Processing agreement sustained archiving

The parties

1. [Name of Controller: organisation], having its registered office at [ADDRESS] in [TOWN/CITY], Chamber of Commerce number [CoC Number], and duly represented by [Name of REPRESENTATIVE], (hereafter referred to as “the Controller”);
   and
2. The Royal Netherlands Academy of Arts and Sciences, having its registered office at Kloveniersburgwal 29 in Amsterdam, the Netherlands, Chamber of Commerce number 54667089, acting on behalf of Data Archiving and Networked Services (DANS), having its registered office at Anna van Saksenlaan 51 in the Hague, and duly represented by H.P.A. Smit, (hereafter referred to as “the Processor”);

jointly referred to hereafter as “the Parties”,

Considering that:

A) The Processor entered into an agreement with the Controller on the following date, __-__-___ , with respect to the provision of services for the benefit of the Controller, consisting of a deposit agreement for the sustained archiving and management of digital (research)data (hereafter referred to as “the Main Agreement”);

B) In performing the work arising from the Main Agreement, the Processor will process Personal Data, as referred to in the General Data Protection Regulation (hereafter also referred to as “the GDPR”);

C) The Parties wish to make further arrangements regarding how the Personal Data may be processed and what measures the Processor will take for protecting the Personal Data, also in view of the obligations of both Parties arising from the General Data Protection Regulation;

D) The Parties – also given the requirement of Article 28 of the General Data Protection Regulation – wish to record the arrangements in writing by means of this Processing Agreement (referred to hereinafter as “the Processing Agreement”).

Agree as follows:

Article 1 Definitions

a. *Dutch Data Protection Authority*: an independent organisation that monitors compliance with the statutory rules for the protection of Personal Data and that advises on new rules;

b. *GDPR*: The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016);

c. *Data Subject*: a natural person to whom Personal Data relates within the meaning of Article 4, under 1, of the GDPR;

d. *Data Leak*: a security breach within the meaning of Article 33 of the GDPR;

e. *Third Party*: any party not being the Data Subject, Controller, Processor, any person directly supervised by the Controller or the Processor who is authorised to process the Personal Data, within the meaning of Article 4, under 10, of the GDPR;

f. *Main Agreement*: the agreement specified in consideration A;

g. *Personal Data Breach*: a breach of security which accidently or unlawfully results in the deletion, loss, alteration, or unauthorised disclosure of, or access to, data that is transmitted, stored, or otherwise processed, within the meaning of Article 4, under 12, of the GDPR;

h. *Task*: the task described in Article 2, paragraph 3, of this Processing Agreement and that is performed by the Processor on behalf of the Controller;

i. *Personal Data*: any information relating to an identified or identifiable natural person (the Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, within the meaning of Article 4, under 1, of the GDPR;

j. *Sub-Processor:* the party who, on the instructions of the Processor, processes Personal Data for the purposes of the Task for the Controller;

k. *Processing*: any operation or set of operations that is performed on Personal Data or on a set of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or deletion, within the meaning of Article 4, under 2, of the GDPR;

l. *Processor*: a natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the Controller without being subject to the Controller's direct supervision, within the meaning of Article 4, under 8, of the GDPR (as included in Parties, under 2);

m. *Processing Agreement*: the present agreement, which is part of the Main Agreement;

n. *Controller*: the natural or legal person, public authority, agency or other body who or which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, within the meaning of Article 4, under 7, of the GDPR (as included in Parties, under 1).

Article 2 General

1 The Processor undertakes, subject to the conditions of this Processing Agreement, to process Personal Data on behalf of the Controller.
2 The provisions of this Processing Agreement will apply to all Processing Operations that take place in performance of the Main Agreement.
3 The Processor will process the Personal Data in a proper and careful manner and in accordance with the provisions of the GDPR and other applicable regulations regarding the Processing of Personal Data.
4 The Processing of Personal Data by the Processor will take place only in so far as necessary and within the framework of the Task to be performed pursuant to the Main Agreement.
5 Without the prior written consent of the Controller, the Processor will not allow Third Parties access to the Personal Data, including group companies of a group to which the Processor belongs, such as subsidiaries or sister companies.
6 Appendix A will include and specify the following items:
- the Personal Data that may be processed for the purpose of performing the Task;
- the retention period of the Personal Data;
- an overview of the category/categories of Data Subjects;
- an overview of the recipient(s) of Personal Data.

b. Appendix B will include and specify the following items:
- the minimum security measures that the Processor will take;
- the employees or groups of employees who will have access to the Personal Data;
- the Processing Operations allowed.

c. Appendix C will include and specify the following:
- an overview of the Sub-processors admitted by the Processor

d. The risk categories will be specified in Appendix A according to the type of Personal Data.

e. If there are several partial Tasks within the Main Task, the information referred to under (a) will be included in Appendix A for each partial Task.

