CESAER

Input note

Topic	Managing risks, enabling openness: strengthening research security across Europe
Date of note	10 November 2026
To	EU institutions
From	CESAER

Introduction

CESAER – the strong and united voice of universities of science and technology in Europe – welcomes the opportunity to contribute to the development of an effective and proportionate European approach to research security.

Universities of science and technology work at the cutting edge of research, where research security considerations often arise early. Many of them are frontrunners in developing and implementing practices to address these challenges. Their experience offers valuable insights into what works, what does not, and how to preserve openness while managing evolving risks.

The May 2024 Council recommendation on enhancing research security established a common European approach to anticipating and managing risks related to the undesirable transfer of critical knowledge and technology, malign influence on research, and ethical or integrity violations. It recommended several concrete measures, including a one-stop shop for information and tools, an assessment of options for a European centre of expertise, a voluntary resilience-testing methodology, a European due diligence platform for prospective third-country partners, and greater consistency between safeguards applied under national and EU funding programmes.

Effective research security frameworks are crucial to enable universities and researchers to remain open, excellent and internationally connected while managing risks responsibly. Open science and research security can mutually reinforce each other through a more holistic, integrated approach that supports making informed decisions about managing and mitigating concrete risks, while preserving the benefits of scientific collaboration for Europe's scientific strength and competitiveness. CESAER therefore supports an approach based on collective responsibility, proportionality and practical support, as highlighted during the 2025 Commission flagship conference on research security. Close and continuous engagement with universities of science and technology and other research-performing organisations will be essential to ensure that emerging measures are effective, proportionate and workable in practice.

Building on CESAER's October 2025 input note, 'Research security as a collective responsibility: empowering universities, enabling Europe', and our March 2026 input note 'Clarifying and optimising civil, dual-use and defence research and innovation in future EU funding programmes', this input note presents updated key messages on three policies and tools currently under development:

(i) the proportionate implementation of research security in FP10;
(ii) a European due-diligence platform, and;
(iii) a European centre of expertise on research security.

A major added value of collective responsibility for research security at EU level is the opportunity to connect and build on established and emerging good practices across Europe, particularly those of frontrunner universities, research funding organisations and member states. This allows actors to advance faster by drawing on shared practical experience and evidence. Realising this potential requires timely exchange of relevant information across institutional and national boundaries, removing unnecessary barriers while respecting confidentiality. Lessons about what works and what does not can then inform compatible approaches across Europe, reducing duplication and fragmentation.

CESAER and its Members stand ready to contribute fully to the development of all three policies and tools, bringing the practical experience and perspective of frontrunner universities of science and technology.

1. Implementing research security proportionately in FP10

FP10 should position effective research security as an enabler of continued openness, excellence and international collaboration in European science. These are essential to Europe's scientific strength, but the risks accompanying open and international research have become increasingly difficult to manage in today's geopolitical environment. A proportionate risk-mitigating framework can help universities and researchers manage these risks responsibly while remaining open and internationally connected. To support this, FP10 should align open science and research security guidance and evaluation criteria. Applicants should not be disadvantaged for identifying and appropriately managing research security risks, and duly justified restrictions on sharing should not be treated as failures of open science.

Instead, research security measures in FP10 should be targeted and proportionate, developed with universities and researchers, and supported by clear rules, responsibilities, guidance and adequate resources. Additional research security requirements should apply only where relevant risks have been identified. They should prioritise managing identified risks wherever possible, safeguard academic freedom and university autonomy, and support equal participation of entities from associated countries in accordance with applicable association agreements.

Effective implementation also depends on a European level playing field, supported by common minimum standards and comparable national support, including through the European Research Area (ERA) Act as elaborated in our input note on the ERA Act. Although institutions will continue to have different individual risk appetites, uneven national frameworks and a lack of support and resources can disadvantage universities and fragment the ERA. They may also displace sensitive R&I activities and associated risks towards systems that have less support in place. Addressing these risks requires coherent support while retaining flexibility for proportionate, context-specific implementation.

We therefore call on the EU institutions to:

- **Publish a publicly accessible framework for implementing research security requirements in FP10 before the first FP10 calls are launched.** It should set out clear risk indicators, information requirements, procedures, responsibilities, possible consequences and timelines. It should prioritise proportionate mitigation where possible and clarify when reassessment and adaptation of safeguards are needed as a project's risk profile changes. The framework should draw on relevant experience with the Horizon Europe Security Appraisal Procedure while reflecting the broader scope of research security in FP10. It should be co-designed and tested with universities and researchers, applied consistently across funding bodies and avoid parallel or duplicative requirements.

