**Agreement for the use of Stichting HIV Monitoring data**

[INSTITUTION], with its registered office at [STREET], [PLACE], Chamber of Commerce No [CoC number], legally represented by [NAME e.g. head of department/division], (hereinafter: **the Institution**),

and

Stichting HIV Monitoring (SHM), with its registered office at Meibergdreef 9, 1105 AZ Amsterdam, Chamber of Commerce No 34160453, legally represented by S. Zaheri, and M. van der Valk, Board of SHM, (hereinafter: **SHM**),

enter into this agreement (hereinafter: **the Agreement**) to arrange the use of SHM data for research purposes.

The following form an integral part of the Agreement:

a) Statement concerning the use of SHM data

b) Appendix 1: General Terms and Conditions

c) Appendix 2: Description of the Study and the Data

d) Appendix 3: Statement on data transfer upon completion or discontinuation of the study

e) Appendix 4: Model clauses (2021/3972/EC)

**Statement concerning the use of SHM data**

The Institution guarantees that the data provided by SHM to the Institution in connection with the study [RESEARCH TITLE and NUMBER] (hereinafter: **the Data**) will exclusively be used for the above-mentioned study (hereinafter: **the Study**)), executed by [NAME STUDY APPLICANT]. A description of the Study and Data is provided in Appendix 2.

Under no circumstances will the Data, in whatever form, be used for any purposes other than for the Study or be disseminated by any means or disclosed to third parties. When the Data are no longer required for the study or, in any event, when the study is completed, the Institution will notify SHM accordingly by email as soon as possible but within no more than one month at the latest. After this notification, SHM will notify the Institution that the received Data can be destroyed and/or transferred. After this notification from SHM, the Institution will destroy all original SHM Data and all copies of any related documents without delay, excluding the analysis data set that is required to reproduce results of the research. A copy of this analysis data set will be shared with SHM. The Institution will then send SHM a signed “Statement regarding data transfer upon completion or discontinuation of the study”, as contained in Appendix 3, as soon as possible but within no more than one month. This statement can be signed on behalf of the Institution by the Study project leader.

The Institution will provide SHM with a copy of all reports (such as poster presentations or publications) that have been published or will be published using the Data.

SHM will retain the original Data for a statutory retention period after publication, in conformity with the Medical Research Involving Human Subjects Act (WMO) and the guidelines of the Central Committee on Research Involving Human Subjects (CCMO). The Institution is responsible for the proper reporting of the data analysis and the retention of the syntaxes/scripts that were written to carry out the analyses and obtain the research results.

The Institution guarantees that anyone using the Data in connection with the Study has read and understood the contents of this statement.

Signed at………………… date ……………………

Institution:

…………………………

[NAME OF Institution Legal Representative e.g. head of department/division]

SHM:

Signed at………………… date ……………………

…………………………

M. van der Valk (Board)

Signed at………………… date ……………………

…………………………

S. Zaheri (Board )

Appendix 1: **General Terms and Conditions**

The Institution and SHM can also be referred to separately as ‘**Party**’ and jointly as ‘**Parties**’.

**Article 1. Provision of Data**

1.1. Pursuant to the Agreement, SHM will provide Data, including personal data, to the Institution, thereby granting the Institution the right to use these Data.

1.2. Terms from the General Data Protection Regulation (hereinafter: **GDPR**), such as “processing”, “personal data”, “data controller” and “processor”, have the same meaning as in the GDPR. Until 25 May 2018, any references in the Agreement to terms or provisions from the GDPR must be understood to have the same meaning as in the Personal Data Protection Act.

1.3. The Institution guarantees that it shall exclusively use the Data received from SHM for the purpose described in the Agreement. Other processing operations will exclusively be performed if explicitly agreed between Parties or required by law.

1.4. SHM will protect the files containing the Data with a password using 7zip and send these files via filesender, and also requests the Institution to make use of filesender for sending the Data. SHM will support this by sending the Institution an invitation for the use of filesender. If the foregoing is not reasonably possible for the Institution, Parties will jointly agree on an alternative acceptable method for the provision of Data in conformity with the GDPR.

