also arise in connection with the funding and procurement of instrumentation and software. Here it should be borne in mind that procuring instrumentation and software is not an end in itself but serves the purpose of enabling and supporting research projects. Questions concerning security-relevant aspects are therefore generally considered in the context of the underlying research project and its subject-specific evaluation. As a rule, procurement in itself does not give rise to a specific security-relevant risk and is therefore generally not evaluated separately.

Nevertheless, statutory requirements and regulations must be observed when instrumentation and software are funded and procured. These are often directly related to the operation and use of the instrumentation and software. Responsibility for ensuring the conditions necessary for safe and legally compliant operation therefore generally lies with the institutions. These include requirements relating to fire safety, occupational health and safety, the Radiation Protection Ordinance and the General Data Protection Regulation.

Where procurement is carried out by the funded institutions themselves, those institutions are responsible for complying with the applicable regulations.

Where procurement is carried out by the DFG, the DFG is likewise bound by the applicable legal framework. The relevant provisions must be observed and the resulting requirements agreed with the funding recipients.

Since these rules are established outside the DFG, they are not covered by specific DFG procedural provisions. Due to European Union competition rules and public procurement regulations, the DFG cannot unilaterally impose restrictions that go beyond the statutory provisions.

Deutsche Forschungsgemeinschaft e. V.
Kennedyallee 40 • 53175 Bonn
Phone: +49 228 885-1
forschungssicherheit@dfg.de
www.dfg.de

Last revised: October 2026