- **Refrain from introducing blanket, one-size-fits-all, in-depth screening of all FP10 proposals; apply additional research security requirements only where relevant risks have been identified.** Initial checks should be short, proportionate and integrated into existing application processes. Further assessments or security plans should be required only for proposals presenting specific risks, without unnecessarily delaying evaluation or time to grant. Provide optional tools at the European level, including AI assistance where appropriate, to support risk assessment while preserving the crucial role of human oversight and responsibility for decisions.
- **Establish a clear and proportionate allocation of research security responsibilities among applicants, beneficiaries, funding bodies, EU member states and the European Commission.** Universities should be responsible for managing research security risks within their remit through appropriate institutional governance and procedures. Competent public authorities should provide necessary information, guidance, tools and support to empower universities to make sufficiently informed decisions. Universities should not be expected to assume responsibilities that belong to intelligence, security or counter-espionage authorities.
- **Ensure that research security requirements apply consistently and proportionately across all project participants**, including universities, companies and members of user groups, with responsibilities shared fairly according to their respective roles and activities.
- **Ensure that FP10 applicants are not disadvantaged for responsibly identifying and managing research security risks.** Align open science and research security guidance and evaluation criteria so that disclosure of such risks, accompanied by adequate, proportionate mitigation, does not in itself weaken the assessment of scientific excellence or prospects of funding, and duly justified restrictions on sharing are not treated as failures of open science. Promote recognition and reward schemes for these responsible practices alongside contributions to open science and research integrity in research assessment and academic careers.
- **Provide dedicated EU and national funding to strengthen universities' institutional research security capacity, including specialist staff, training and due-diligence systems.** Necessary project-specific research security costs should be eligible under FP10. This should avoid the 'autonomy trap' of assigning universities responsibilities without providing the resources and means to fulfil them. Furthermore, support the development of interdisciplinary postgraduate programmes, including dedicated master's degrees, to train specialised staff in research security, export controls and sanctions, combined with relevant technological expertise. Where appropriate, these subjects could also be incorporated into existing postgraduate curricula.
- **Provide greater legal clarity in call texts for EU funding programmes while maintaining open and non-prescriptive calls as the default.** Where feasible, the Commission should flag activities likely to involve export-controlled or military items and technologies, helping applicants anticipate potential compliance requirements. This approach does not replace the responsibility of EU member states, which retain the authority to enforce export control laws and decide whether a licence is required. More details can be found in our March 2026 input note on dual-use technologies.
- **Ensure that entities from countries associated to FP10 participate on an equal footing with entities from EU member states, in accordance with the applicable association agreements.** Restrictions affecting entities from associated countries should be exceptional and subject to the same principles of necessity, proportionality and transparency as restrictions affecting EU entities. They should be based on specific and demonstrable security risks and should not result solely from an entity's country of establishment or an individual researcher's nationality.

- **Anchor research security in the upcoming European Research Area Act to establish a level playing field for implementing research security in FP10.** As elaborated in our input to the ERA Act, binding common minimum standards should be established at EU level for national research security frameworks, guidance and support, requiring EU member states to provide adequate resources and accessible assistance to universities while preserving institutional autonomy and flexibility for proportionate, context-specific implementation.
- **Support FP10 consortia in agreeing clear arrangements for coordinating research-security matters**, with early involvement of principal investigators and coordination responsibilities allocated according to partners' expertise and consortium governance. These arrangements should enable the consortium to share concerns and address research security issues affecting specific partners, while respecting institutional autonomy and each beneficiary's own legal obligations.
- **Ensure coordination across Commission services, including DG RTD and DG TRADE, on research security, economic security and export controls.** Align terminology, guidance and support tools while respecting their distinct purposes and legal bases, so that universities receive coherent advice and avoid conflicting or duplicative requirements.

2. A European due-diligence platform

Integrating research security into FP10 requires both a coherent funding framework and practical tools that empower universities to make informed decisions. We welcome the development of a European due-diligence platform as part of this approach. Its role should be to provide reliable, up-to-date and sufficiently granular information that supports proportionate, context-sensitive assessments and responsible international collaboration. It should complement clear and proportionate FP10 application and funding processes, while leaving institutional decisions with universities.

The platform's concrete added value to strengthening research security across Europe will depend on a clear mandate, equal access, robust confidentiality safeguards and effective mechanisms to correct inaccurate information. Close involvement of universities in its development and testing, together with adequate resources and expert support, will be essential to making it useful in practice.

During the design and pilot phase

CESAER calls on the European Commission to:

- **Allow universities to co-design, test and evaluate the European due-diligence platform**, including its reliability, functionality, usability, proportionality and potential effects on international collaboration. CESAER Members welcome the planned pilot and are keen to contribute expertise to its design, testing and evaluation.
- **Design the European due-diligence platform to strengthen informed, proportionate and context-sensitive institutional decision-making.** Provide clear, evidence-based risk indicators that make significant risks visible in context, enabling universities to safeguard research and innovation while sustaining responsible international collaboration. Its information should inform, rather than predetermine or replace, institutional assessments of individual partnerships based on their respective risk appetites.