**Article 2. Obligations of Parties**

2.1. Parties declare mutually that the processing of the provided personal data pursuant to the Agreement will take place in a proper and careful manner. Each Party must, in its capacity as data controller within the meaning of Article 4 (7) of the GDPR, ensure that the processing operations taking place under its responsibility comply with the applicable laws and regulations.

2.2. The provided Data must be used by the Institution in a scientifically responsible manner in accordance with the Dutch Academic Integrity Code. (http://www.vsnu.nl/files/documents/Netherlands%20Code%20of%20Conduct%20for%20Research%20Integrity%202018.pdf).

2.3. The Institution ensures that the storage and processing of personal data obtained from SHM will take place in strict separation from the personal data that it processes for itself or for third parties.

2.4. All personal data supplied between Parties are subject to an obligation of secrecy towards third parties.

2.5. This obligation of secrecy is not applicable insofar as the Party providing the data has given consent to provide the information to third parties, or if the provision of the information to third parties is logical and necessary in view of the purpose for which the personal data were provided and/or for the fulfilment of this Agreement, or if the information must be disclosed to a third party pursuant to a statutory obligation or court ruling.

2.6. The obligations arising from Article 2 also apply to those who process personal data under the authority of the Parties, including, but not restricted to, employees in the broadest sense of the word.

2.7. If the Institution outsources any part or parts of the initial or further processing of the provided personal data to a processor, it will ensure that the processor processes the personal data in a proper and careful manner and in accordance with the applicable laws and regulations. Arrangements concerning the processing of personal data by a processor will be recorded in a suitable processor agreement. At the request of SHM, the Institution will provide insight into these processor agreements as well as a full list of the processors used by the Institution.

2.8. SHM endeavours to ensure that it does not provide more personal data to the Institution than necessary to achieve the intended purpose of the provision of information.

2.9 SHM endeavours to de-identify or pseudonymize the personal data insofar as possible or to make the personal data as untraceable as possible before their provision to the Institution.

2.10 The Institution guarantees that any Data linked to traceable personal data will not leave the Institution. SHM may carry out checks to ensure compliance with this provision and, in the event of actual or suspected non-compliance, may challenge the relevant employee of the Institution, such as a researcher or student, and report incorrect usage of SHM’s patient codes.

2.11 Because the Institution is established in a country outside the EEA, Parties also agree on the ‘Model Clauses (2004/915/EC)’ attached as Appendix 4 by concluding this Data Exchange Agreement. Each of Parties in turn is considered to be a Data exporter, or Data importer. The details laid down in Appendix 2 shall apply to Annex B of the EU Standard Model Clauses.

**Article 3. Security**

3.1. Each Party undertakes to ensure the security of personal data falling under their responsibility.

3.2. The Institution will implement and maintain sufficient and suitable technical and organizational security measures. Taking account of the nature of the personal data, the risk of the processing operations to be performed, available technology and implementation costs, these security measures will ensure an adequate level of protection to safeguard the personal data against any form of unlawful processing (such as unauthorized access, corruption, alteration or disclosure). These measures shall at least include (but are not restricted to):

a) storage of the Data on a computer or laptop that is protected with a strong password, effective virus scanner and firewall;

b) measures ensuring the physical and logical security of the Data;

c) measures ensuring that only authorized persons have access to the Data;

d) measures protecting the Data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;

e) measures preventing negligence or intentional improper use of the Data by employees.

3.3. The Institution will at all times have an effective written data protection policy for the processing of personal data, which will at least set out the measures mentioned in paragraph 2 of this Article 3. SHM has the right to check or instruct a third party to check compliance with the measures mentioned above under 3.2 and 3.3. The Institution will, at SHM’s request, provide an opportunity for such a compliance check at least once a year at a time to be agreed between Parties as well as on any other occasion that SHM may consider this appropriate in view of actual or suspected information or privacy incidents.

3.4. The Institution acknowledges that security requirements are subject to continuous change and that frequent evaluation and regular improvement of obsolete security measures is crucial to achieve effective security. The Institution will therefore evaluate, adjust, supplement and improve the measures on an ongoing basis in order to continue meeting its obligations under this Article 3.

