FRONTEX

EUROPEAN BORDER AND COAST GUARD AGENCY

FRONTEX RESEARCH GRANTS PROGRAMME

Call for Proposals 2022/CFP/RIU/01

NOVEL TECHNOLOGIES FOR BORDER MANAGEMENT (OPEN THEME)

Annex 3.6 - Model Grant Agreement for mono-beneficiary action

Addendum - Model Data Processing Agreement

Data Processing Agreement

Implementation of the Grant Agreement No [insert]

The Data Controller for Frontex Research Grants Programme – Call for Proposals N. 2022/CFP/RIU/01 [insert function, forename and surname] (*hereinafter referred to as the Controller)*

and

[insert function, forename and surname of the Data Processor for the beneficiary] (*hereinafter referred to as the Processor),*

together referred to as Parties,

hereby agree on the conditions, procedures and principles of processing of personal data in the framework of the Grant Agreement N. [insert the Grant Agreement number] for the action entitled **[insert the title of the action in bold**] under the Frontex Research Grants Programme signed on [insert the date on which the last party signed the Grant Agreement] (hereinafter referred to as the "Grant Agreement").

This Data Processing Agreement is hereby incorporated and forms a part of the Grant Agreement and is subject to the terms and conditions therein. In the event of conflict between this Data Processing Agreement and the Grant Agreement, the terms of this Data Processing Agreement prevail.

HAVE AGREED

Article 1
Definitions

"Personal data", "special categories of data", "processing of personal data", "Controller", "Processor", "data subject", "recipient" and "data breach" have the same meaning as in Article 3 of Regulation (EU) 2018/1725[1] (*hereinafter referred to as Regulation 2018/1725)* and in Article 4 of Regulation (EU) 2016/679[2] (*hereinafter referred to as GDPR)*.

Article 2
General provisions

1. The [insert function within Frontex] is the Controller of processing of personal data in the framework of the processing activity [name of the activity].
2. [Name of the beneficiary] is the Processor of personal data on behalf of the controller in accordance with the Grant Agreement.
3. Data protection legislation applicable to the Controller is Regulation (EU) 2018/1725.
4. Data protection legislation applicable to the Processor is Regulation (EU) 2016/679 (GDPR).

[1] *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC,* OJ L 295, 21.11.2018, p. 39–98.

[2] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* OJ L 119, 4.5.2016, p. 1–88.

Article 3
Purposes, nature and scope of processing of personal data

1. The purposes of processing the personal data are:
   a. [list of purposes of processing the personal data]

2. The Processor shall not, under any circumstances, process personal data defined in this Agreement, for any other purposes than those described above.

Article 4
Categories of personal data to be processed

The following categories of administrative personal data can be processed by the Processor:

a. [list of categories of administrative personal data]

Article 5
Categories of data subjects

Data of the following categories of data subjects can be processed by the Processor:

a. [list of categories of data subjects]

Article 6
Duration of processing, retention of personal data, deletion/destruction/return of personal data

1. The Processor may process personal data in accordance with this Agreement upon entry into force of the Grant Agreement and only during the duration of that Grant Agreement.
2. The data shall be processed by the processor no longer than the duration of the Grant Agreement.
3. The Processor shall not process any personal data on the basis of this Agreement after the Grant Agreement is terminated.
4. Upon termination of the Grant Agreement, the Processor shall return all the personal data remaining in its possession to the Controller. The Processor shall certify to the Controller that all personal data has been returned and copies deleted.

Article 7
Storage and data location

Personal data processed by the Processor shall be processed in the territory of EU/EEA.

Article 8
Confidentiality and access to personal data

1. The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the Processor's authority who have committed themselves to confidentiality, or are under an appropriate statutory obligation of confidentiality, and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
2. The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

Article 9
Security measures

1. The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure.
2. Personal data shall not be stored in nor transferred outside EU/EEA and it shall not be stored in nor transferred to a cloud service (including any personal data processed as part of fault management / troubleshooting / technical support) without prior authorisation by the Controller.
3. Personal data management documentation (including description of categories of data collected and processed as part of fault management/troubleshooting/technical support) and detailed description of security measures and communication channels shall be provided to the controller upon request.
4. The Processor shall, independently from the Controller, evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Controller shall provide the Processor with all information necessary to identify and evaluate such risks.
5. The following security measures shall be implemented by the Controller and the Processor, where applicable:
    a. encryption of personal data;
    b. controlled access of the personal data;
    c. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    d. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    e. conducting regularly threat assessment or penetration testing on systems and assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
    f. ensuring IT equipment, including portable equipment is kept in controller access areas;
    g. not leaving portable equipment containing personal unattended; ensuring that staff use appropriate secure passwords for logging into systems or databases containing personal data;
    h. ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices, where necessary;
    i. limiting access to relevant databases and systems to those of its personnel who need to have access to personal data, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged in the processing;
    j. ensuring all staff handling personal data have been made aware of their responsibilities in regard to processing personal data;
    k. ensuring necessary logging and traceability of the actions performed upon personal data;
    l. allowing for inspections and assessments to be undertaken by the other Party in respect of the security measures taken or producing evidence of those measures if requested.
6. The Processor shall assist the Controller in ensuring compliance with the Controller's obligations, providing the Controller with information concerning the technical and organisational measures already implemented by the Processor along with all other information necessary for the Controller to comply with the Controller's obligation under Article 33 of the Regulation 2018/1725.
7. If subsequently – in the assessment of the Controller – mitigation of the identified risks require further measures to be implemented by the Processor, than those already implemented by the Processor pursuant to Article 32 of the GDPR, the Controller shall specify these additional measures to be implemented.