7 For the performance of the Task, only the Personal Data that are necessary for the purpose determined by the Controller can be processed. The Controller will determine which data are necessary and will ensure that the Personal Data in question are correct, sufficient and not excessive in accordance with Article 5 of the GDPR.
8 Pursuant to Article 3 of the GDPR, the Processing Operations for Personal Data will not fall outside the territorial scope of the GDPR.
9 If, contrary to this Processing Agreement and/or the GDPR and/or other applicable legislation and regulations concerning the Processing of Personal Data, the Processor determines the purpose and means of/for the Processing of Personal Data, the Processor will be considered to be the Controller for those Processing Operations.

Article 3 Obligation to provide information

1 The Processor will inform the Controller of any future changes in the performance of the Main Agreement, so that the Controller can monitor compliance with arrangements with the Processor. This will include the engagement of Sub-Processors.

2 The Processor will inform the Controller of any questions or complaints from Data Subjects.

3 The Processor will inform the Controller if the Processor has received an instruction from the Controller that contravenes the GDPR or other applicable regulations regarding the Processing of Personal Data.

4 The Processor will notify the Controller immediately if the Processor has reason to believe that the Processor cannot comply with the Processing Agreement.

Article 4 Obligations of the Processor

1 The Processor will not retain Personal Data made available to it in the context of the Main Agreement for any longer than is necessary:
a. for the performance of this Processing Agreement;
b. for processing with a view to archiving in the public interest, scientific or historical research, or statistical purposes; or
c. to fulfil a legal obligation to which the Processor is subject.

2 The Processor will process the Personal Data solely by order of and in accordance with the instructions of the Controller. The Processor will provide its employees with access to the Personal Data in so far as necessary for the performance of this Processing Agreement and the Main Agreement.

3 The obligations of the Processor arising from this Processing Agreement will also apply to those who process Personal Data subject to the authority of the Processor, including but not restricted to employees and Third Parties engaged, in the broadest sense.

4 The Processor will not process the Personal Data for its own benefit, for the benefit of Third Parties, and/or for its own advertising or other purposes unless pursuant to different mandatory legal obligations to which it is subject.

5 The Processor will keep a register of Processing Operations.

6 The Processor will cooperate with the data protection officer designated by the Controller (within the meaning of Article 37 of the GDPR) as soon as the data protection officer requires such in the performance of his or her duties.

Article 5 Obligations of the Controller

1 The Controller will ensure a legitimate basis for the Processing of Personal Data, within the meaning of Article 6 of the GDPR.

Article 6 Use of Sub-Processors

1 The Controller will grant the Processor permission for the use of Sub-Processors. The Processor will inform the Controller of intended changes regarding the addition or replacement of Sub-Processors.

2 The Processor will conclude the same arrangements with Sub-Processors as those made between the Controller and the Processor in the Processing Agreement.

The Processor will draw up a written agreement with the Sub-Processor in question that will comprise at least the following obligations for the Sub-Processor:

a) to act in accordance with the present Processing Agreement; and
b) to follow and implement, fully and without any delay, all instructions given by the Processor and the Controller concerning the Processing of Personal Data; and
c) to process Personal Data only in accordance with the Processor's instructions; and
d) not to give access to Personal Data to any Third Party – including any Sub-Processors of Sub-Processors – without the prior written consent of the Controller; and
e) to enable the Processor and the Controller to act efficiently, in a timely manner, and in accordance with the requirements set by the GDPR, in the event of a (suspected) Personal Data Breach as referred to in the GDPR.