**Article 4. Reporting of Data Breaches**

4.1. Parties are and remain independently responsible for reporting any data breaches that take place under their responsibility to the Personal Data Authority and/or the data subjects. A data breach is defined as: a security incident leading to the accidental or unlawful destruction, loss or alteration of Data or the unauthorized disclosure of or access to Data that have been transmitted, stored or otherwise processed within the meaning of Article 4 (12) of the GDPR.

4.2. The Institution is, without prejudice to the other obligations set out in this Article, obliged to reverse or minimize any negative consequences arising from a data breach as promptly as possible.

4.3. Parties will notify each other of an identified data breach relating to the data as mentioned under Article 4.1 within 24 hours of discovery. The Party nominated as data controller within the meaning of the GDPR is responsible, in conformity with the provisions of the GDPR, for deciding whether and how the Personal Data Authority and the data subjects must be informed. If the data subjects must be informed, Parties will discuss the best way to proceed with each other. Parties will assist each other to the best of their ability in this connection and will share all relevant information.

**Article 5. Attribution Rules**

5.1Submitted or published Articles must refer to Stichting HIV Monitoring and the Ministry of Health, Welfare and Sport, and the ATHENA cohort must be added as group author: "on behalf of the ATHENA observational HIV cohort" and "The ATHENA database is managed by Stichting HIV Monitoring and supported by a grant from the Dutch Ministry of Health, Welfare and Sport through the Centre for Infectious Disease Control of the National Institute for Public Health and the Environment". In addition, SHM acknowledgements must be included as an appendix; these will be provided by SHM on request.

**Article 6. Data Subject Rights**

6.1 A Party will independently handle a request from a data subject for access to the Data, within the meaning of Article 15 of the GDPR, or for the improvement, addition, alteration or restriction of Data within the meaning of Section 3 of the GDPR if said Party is the data controller for the requested processing operation.

6.2 A Party who receives a request (as mentioned in the preceding paragraph) for a processing operation for which it is not the data controller will forward the request to the Party that is the data controller for the requested processing operation. The data subject who submitted the request may be sent notification of this.

6.3 Parties will provide each other with all necessary information and assistance to enable the other Party to handle the request (as mentioned in paragraph 1).

**Article 7. Supervision and non-compliance**

7.1 On request, the Institution will provide SHM with all information on the manner in which the Agreement was fulfilled as well as access to all related Data and documents.

7.2 If the Institution acts in breach of this Agreement, SHM can suspend or withdraw the right to use the Data as described in Article 1 (1) and claim compensation for damages.

**Article 8. Liability**

8.1 SHM will make every effort to meet its obligations arising from this Agreement and accepts statutory obligations to pay compensation insofar as provided for in this Article.

8.2 SHM is exclusively liable in the event of a culpable failure to meet its obligations arising from this Agreement and exclusively for direct damage up to a maximum amount of €10,000 (ten thousand euros).

8.3 Direct damage is damage arising from a culpable failure to fulfil this Agreement and will exclusively consist of the compensation for damage resulting directly from said failure, i.e. compensation of the value of the action that was not performed (replacement compensation) up to the maximum amount mentioned in the preceding paragraph.

8.4 SHM rejects all liability for any other form of damage, including additional compensation in whatever form, compensation for indirect loss or consequential loss or compensation for lost revenue or profit or data loss. Nor is SHM liable for mistakes made by the Institution or those working under the authority of the Institution, or for damage resulting from the provision of incorrect or incomplete information by the Institution.

8.5 SHM is under no circumstances liable for any damage arising from delays, damage arising from loss of business details or the supplied data, damage arising from failure to meet deadlines as a result of changed circumstances, damage arising from the provision of inadequate cooperation or information by the Institution, or damage arising from information, research reports or advice provided by SHM whose content does not form an explicit part of this Agreement.

8.6 Any restriction or exclusion of liability provided for in this Agreement does not apply if the damage results from deliberate intent or conscious recklessness of the management of SHM or the Institution.

8.7 The Institution is liable for any damage arising from the non-performance of this Agreement or from any other further conditions agreed in connection with this Agreement.

8.8 The Institution indemnifies SHM against all claims from third parties (including data subjects) and will compensate SHM in full for any loss arising from such claims.

8.9 Any entitlement to compensation is subject to the condition that the Institution reports the damage to SHM in writing within 30 days of discovering the damage.