Article 10
Disclosure of personal data

The Processor shall not disclose any personal data to any party without prior written authorisation by the Controller.

Article 11

Transfers of personal data outside EU or EEA

1. Any transfer of personal data to third countries (countries outside EU and EEA) or international organisations by the data Processor shall only occur on the basis of documented instructions or authorisation from the data Controller.

2. In case the transfer to third countries or international organisations, which the Processor has not been instructed to perform by the data Controller, is required under EU or Member State law to which the data Processor is subject, the data Processor shall inform the data Controller of that legal requirement prior to processing.

3. Without documented instructions from the Controller, the Processor shall not:

   a. transfer personal data to a Controller or a Processor in a third country or in an international organization;

   b. engage in the processing of personal data a sub-Processor in a third country;

   c. have the personal data processed in by the Processor or sub-Processor in a third country.

Article 12
Sub-contracting and sub-processing

1. The Processor shall not engage any Processor (sub-Processor) for the fulfilment of the Grant Agreement without the prior specific written authorisation of the Controller.

2. Any sub-Processor engaged by the processor shall meet the requirements specified in Article 28(2) and (4) GDPR.

3. Where the Processor engages any other sub-Processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the Agreement shall be imposed on that sub-Processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Agreement and the GDPR.

4. The Processor shall therefore be responsible for requiring that any other sub-Processor at least complies with the obligations to which the Processor is subject pursuant to this agreement and the GDPR.

5. A copy of such a sub-Processor agreement and subsequent amendments shall – at the Controller's request – be submitted to the Controller, thereby giving the Controller the opportunity to ensure that the same data protection obligations as set out in the Agreement are imposed on any other sub-Processor. Clauses on business related issues that do not affect the legal data protection content of the sub-Processor agreement, shall not require submission to the Controller.

6. If the sub-Processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the Controller as regards the fulfilment of the obligations of the sub-Processor. This does not affect the rights of the data subjects under the Regulation 2018/1725 and GDPR – against the Controller and the Processor, including the sub-Processor.

Article 13
Auditing rights of the Controller

1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and this Agreement, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

2. The Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Processor's physical facilities on presentation of appropriate identification.

Article 14
Data subject requests

1. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights.

2. This entails that the Processor shall, insofar as this is possible, assist the Controller in the Controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject;

   b. the right to be informed when personal data have not been obtained from the data subject;

   c. the right of access by the data subject;

   d. the right to rectification;

e. the right to erasure (‘the right to be forgotten’);

f. the right to restriction of processing;

g. notification obligation regarding rectification or erasure of personal data or restriction of processing;

h. the right to data portability;

i. the right to object;

j. the right not to be subject to a decision based solely on automated processing, including profiling.

3. The Processor shall respond to the Controller´s request for assistance no later than within five (5) working days after the request was received.
4. The Processor shall inform the Controller about the data subject requests that the Processor received no later than five (5) working days from the date the Processor received the request.

Article 15
Assistance with the obligations of the Controller

The Processor shall, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:

a. the Controller´s obligation to prepare record of processing operation(s) and any other relevant data protection documentation;

b. the Controller´s obligation to respond to the requests by the competent supervisory authority (European Data Protection Supervisor);

c. the Controller’s obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify a personal data breach to the competent supervisory authority (European Data Protection Supervisor), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

d. the Controller’s obligation to without undue delay communicate a personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

Article 16
Personal data breaches

1. In case of any personal data breach, the Processor shall, without undue delay after having become aware of it, notify the Controller of the personal data breach. The notification should be made at the latest within 24 hours of identification of the data breach to enable the Parties to consider what action is required, in order to resolve the issue in accordance with the applicable data protection legislation.
2. The Processor’s notification to the Controller shall take place without undue delay after the Processor has become aware of the data breach to enable the Controller to comply with the Controller’s obligation to notify the personal data breach to the competent supervisory authority in accordance with Regulation 2018/1725.
3. The Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the following information in accordance with Article 34(3) of Regulation 2018/1725:

a. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Article 17
Supervision

1. European Data Protection Supervisor is the competent data protection supervisory authority for processing of personal data by the Controller.
2. [insert] is the competent data protection supervisory authority for processing of personal data by the Processor.
3. In respect of breaches relating to this Agreement, each Party shall abide by any binding decision of the competent data protection authority.

Article 18
Contact information

1. Each Party nominate a single point of contact within their organisation who can be contacted in respect of queries or complaints regarding this agreement:

   For the Controller: [insert function, forename and surname] e-mail: [insert] Tel. [insert]

   For the Processor: [insert function, forename and surname] e-mail: [insert] Tel. [insert]
2. Parties shall inform each other about contact details of the contact points and contact information that can be provided, if necessary, to the Data Subjects or the competent data protection supervisory authority.
3. Data Protection Officer of the Controller can be reached at: dataprotectionoffice@frontex.europa.eu
4. Data Protection Officer of the Processor can be reached at: [insert email]

Article 19
Final provisions

1. The Agreement enters into force on the date on which the last party signs it.
2. The Agreement shall apply for the duration of the Grant Agreement.
3. In the event that the Processor fails to respect its undertakings under this Agreement, the Controller may request suspension of the processing until the Processor meets its obligations under the Agreement, or the Grant Agreement.

SIGNATURES

On behalf of the Processor [signature]	On behalf of the Controller [signature]

Done at [insert] on [insert]

In duplicate in English.