3 Upon request, the Controller will receive an overview from the Processor regarding the Sub-Processors engaged.

Article 7 Security

1 The Processor will put in place appropriate technical and organisational measures to protect Personal Data from being lost and from any form of unlawful Processing, such as, but not limited to:
a. damage to or loss of Personal Data;
b. unauthorised alteration of Personal Data;
c. misappropriation of Personal Data;
d. cognisance of Personal Data by unauthorised persons.

2 Taking account of the state of technology and the cost of implementing them, the measures will guarantee an appropriate level of security in view of the risks associated with such Processing and the nature of the Personal Data being protected.

3 The Processor will record the measures in writing and will ensure that the security as referred to in this article complies with the security requirements pursuant to the GDPR.

4 The Processor will, upon request, provide the Controller with written information regarding the security of Personal Data and how it is organised.

5 The Processor will inform the Controller of any substantial change in one or more of the security measures.

6 Adherence to an approved code of conduct as referred to in Article 40 of the GDPR or an approved certification mechanism as referred to in Article 42 of the GDPR may be used as an element to demonstrate compliance with the obligations within the meaning of the present article.

Article 8 Obligation to report Data Leaks

1 In the event of a Data Leak, the Processor will inform the Controller without unreasonable delay by contacting the Controller's contact person listed in Appendix D.

2 The Processor will provide the above report with the information set out in Appendix D.

3 The Processor will take measures to prevent or restrict (further) unauthorised cognisance, modification or disclosure, or any other unlawful Processing and to terminate and prevent in future any breach of security measures, breach of the confidentiality obligation or further loss of confidential information.

4 At the request of the Controller, the Processor will, in so far as possible, assist in informing the competent authorities and Data Subjects.

5 The Processor will conclude written arrangements with Sub-Processors regarding the obligation to report possible Data Leaks to the Processor, which will enable the Processor and the Controller to comply with obligations in the event of a Data Leak as specified in paragraph 1 of this article.

a. These arrangements will in any case include the obligation that the Sub-Processor will inform the Processor of a Data Leak as specified in paragraph 1 of the present article within 18 hours of the initial discovery, by contacting the Processor’s contact person as listed in Appendix D.

b. The arrangements will in any case include the obligation that the Sub-Processor, at the request of the Controller, will cooperate with the provision of information to the competent authorities and Data Subjects.

6 The reporting of Data Leaks to the Data Protection Authority and (possibly) Data Subjects will be the responsibility of the Controller.

Article 9 Obligations regarding Data Subjects

1 The Processor will cooperate fully in order to ensure that the Controller can comply with its statutory obligations in the event that a Data Subject exercises his or her rights pursuant to the GDPR.

2 In the event of a Data Subject making a request to the Processor to exercise his or her legal rights, the Processor will forward such a request to the Controller, and the Controller will deal further with the request. The Processor may inform the Data Subject of this.

Article 10 Audit

1 The Processor will perform assessments to evaluate whether the security measures in Article 7 of the Processing Agreement are adequate. If requested by the Controller, the Processor will provide a report of this assessment, unless an assessment does not relate to Processing Operations performed by the Processor for the Controller.

2 If the Controller requests an independent audit, the Controller and the Processor will agree to appoint an independent IT auditor or expert to conduct an audit of the Processor's organisation to determine whether the Processor complies with the agreed security measures set out in the Processing Agreement.

a. The frequency of the audit is no more than once every three years.

b. If only public Personal Data are processed, a low risk will be considered to apply and there will be no obligation to conduct an audit.

3 The costs of the audit on request will be borne by the Controller.

4 If it is determined during an audit that the Processor does not comply with the provisions of the Main Agreement and the Processing Agreement, the

Processor will take all reasonably necessary measures to ensure that it does henceforth comply.

Article 11 International traffic

1 The Processor warrants that any Processing of Personal Data performed by or on behalf of the Processor, including by the Sub-Processors that the Processor has engaged in connection with the performance of the Main Agreement, will take place within the European Economic Area (EEA).

2 Without the Controller's prior written consent, the Processor will not be permitted to transfer or store Personal Data to/in a country outside the EEA.

3 If the Processor wishes to make Personal Data accessible from a non-EEA country, prior written consent must be requested from the Controller, even if the country concerned has an appropriate level of protection.