**Article 9. Force majeure**

9.1 SHM cannot be required to fulfil any obligation under this Agreement if this is prevented by force majeure. SHM is not liable for any damage arising from force majeure.

9.2 Force majeure at least includes power failures, internet failures, telecom infrastructure failures, network attacks (including DoS/DDoS attacks), malware or other malicious software, civil unrest, mobilization, war, import and export restrictions, strikes stagnating supply, fire and flooding, as well as cases where SHM is unable to fulfil the Agreement due to supplier failures, irrespective of the reason for said failures.

9.3 Prolonged force majeure does not entitle either Party to terminate this Agreement. During this period, neither Party is entitled to claim damages for any non-performance of the Agreement that is attributable to force majeure. The above does not affect any payment obligations relating to damage that is not directly or indirectly attributable to force majeure.

**Article 10. Disputes**

10.1 Parties will make every effort to find an appropriate solution for any disputes that may arise regarding the fulfilment of the Agreement. If the Parties are unable to resolve the matter, they will set up a disputes committee consisting of one member nominated by the Institution and one member nominated by SHM. These two members will nominate a third person to act as independent member and chairperson. If either Party disagrees with the verdict of this disputes committee, the dispute can be put to the competent court in the district where SHM is established.

**Article 11. Progress Report**

11.1 SHM expects to receive a progress report from the project leader at the start of each year, which will be published in SHM’s annual report. The project leader receives a template which must be completed for this purpose. The report must at least contain the following information:

a) summary of the progress, including background, methods, results and conclusions;

b) a list of publications in peer-reviewed journals or other printed publications originating from the research project; and

c) summaries of presentations, authors, date and place of presentation.

**Article 12. Duration and termination of the Agreement**

12.1 This Agreement commences on the date of signature by both Parties and is entered into for the period of the Study.

12.2 This Agreement ends automatically if the recognition of SHM as an HIV monitoring organization is ended and/or if SHM is dissolved.

12.3 This Agreement ends automatically if the Institution is declared bankrupt, requests suspension of payments, has all its assets placed under attachment, or is liquidated or dissolved.

12.4 The Agreement can only be terminated by both parties jointly. Early termination of the Agreement does not in any way release Parties from any obligations arising from this Agreement that are intended to continue after the termination of the Agreement.

**Article 13. Other provisions**

13.1 Parties may only amend this Agreement with mutual consent and will make every effort to make appropriate amendments to this Agreement whenever necessary as a result of legal or regulatory amendments.

13.2 If any provision in this Agreement proves to be invalid, this will not affect the validity of the entire Agreement. Parties will make every effort to replace the invalid provisions with new valid provisions that approximate the intention of the invalid provisions and this Agreement insofar as possible.

13.3 The logs and communications with the Institution as stored by SHM are deemed to be correct unless the Institution provides proof to the contrary.

13.4 This Agreement and its performance are governed by Dutch law.

13.5 In the event of any conflict between different agreements or their appendices, the order of precedence shall be as follows:

a) the Model Clauses (Appendix 4)

b) the Statement concerning the use of SHM data

c) these General Terms and Conditions (Appendix 1)

d) any other agreements or conditions.

Appendix 2: **Description of the Study and Data**

In connection with the following study:

[DESCRIPTION OF STUDY, SUCH AS RESEARCH TITLE AND NUMBER]

SHM shall provide the following Data to the Institution:

[DESCRIPTION OF DATA]

Appendix 3: **Statement regarding data transfer upon completion or discontinuation of the study.**

[INSTITUTION] (hereinafter: the Institution) declares that all SHM data received by the Institution in relation to the study

[STUDY + STUDY NUMBER], started on [DATA RECEIPT DATE] and ended on [RESEARCH END DATE],

were destroyed on [DATE].

- After the completion or discontinuation of analyses performed by the Institution, the Institution destroyed all original SHM data that were provided to the Institution in connection with the abovementioned study.

- The Institution has exclusively retained the analysis data set that is necessary to reproduce the research results in order to meet the moral and scientific obligation to enable verification of the research.

- A copy of the analysis data set will be shared with SHM. [NAME + CONTACT DETAILS] is the contact person for the analysis data set.

