Steward Data Processing Agreement V1

https://sovrin.org/

This Data Processing Agreement ("**DPA**") supplements the Sovrin Steward Agreement ("**SSA**") between the Sovrin Foundation and Steward, as may be amended from time to time, and is hereby incorporated by reference into the SSA. All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the SSA or in the Sovrin Governance Framework. In the event of any inconsistency or conflict between this DPA and the SSA, this DPA will govern. This DPA will survive termination of the SSA as long as Steward Processes Personal Data. The Sovrin Foundation and Steward agree as follows:

1. Definitions.

(a) "**GDPR**" means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and any amendment or replacement to it.

(b) "**Impermissible Personal Data**" means the Personal Data that a Transaction Author writes to the Sovrin Ledger and that a Steward Processes that is not Permissible Personal Data in accordance with the Transaction Author Agreement.

(c) "**Permissible Personal Data**" means the Personal Data expressly listed in Schedule 1 that a Transaction Author writes to the Sovrin Ledger in accordance with the Transaction Author Agreement and that a Steward Processes through the Steward Node.

(d) **"Personal Data**" means information that relates, directly or indirectly, to a data subject, including without limitation, names, email addresses, postal addresses, identification numbers, location data, online identifiers, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the data subject.

(e) "**Process**" or "**Processing**" means any operation or set of operations which is performed on Node Data, whether or not by automated means, such as the access, collection, use, storage, disclosure, dissemination, combination, recording, organization, structuring, adaption, alteration, copying, transfer, retrieval, consultation, disposal, restriction, erasure and/or destruction of Node Data.

(f) "**Node Data**" means any information which includes any Personal Data that Steward Processes through the Steward Node.

(g) "**Security Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Node Data or otherwise affecting Steward's operation of the Steward Node in compliance with this DPA.

(h) "**Sovrin Governance Framework**" means the Sovrin Foundation's governance policies and rules available at https://sovrin.org/governance-framework/ or any successor website.

(i) "**Standard Contractual Clauses**" means the standard contractual clauses, as agreed by the European Commission, for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection as set out in Commission

Decision C(2010) 593, as updated, amended replaced or superseded from time to time by the European Commission.

(j) "**Subprocessor**" means any processor engaged by Steward who will access or receive Personal Data from Steward for Processing.

The terms "controller", "data subject", "personal data", "processor", and "supervisory authority" as used in this DPA will have the meanings ascribed to them in the GDPR.

2. Purpose of Processing Personal Data. In connection with performing its services obligations under the SSA (the "**Services**") Steward may Process Node Data in accordance with this DPA. Specific details of the Processing activities including categories and type of Node Data that Steward will Process in connection with the SSA are set forth in Schedule 1 (Scope of Processing).

3. Processor and Controller Responsibilities.

(a) The Sovrin Foundation and Steward agree that the Sovrin Foundation is the legal entity that serves as the designated data controller for Personal Data written to the Sovrin Ledger for the purpose of making decisions relating to the architecture, operation and governance of the Sovrin Network and being the point of contact as explained in Section 3(c) below. Therefore, the parties acknowledge and agree that: (a) Steward is a processor of Node Data under the GDPR and (b) the Sovrin Foundation is the designated controller of Node Data under the GDPR and will be responsible for the lawfulness of the Processing of such data in compliance with the GDPR and other data privacy laws applicable to it as data controller.

(b) Transaction Authors are independent controllers of any Personal Data they write to the Sovrin Ledger. Transaction Authors and the Sovrin Foundation independently determine the purposes and means of Processing Personal Data. In no event will Transaction Authors be deemed joint controllers with the Sovrin Foundation under Article 26 of the GDPR or deemed to jointly determine and control the purposes and means of Processing Personal Data. The Sovrin Foundation will provide the list of all other controllers (i.e., Transaction Authors) on behalf of which the Steward Processes Personal Data through the Sovrin Ledger by referring Stewards to information available on the Sovrin Ledger.

(c) As an accommodation to Steward, the Sovrin Foundation shall serve as the administrative coordinator for a Transaction Author's exercise of its rights and performance of its obligations under the GDPR by serving as a single point of contact for Steward and by obtaining all necessary permissions from the other controllers (i.e., Transaction Authors) for the Processing of the Node Data. Steward shall be discharged of its obligation to inform or notify another Controller when it has provided such information or notice required under the GDPR to the Sovrin Foundation. Similarly, Steward will serve as a single point of contact for Sovrin Foundation with respect to its obligations as a processor under this DPA. However, in no event will the Sovrin Foundation be held liable for the actions or omissions of any Transaction Author arising out of any Personal Data that such Transaction Author writes to the Sovrin Ledger in breach of the Transaction Author Agreement and the Sovrin Governance Framework, including but not limited to any Impermissible Personal Data. Notwithstanding the foregoing, if a Transaction Author writes Permissible Personal Data to

the Sovrin Ledger in express compliance with the Transaction Author Agreement and the Sovrin Governance Framework, the Sovrin Foundation is responsible for the lawfulness of such Processing once such Permissible Personal Data is written to the Sovrin Ledger.