4 The Controller may attach conditions to the consent.

5 The Processor will ensure that, in view of the circumstances applicable to the transfer of the Personal Data or any information whatsoever, the countries referred to, located outside the EEA, offer adequate protection.

6 If the technical features of a transmission medium make such a guarantee impossible, the transmission of data will be carried out solely in encrypted form, using advanced encryption technologies (being at least as advanced as is customary within the market). The Processor will provide information on the location or locations where the data Processing takes place prior to the conclusion of the Processing Agreement.

Article 12 Detection requests

1 The Processor will inform the Controller immediately if the Processor receives a request or an order from a Dutch or foreign regulator or public authority, or from an investigation, prosecution or national security authority to provide Personal Data (or access to Personal Data).

2 In dealing with such request or order, the Processor will comply with all instructions of the Controller (including the instruction to leave the handling of the request or order wholly or partly to the Controller) and will provide all reasonably necessary cooperation.

3 If the Processor is prohibited by virtue of the request or order from complying with its obligations within the meaning of paragraphs 1 and 2 of this article, then the Processor will safeguard the reasonable interests of the Controller. To that end, the Processor will in any event:

a. have a legal check carried out regarding to what extent (i) the Processor is legally obliged to comply with the request or order; and to what extent (ii) the Processor is actually prohibited from fulfilling its obligations towards the Controller on the basis of the above;

b. cooperate with the request or order only if it is legally obliged to do so and, where possible, object (in court or otherwise) to the request or order or the prohibition on informing the Controller about it or following the Controller's instructions;

c. not provide more or other Personal Data than strictly necessary to comply with the request or order;

d. in situations of transfer of the data to a country outside EEA: investigate the options to comply with Articles 44 to 46 of the GDPR;
e. immediately inform the Controller as soon as such is permitted.

4 In the present article, "legally" will be taken to refer not only to Dutch but also to foreign legislation and regulations.

Article 13 Confidentiality

1 All Personal Data processed in the context of the Processing Agreement and/or the Main Agreement are confidential data.

2 The Processor will keep all (Personal) data secret which it knows or can reasonably presume to be confidential and of which it becomes aware or which are at its disposal in the context of performance of the Main Agreement and/or the Processing Agreement, and will not in any way disclose, either internally or externally, and/or provide such data to Third Parties except if:
a. it is necessary to disclose and/or provide such data in order to perform the Main Agreement;
b. any mandatory Dutch legal requirement or Dutch judicial ruling obliges the Processor to disclose and/or provide such data or information, with the Processor first informing the Controller of this;
c. disclosure and/or provision of such data is effectuated with the prior written consent of the Controller; or
d. the information concerned was already lawfully public in a manner other than through the acts or omissions of the Processor.

3 The Processor will contractually oblige persons working for it (including employees) and Sub-Processors who are involved in the Processing of confidential data to keep such confidential data confidential.

4 The Processor will make all data in its possession within the framework of performance of the Main and/or the Processing Agreement, including any copies thereof, available to the Controller at the latter's first request.

5 The present article and the confidentiality obligation referred to herein will remain in force after termination of the Main Agreement and/or the Processing Agreement.

Article 14 Liability

1 The Processor will be responsible for the Processing of the Personal Data pursuant to this Processing Agreement, in accordance with the instructions of the Controller and under the explicit (final) responsibility of the Controller.

2 Barring intent or gross negligence, the Controller will indemnify the Processor against all damage suffered by the Controller as a result of an attributable shortcoming on the part of the Processor, or of Sub-Processors or others engaged by the Processor, with regard to obligations under the Main Agreement, the Processing Agreement, the GDPR or other applicable legislation, including regulations concerning Personal Data processing, in view of the free and public-interest nature of the disclosure of research data through the services of the Processor.

3 The controller will indemnify the Processor against all claims from third parties, including data subjects, that may be brought against the Processor, Sub-Processors or others engaged by the Processor, with regard to obligations

under the Main Agreement, the Processing Agreement, the GDPR or other applicable legislation, including regulations concerning Personal Data processing, in view of the free and public-interest nature of the disclosure of research data through the services of the Processor.