- The Institution is responsible for the proper reporting of the data analysis and the retention of the syntaxes/scripts written to carry out the analyses and obtain the research results.

- If a scientific journal requests the provision of the analysis data set, the Institution will request SHM’s consent for said provision and decide, together with SHM, in what form this provision of data can take place, while sufficiently safeguarding the privacy of Study participants whose Data are being shared.

- The Institution will provide SHM with a copy of all reports produced with these Data.

Signed at [PLACE], date [DATE]

[NAME OF INSTITUTION]

………………………….

[NAME + JOB TITLE]

Appendix 4**: Model clauses (2021/3972/EC)**

**STANDARD CONTRACTUAL CLAUSES**

**SECTION I**

*Clause 1*

***Purpose and scope***

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[[1]](#footnote-1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A.(hereinafter each “data exporter”), and

(ii) the entity/ies in a third country receiving the personal data from the data

exporter, directly or indirectly via another entity also Party to these Clauses, as

listed in Annex I.A. (hereinafter each “data importer”) have agreed to these standard contractual clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in

Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

(a) These Clauses set out appropriate safeguards, including enforceable data subject

rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to controllers, from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is

subject by virtue of Regulation (EU) 2016/679.

Clause 3

**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries,

against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause

8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and

Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause

8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause

9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three:

Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four:Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU)

2016/679.

Clause 4

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of

Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and

obligations provided for in Regulation (EU) 2016/679.

Clause 5

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are

transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses

from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES**

Clause 8

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data

importer is able, through the implementation of appropriate technical and organisational

measures, to satisfy its obligations under these Clauses.

**8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the

transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject’s prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in

the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of

another natural person.

**8.2 Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to

Clause 9, the data importer shall inform them, either directly or through the data

exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing

meaningful information), the purpose of such onward transfer and the ground

therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information,

including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate

effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter

under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3 Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or

received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

**8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[[2]](#footnote-2) of the data and all back-ups at the end of the retention period.

**8.5 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in

Annex II. The data importer shall carry out regular checks to ensure that these

measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and

freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 12. Such notification shall contain:

i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences,

iii) the measures taken or proposed to address the breach, and

iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data

breach, including its effects and any remedial action taken, and keep a record thereof.

**8.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

**8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the

European Union3[[3]](#footnote-3) (in the same country as the data importer or in another third country,

hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45

of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the

context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of

another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the

explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

**8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a

processor, processes the data only on its instructions.

**8.9 Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent

supervisory authority on request.

Clause 9

**Data subject rights**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the

processing of his/her personal data and the exercise of his/her rights under these

Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request[[4]](#footnote-4). The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of

recipients (as appropriate with a view to providing meaningful information) to

which the personal data has been or will be onward transferred, the purpose of

such onward transfers and their ground pursuant to Clause 8.7; and provide

information on the right to lodge a complaint with a supervisory authority in

accordance with Clause 11(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated

processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest

the decision, express his/her point of view and obtain review by a human

being.

(e) Where requests from a data subject are excessive, in particular because of their

repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of

Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 10

**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible

format, through individual notice or on its website, of a contact point authorised to

handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards

compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 12;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 11

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be

entitled to claim back from the other Party/ies that part of the compensation

corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to

avoid its own liability.

Clause 12

**Supervision**

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY**

**PUBLIC AUTHORITIES**

Clause 13

**Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the

processing chain, the number of actors involved and the transmission channels

used; intended onward transfers; the type of recipient; the purpose of

processing; the categories and format of the transferred personal data; the

economic sector in which the transfer occurs; the storage location of the data

transferred;

 (ii) the laws and practices of the third country of destination– including those

requiring the disclosure of data to public authorities or authorising access by

such authorities – relevant in light of the specific circumstances of the transfer,

and the applicable limitations and safeguards[[5]](#footnote-5);

(iii) any relevant contractual, technical or organisational safeguards put in place to

supplement the safeguards under these Clauses, including measures applied

during transmission and to the processing of the personal data in the country of

destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it

available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 15(d) and (e) shall apply.

