



EUROPEAN COMMISSION
 Directorate-General for Migration and Home Affairs
 Directorate-General for Research and Innovation

Guidance note – Potential misuse of research


1. Background

Some research involves materials, methods or technologies or generates knowledge or applications that could be misused. Although such research is carried out with benign intentions, it has the potential to harm humans, animals or the environment and may have substantial negative impacts on the security of individuals, groups or states. Certain research activities could lead to results whose unauthorised disclosure could prejudice the interests of the EU or its Member States.

Although the risk of misuse of research can never be fully eliminated, it must be minimised by recognising the risks and taking the right precautions.

Projects must properly address the risk of misuse and comply with international, EU and national laws that address concerns relating to potential misuse of materials, technologies and information.

This note helps to identify and address potential misuse of research.

 This note does not cover research misconduct (*e.g. falsification of research results, fabrication of scientific evidence and plagiarism*).

Activities using and/or generating information that might raise security concerns are dealt with separately and must be flagged in the Security Issues Table. These are research activities that could

- a) generate knowledge, materials and technologies that could be adapted for criminal/terrorist activities; or
- b) result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery.

Misuse not related to the security dimension must be addressed under the Ethics Issues Table and analysed as part of the relevant ethics sections (Humans, Personal data, Animals, Environment, Health and safety, Artificial intelligence or Other ethics issues).

2. Identifying potential misuse

To identify any possible misuse, consider the risks associated with the research planned in the project and any unethical or malevolent ways in which the materials, methods, technologies or knowledge involved could be used.

The research most vulnerable to misuse is research that:

- generates knowledge, materials and technologies that could be used for criminal or terrorist purposes

- could result in the development of chemical, biological, radiological or nuclear (CBRN) weapons or any method for their delivery
- involves developing surveillance technologies that could curtail human rights and civil liberties
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people
- develops materials/methods/technologies and knowledge that could harm humans, animals or the environment if they were released, modified or enhanced.

When designing a proposal, consider not only the immediate aims and intended applications of the activities you plan, but also whether your research could serve unethical or malevolent purposes. Therefore, also consider whether there are any risks that will outlast the duration of the project itself.

Questions to identify potential misuse include:

- Could the materials/methods/technologies or knowledge concerned physically or in any other way harm people, animals or the environment, by themselves or if modified or enhanced?
- Could the materials/methods/technologies or knowledge concerned, physically or in any other way, have direct negative impacts on the security of individuals, groups or states?
- Could the unauthorised disclosure of the materials/methods/technologies or knowledge concerned prejudice the interests of the European Union or of its Member States?
- Does the activity involve the development of surveillance technologies?
- What would happen if they ended up in the wrong hands?
- Could they serve any purposes other than the intended ones? If so, would that be unethical?
- Does the activity involve minorities or vulnerable groups or activities involving the development of social, behavioural or genetic profiling technologies?
- Does the activity generate knowledge, materials and technologies that could be used for criminal or terrorist purposes?
- Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons or any method for their delivery?

Sample situations

Example 1 – Research into biological agents

A research lab successfully reconstitutes an extinct virus. Although this is a scientific breakthrough, releasing the virus – whether accidentally or on purpose – would jeopardise public health and safety and might result in millions of deaths.

Example 2 – Vulnerability studies in the field of airport security

To improve airport security in Europe, a team of researchers conducts a series of vulnerability assessments to identify shortcomings in the security systems of certain airports. Their findings could help make airports less vulnerable to threats. However, if such findings end up in the wrong hands, they could be used to plan an attack on these particular airports.

3. Addressing potential misuse

There are various ways to mitigate risk. Depending on the activity planned and the potential misuse, applicants may choose to:


- take additional security measures, *e.g. physical security measures, classification of certain deliverables and/or limiting the dissemination of sensitive information with security recommendation which leads to publishing only part of the research results, security clearance for those involved in the project*
- take additional safety measures, *e.g. compulsory safety training for staff*
- adjust the research design, *e.g. use dummy data*
- regulate export.

You may also consider appointing an independent ethics advisor and/or project security officer or an ethics board and/or a security advisory board (composed of experts from different backgrounds who, in principle, are not involved in managing the project's research activities) to assist your project in designing and implementing the relevant measures.

If you are planning research that may give rise to concerns about potential misuse, you will need to do the following when preparing your proposal:

- fill in the Security Issues Table and/or the Ethics Issues Table in your proposal
- explain the risks for misuse in the Security Section and/or in the Ethics Self-Assessment section of your proposal
- explain how you will prevent or mitigate this potential misuse
- provide the details on applicable international, EU and national laws that address concerns relating to potential misuse of materials/methods/technologies or knowledge that could harm humans, animals or the environment if they were released, modified or enhanced
- if required, attach copies of authorisations, security clearances and ethics approvals.

If your proposal is selected for funding, the security review and/or ethics review of your proposal may result in specific contractual requirements/deliverables in the Grant Agreement.

 Please also be aware that breach of any of these obligations may lead to grant reduction or termination.

Specific cases

Research with a potential impact on human rights — Concerns in this field relate primarily to research on surveillance technologies, new data-gathering and data-merging technologies. However, also social or genetic research could lead to discrimination or stigmatisation

In your risk assessment, clearly indicate how your research activities or resulting technologies, applications or knowledge could be misapplied for stigmatisation, discrimination, harassment or intimidation, any potential negative impacts on human rights and civil liberties, and detail how those risks will be addressed.

Risk mitigation measures may include:

- a human rights impact assessment
- involving human rights experts in your research
- training personnel and/or technological safeguards
- caution when publishing or otherwise disseminating results (*e.g. through privacy by design*)
- adapting the research design (*e.g. using dummy data*).

Research using or developing AI-based technologies — For all research activities concerning the development or/and use of *artificial intelligence (AI) -based systems or techniques*, the ‘ethics by design’ approach must be adopted. The latter aims at integrating ethical values and principles based requirements into the design, development and/or implementation process of the developed/used AI solution application, to ensure that emerging ethical issues are followed up closely and can be addressed effectively. The adherence to the ethics by design approach will greatly facilitate your ethics compliance. For more information, *please consult [Guidelines on ethics by design for Artificial Intelligence](#)*.

Further reading

[How to complete your ethics self-assessment](#)

[FP7: A comprehensive strategy on how to minimize research misconduct and the potential misuse of research in EU-funded research](#)

[Responsible life sciences research for global health security: A guidance document](#)

[Biorisk management: Laboratory biosecurity guidance](#)

[Guidelines on ethics by design for Artificial Intelligence](#)

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
1.0	03.11.2015	Initial version.
1.1	07.01.2020	Updated to VM4.0 / insertion of header
2.0	14.09.2021	Update for new MFF (2021-2027).