Article 15 Intellectual and other property rights and control

1 All intellectual and other property rights in respect of particulars, data, information, and any other material or content that the Controller enters, transmits, posts, or otherwise processes with the assistance of the Processor will at all times remain vested in the Controller or their respective licensors.
2 The Processor will have no independent control of such information that it processes. Control will be vested in the Controller.

Article 16 Alterations

1 If an alteration in the Personal Data to be processed or a risk analysis of the Processing of Personal Data gives cause to do so, the Parties will enter into consultations, at the request of the Controller, regarding amending the arrangements made within this Processing Agreement.
2 The new arrangements that are to be made must have been recorded in writing prior to their application and must form part of this Processing Agreement.
3 Such alterations may never result in the Controller and/or the Processor being unable to comply with the GDPR or other relevant legislation and regulations with regard to the Processing of Personal Data.

Article 17 Duration and termination

1 This Processing Agreement will enter into force on the same date as the Main Agreement and will also terminate simultaneously with the Main Agreement.
2 Without prejudice to the provisions of paragraph 3, it will not be possible to terminate the Processing Agreement separately from the Main Agreement.
3 The Controller and the Processor will be entitled to terminate the Processing Agreement if the Processor does not comply, or can no longer comply, with the Processing Agreement and/or the GDPR and/or other applicable legislation and regulations concerning the Processing of Personal Data. A reasonable period of notice will be observed in the event of termination.
4 Upon termination, for whatever reason, of the Main Agreement or upon termination of the Processing Agreement as referred to in paragraph 3 of the present article, the Processor will ensure that, at the discretion of Controller:
   a. all or part of the Personal Data, as determined by the Controller, that have been made available to the Processor in connection with the Task are deleted at all locations;
   b. all or part of the Personal Data, as determined by the Controller, that have been made available to Processor in connection with the Task are made available to a following Processor; or
   c. the Controller is enabled to withdraw all or part of the Personal Data, as determined by Controller, from the Task.
5 The Processor is permitted to make an exception to the obligation to delete referred to in Article 4(a), if the processing is continued with a view to

archiving in the public interest, scientific or historical research or statistical purposes, and is in accordance with the GDPR.

6 Destruction and/or disclosure and/or extraction of Personal Data will be executed as agreed in the Main Agreement.

7 Upon the Processing Agreement terminating, the Processor will (including in the event of that which is specified in paragraph 4, opening words and b of the present article) guarantee data portability in such a way that the (updated) (Personal) data are provided to the Controller and that there is no question of loss of functionality or of the (updated) (Personal) data or parts thereof.

Article 18 Applicable law and settlement of disputes

1 In the event of any conflict between provisions of this Processing Agreement and the Main Agreement, the provisions of this Processing Agreement will prevail.

2 This Processing Agreement and the performance thereof will be governed by Dutch law.

3 Any general conditions of delivery or other general or special terms and conditions of the Controller and Processor will not apply to this Processing Agreement.

4 Any disputes arising between the Parties in connection with this Processing Agreement will be submitted for adjudication to the competent court in the place where the Controller has its registered office.

Agreed and signed in duplicate,

Controller

Processor

Date:

Date:

Appendix A: Specification of Personal Data
Appendix B: Processor’s Security Measures
Appendix C: Sub-Processors
Appendix D: Obligation to report Data Leaks

Appendix A: Specification of Personal Data

TASK

Name of task

Sustained archiving and managing of digital (research) data

Description of task

Sustained archiving and managing of digital (research) data under the conditions of the Main agreement concerning Dataset with *persistent identifier*: [*persistent identifier* dataset]

PERSONAL DATA TO BE PROCESSED

The Processor will process the following Personal Data, belonging to the stated risk category, for the Controller. The Processor will not retain these Personal Data for any longer than is necessary to perform the Underlying Agreement or to comply with a statutory obligation to which the Processor is subject. The retention periods specified below apply to Personal Data that are processed for the purpose of the correct performance of the Task.

Personal data	Risk category (Normal/High)	Retention period

DATA SUBJECTS

List of the groups of persons whose Personal Data are processed.

RECIPIENTS

List of the groups of persons to whom Personal Data are provided.

Appendix B: Processor’s Security Measures

SECURITY MEASURES IN PLACE

Specification of the security measures that the Processor will in any case apply.:

The data will be stored in a secure data centre. The data will be stored in two locations. The servers will be protected by a firewall and a strict admission policy will apply to all servers, data and back-up data.