Clause 14

**Obligations of the data importer in case of access by public authorities**

**14.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data

subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial

authorities, under the laws of the country of destination for the disclosure of

personal data transferred pursuant to these Clauses; such notification shall

include information about the personal data requested, the requesting authority,

the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data

transferred pursuant to these Clauses in accordance with the laws of the

country of destination; such notification shall include all information available

to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data

subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer

agrees to provide the data exporter, at regular intervals for the duration of the

contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer

pursuant to Clause 13(e) and Clause 15 to inform the data exporter promptly where it is unable to comply with these Clauses.

**14.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in

particular whether it remains within the powers granted to the requesting public

authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same

conditions, pursue possibilities of appeal. When challenging a request, the data

importer shall seek interim measures with a view to suspending the effects of the

request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 13(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

Clause 15

**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply

with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 13(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data

importer pursuant to paragraph (b) and compliance with these Clauses is not

restored within a reasonable time and in any event within one month of

suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court

or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer

shall continue to ensure compliance with these Clauses. In case of local laws

applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where

(i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply;

or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 16

**Governing law**

These Clauses shall be governed by the law of one of the EU Member States,

provided such law allows for third-party beneficiary rights. The Parties agree that this

shall be the law of \_\_\_\_\_\_\_ (specify Member State).

Clause 17

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU

Member State.

(b) The Parties agree that those shall be the courts of \_\_\_\_\_ (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

**ANNEX I**

**LIST OF PARTIES** (add all parties involved)

Data exporter(s):

Name: Stichting HIV Monitoring

Address: Meibergdreef 9, 1105 AZ Amsterdam

E-mail: hiv.monitoring@amsterdamumc.nl

Contact data protection officer: Annemieke Feyt, privacy.shm@amsterdamumc.nl

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: data transfer for research

Signature and date: …

Role: controller

2. xx

Data importer(s):

Name: …

Address: …

Contact data protection officer: …. (if applicable)

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. xx

**DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Hiv-patiënts

Categories of personal data transferred

………………………..

Sensitive data transferred and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed

specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

………………………..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

…………………………

Nature of the processing

Research

Purpose(s) of the data transfer and further processing

………………………..

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

……………………..

**COMPETENT SUPERVISORY AUTHORITY**

AP Autoriteit Persoonsgegevens in the Netherlands: <https://autoriteitpersoonsgegevens.nl/nl>

**ANNEX 2**

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING**

**TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY**

**OF THE DATA**

SHM: data exporter

Data disclosure agreement:

* Data disclosure agreement will be concluded with the data importer.

Datasets:

* In the created datasets, day of birth will be replaced by age of year of birth.
* In the created datasets, the M-number will be replaced by a random created number (SAS script). The key between this random number and M-number will stay at SHM and is only insightful for the SHM analysts.
* Datasets will be encrypted and sent by save e-mail with a key sent by a communication channel other than mail.

Research completed or discontinued

* Within one month after completion or discontinued original SHM data and copies of the data needs to be destroyed.

<name company>: data importer

<Description of measures, see below>

*EXPLANATORY NOTE:*

*The technical and organisational measures must be described in specific (and not generic)terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.*

*Description of the technical and organisational measures implemented by the data*

*importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks forthe rights and freedoms of natural persons.*

*[Examples of possible measures:]*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of*

*processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal*

*data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical*

*and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are*

*processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also describe the specific technical and organisational*

*measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporte*

1. Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union

institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing)

not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of 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 of 21.11.2018, p. 39), to the extent these Clauses and the data protection 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 of 21.11.2018, p. 39), to the extent these Clauses and the data protection

obligations as set out in the contract or other legal act between the controller and the processor pursuant to

Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the

controller and processor rely on the standard contractual clauses included in Decision […]. [↑](#footnote-ref-1)
2. This requires rendering the data anonymous in such a way that the individual is no longer identifiable by

anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible. [↑](#footnote-ref-2)
3. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the

European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union

data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has

been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party

located in the EEA does not qualify as an onward transfer for the purpose of these Clauses. [↑](#footnote-ref-3)
4. That period may be extended by a maximum of two more months, to the extent necessary taking into account

the complexity and number of requests. The data importer shall duly and promptly inform the data subject of

any such extension. [↑](#footnote-ref-4)
5. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from comply with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. [↑](#footnote-ref-5)