- **Provide universities in FP10-associated countries with access to the European due-diligence platform on the same terms as universities in EU member states**, particularly when they participate in the same European research consortia and are expected to apply comparable research security requirements. Safeguarding sensitive information and ensuring European digital sovereignty should be central considerations in determining access to the platform.
- **Build purpose limitation, access controls and confidentiality safeguards into the European due-diligence platform.** Define who may access it, how access is authorised, permitted uses of searches and user-provided information, and retention periods. Allow universities to designate sufficient authorised users to avoid bottlenecks in supporting large research communities. Clarify which findings they may use in institutional processes and share with researchers, and in what form, to support informed decisions while protecting confidential information.
- **Ensure that the European due-diligence platform supports European digital sovereignty and safeguards researchers' safety**. Its hosting, governance and technical architecture should ensure effective control over platform data and protect against compelled disclosure under national security laws that could allow intelligence services outside EU member states and FP10-associated countries to access those data, including queries and information about people and entities. Individual researchers' safety should be a core design requirement of the platform.

Once the platform is operational

CESAER calls on the EU institutions to:

- **Provide free access to the platform and dedicated resources for universities to appoint and train authorised personnel** who can interpret its information and support proportionate institutional decision-making. Access arrangements should not create unfunded responsibilities or disadvantage universities with fewer resources.
- **Provide reliable, regularly updated and granular risk information that considers relevant country context and identifies whether concerns apply to an institution as a whole or to particular departments or activities.** Risk assessments must not overlook wider risks arising from institutional governance, obligations or affiliations. Equally, concerns limited to a particular department or research activity should not lead to a general risk label for the whole institution or country. Apply consistent criteria, avoid discrimination based solely on nationality, and distinguish verified facts from risk indicators and contextual information.
- **Ensure transparency and effective correction mechanisms for individual assessments.** Subject to legitimate security and confidentiality limits, provide contextual information beyond risk scores, explaining the evidence, methodology, assessment date and what is not covered. Allow authorised users to flag factual errors, information gaps and subsequent changes in a partner's activities or affiliations, including shifts towards defence applications, for prompt review and updating.
- **Clarify how users of the platform may reasonably rely on its information and what additional verification may be needed.** Explain its legal status and the responsibilities of the platform operator, competent authorities and universities. Provide explicit protection against retrospective penalties imposed solely because information or a partner's status later changes, where universities fulfilled their obligations and reasonably relied on information available at the time. Clarify responsibilities for responding to new information or changed circumstances, including reassessment, mitigation or ending cooperation where necessary.

- **Connect the due-diligence platform to EU and national research security initiatives**, including the European centre of expertise and national contact points, so universities can obtain confidential expert advice on interpreting information, verifying concerns and identifying proportionate mitigation measures.
- **Facilitate secure exchanges among authorised users of the due-diligence platform across institutions and countries** to support consistent interpretation while respecting confidentiality and institutional judgement.

3. A European centre of expertise on research security

A European centre of expertise should strengthen the evidence base on research security and translate findings into practical support for universities. Alongside its research role, it should provide guidance, confidential advice and peer learning, with a clear mandate that complements the due-diligence platform and national support structures. Its value will depend on independent expertise, public accountability, adequate resources and sustained involvement of universities and researchers.

An externally contracted model must preserve continuity and ensure that publicly funded knowledge remains available beyond individual contracts.

CESAER calls on the European Commission to:

- **Give the centre a clear mandate, adequate resources and continuity beyond individual contracts to build a strong European evidence base on research security**. Ensure public oversight and arrangements to retain and transfer publicly funded knowledge and outputs if providers change, avoiding dependence on a single contractor.
- **Include an EU-level research security helpdesk within the centre of expertise**. Provide universities and researchers with confidential, practical guidance on assessing and managing risks. Work with national contact points and competent authorities to develop consistent guidance, identify conflicting interpretations and refer unresolved issues for clarification. Clearly distinguish advisory support from legally binding requirements and decisions.
- **Translate the centre's research into practical guidance and resources that strengthen universities' in-house expertise**, including adaptable tools, methodologies, case studies and training materials. Develop and test these with the research community for integration into existing institutional processes.
- **Work with universities experienced across the civil–defence–space continuum to develop practical guidance on how to effectively manage evolving dual-use pathways.** Draw on confidential exchanges of operational practice to elaborate the defence-proximity approach that CESAER proposed in our March 2026 input note, while clarifying how research security, export controls and programme-specific rules interact.
- **Involve universities and other research-performing organisations from the outset and throughout the centre's work**, through an expert advisory structure representing different national contexts and levels of research security capacity. Enable participation in advisory work and tool development, including testing confidential and proportional institutional resilience approaches focused on learning and capacity-building. Provide financial support where limited institutional resources would otherwise prevent participation.

- **Coordinate assessments of the effectiveness, proportionality and full costs and benefits of research security measures.** Examine universities' administrative burdens and effects on academic freedom, international cooperation, researcher mobility, research performance and non-discrimination. Use emerging findings to improve practical tools and guidance, alongside longer-term evaluation informing European and national policies.
- **Ensure that the European centre of expertise complements the due-diligence platform, national centres and contact points, and other relevant initiatives**, with clearly defined roles and referral pathways to minimise duplication and the risk of conflicting advice. Its establishment must not replace national responsibility for coherent national frameworks, guidance and accessible support. Ensure universities can engage directly with the European centre of expertise where no national contact point exists.

For more information, please contact Advisor for Research Vincent Klein Ikkink.