Specification of the certificates held by the Processor and their period of validity.

The Processor’s archival system is certified according to CoreTrustSeal (CTS) and Nestor Seal (DIN 31644). See https://www.coretrustseal.org/ and https://www.langzeitarchivierung.de/Webs/nestor/EN/Zertifizierung/nestor_Siegel/nestor_siegel_node.html

The Vancis datacenter comes under SURFCumulus by SURF. Vancis certifications include ISO9001 and ISO27001. See https://vancis.nl/over-vancis/certificeringen/.

DESCRIPTION OF THE (GROUP OF) EMPLOYEES WITH ACCESS TO PERSONAL DATA

Description of the (group of) employees with access to personal data and the description of the processing operations which may be carried out on Personal Data.

(Group of) Employees	Personal data	Processing types
DANS IT Support staff	All personal data to be processed, as specified in Appendix A	Storage
DANS Archival staff	All personal data to be processed, as specified in Appendix A	Storage and processing for the purposes of reuse and sustained archiving
KNAW ICT Service	All personal data to be processed, as specified in Appendix A	Storage

Appendix C: sub-processors

The Controller has:

☒ given the Processor general consent for engaging Sub-Processors.

Appendix D: Obligation to report Data Leaks

List of contact persons for notification of a data leak

The following should be contacted to report a Data Leak within the meaning of Clause 8 of the Processor Agreement:

CONTROLLER:

Name of organisation

Name of contact person

Position

E-mail address

Phone number

PROCESSOR:

Name of organisation DANS

Name of contact person Emilie Kraaikamp

Position Legal Support Officer

E-mail address privacy@dans.knaw.nl

Phone number +31 (0) 6 23297450

INFORMATION TO BE PROVIDED IN THE EVENT OF A DATA LEAK

If Processor is required to inform Controller pursuant to Clause 8 of the Processor Agreement, the following form must be filled in as completely as possible and provided to Controller.

INFORMATION ABOUT DATA LEAK

Provide a summary of the incident in which there has been a breach of the security of Personal Data:

For how many persons has Personal Data been involved in the breach?
(Fill in numbers of persons)

Minimal ______ Maximum ______

Specify the group of persons whose Personal Data has been involved in the breach:

When did the breach occur?
(Select one of the following options and provide information where necessary.)

Precisely on ______ (date)

Between ______ (date) and ______ (date)

Not yet known □

When was the breach discovered?

Date ______

Time ______

What is the nature of the breach?
(You can check more than one option.)

☐ Read (confidentiality)

☐ Copied

☐ Altered (integrity)

☐ Removed or deleted (availability)

☐ Stolen

☐ Not yet known

What type of Personal Data is concerned?
(You can check more than one option.)

☐ Name and address details

☐ Telephone numbers

☐ E-mail addresses or other addresses for electronic communication

☐ Access or identification details

☐ Financial data

☐ Citizen Service Number [*Burgerservicenummer*, "BSN"]

☐ Copies of passports or other identity documents

☐ Gender, date of birth, and/or age

☐ Special Personal Data

☐ Other data, namely:

What consequences can the breach have for the personal privacy of the Data Subjects concerned?
(You can check more than one option.)

□ Stigmatisation or exclusion

□ Damage to health

□ Exposure to fraud/identity fraud

□ Exposure to spam or phishing

□ Other consequences, namely:

FOLLOW-UP ACTION IN RESPONSE TO DATA LEAK

Specify the technical and organisational measures that your organisation has taken to deal with the breach and to prevent further breaches:

PROTECTION MEASURES

Was the personal data encrypted, hashed, or otherwise incomprehensible or inaccessible to unauthorised persons at the point when the data leak was discovered?

□ Yes

□ No

□ Partly, namely:

If the Personal Data had been rendered completely or partially incomprehensible or inaccessible, in what way was that done? (Answer this question if you chose the option “Yes” or “Partly, namely” in response to the previous question. If you used encryption, please explain the encryption method.)

Encryption method:

INTERNATIONAL ASPECTS

Does the infringement concern persons in other EU countries?
(Select one of the following options)

□ Yes

□ No

□ Not yet known