4. **Steward Responsibilities**. Steward will:

(a) Process Node Data only in accordance with the Sovrin Governance Framework and other lawful documented instructions ("**Additional Instruction**") from the Sovrin Foundation. If Steward notifies Sovrin Foundation that such other instruction is not feasible, the parties shall work together to find an alternative. If neither the Additional Instruction nor an alternative is feasible, the Sovrin Foundation may terminate the affected Services pursuant to the SSA. Steward will inform the Sovrin Foundation if it is aware or reasonably suspects that the Sovrin Foundation's instructions regarding the Processing of Node Data may breach the GDPR and may suspend the performance of such instruction until the Sovrin Foundation has modified the instruction or confirmed its lawfulness in documented form;

(b) ensure that persons authorized to Process the Node Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality even if such Node Data is public or already in the possession of Steward;

(c) promptly notify and reasonably assist the Sovrin Foundation, if it receives a request from a data subject for access to, correction, amendment, deletion of or objection to the Processing of Node Data relating to such individual;

(d) assist the Sovrin Foundation, at the Sovrin Foundation's request, in complying with the Sovrin Foundation's obligations to respond to data subject requests and its compliance regarding Node Data Processed by Steward, to the extent technically feasible given the architecture of the Sovrin Network taking into account the nature of the Processing and the information available to Steward;

(e) at the direction of the Sovrin Foundation, cooperate and assist the Sovrin Foundation in conducting a data protection impact assessment and related consultations with any supervisory authority; and

(f) comply with the GDPR and other data privacy laws applicable to Steward as a processor in Processing the Node Data and in the performance of the Services.

5. **Subprocessors.** The Sovrin Foundation generally authorizes the use of Subprocessors to Process Node Data in connection with fulfilling Steward's obligations under the SSA and/or this DPA; provided that such Subprocessors meet the requirements set forth in the Sovrin Governance Framework. Steward will remain fully responsible for fulfilment of its obligations under this DPA and will remain the primary point of contact regarding any Processing of Node Data. Steward will be responsible for the acts and omissions of its Subprocessors and anyone else to which the Processing of Node Data or operation of the Node has been delegated by it. Steward will impose contractual obligations on its Subprocessors that are at least equivalent to those obligations imposed on Steward under this DPA. Upon Sovrin Foundation's request, Sovrin Foundation has the right to review and recommend changes to the relevant subprocessing contract between Steward and its

Subprocessors, and Steward will reasonably comply with such request. Steward will notify the Sovrin Foundation in writing (email acceptable) of any proposed changes to its Subprocessors and give the Sovrin Foundation the opportunity to object to such changes. Within thirty (30) days after Steward notifies the Sovrin Foundation of the intended change, the Sovrin Foundation can object to the addition of a Subprocessor on the basis that such addition would cause the Sovrin Foundation to violate the GDPR or other applicable privacy laws. Such objection shall be in writing and include specific reasons for its objection and reasonable options to mitigate, if any. If the Sovrin Foundation does not object within such period, the respective Subprocessor will be permitted to Process Node Data. If the Sovrin Foundation objects to the addition of a Subprocessor in accordance with this Section 5 and Steward cannot reasonably accommodate such objection, Steward will promptly notify it in writing stating in reasonable detail the reason for such inability to accommodate such objection. In such event, the parties shall cooperate in good faith to find a feasible workaround; provided that, if the parties are unable to find a feasible workaround within thirty (30) days of Steward's notice, then the Sovrin Foundation may terminate the affected Services as set out in the SSA without any liability to Steward.

6. **Data Transfers.** For all Stewards not based in the European Economic Area (EEA), by signing this DPA, each party is deemed to have signed the Standard Contractual Clauses, attached hereto as Schedule 2, with the Sovrin Foundation, on its own and on behalf of the respective Transaction Authors, as the "Data Exporter" and Steward as the "Data Importer" (as each of these terms is defined in the Standard Contractual Clauses). If a Subprocessor of Steward is a Data Importer, Steward agrees that it will enter into the EU controller to non-EU or EEA processor Standard Contractual Clauses on behalf of such Subprocessor if it is an affiliate of Steward, otherwise Steward will enter into a written agreement imposing obligations on such Subprocessor at least as stringent as those imposed on Steward in accordance with Clause 11 of the Standard Contractual Clauses.

7. **Security Safeguards**. Steward will implement, maintain and monitor a comprehensive written information security policy that contains appropriate technical and organizational measures (the "**Steward TOMs**") to protect the security and confidentiality of Node Data. The Steward TOMs will be appropriate to the Node Data that Steward Processes and will meet the requirements set forth in Article 32 of the GDPR, the SSA and the Sovrin Governance Framework. The Steward TOMs will meet the standards in Appendix 2 of the Standard Contractual Clauses attached hereto and the Steward Technical and Organizational Policies as set forth in the Sovrin Governance Framework (the "**Steward TOPs**"). The parties agree the Steward TOPS satisfy the requirements of this Section 7. The Sovrin Foundation may update the Steward TOPs pursuant to the Sovrin Governance Framework in light of the development and progression of technology. Such updates will be communicated to Steward via electronic communication and/or notification on the Sovrin Foundation website. Accordingly, Steward reserves the right to implement Steward TOMs that exceed the requirements of the Steward TOPs; provided that the functionality and security of the Services are not degraded.

8. **Audits**. Upon reasonable notice to Steward, the Sovrin Foundation may conduct or may engage an independent third party which shall not be a direct competitor of Steward and shall be bound to obligations of confidentiality ("**Auditor**") to conduct an information security audit of Steward to meet its audit requirements under Article 28 of the GDPR and its obligations under Articles 32 to 36 of the GDPR. Prior to commencement of the audit, the parties will agree in writing to the terms and conditions governing the conduct of the audit. Steward will reasonably cooperate with the Sovrin Foundation and/or its Auditor in conducting such audit; provided that, nothing in this DPA will

require Steward to provide information to the Sovrin Foundation that is publicly available on the Sovrin Ledger. Sovrin Foundation agrees to reimburse reasonable and documented expenses incurred by Steward related to any information security audit initiated by Sovrin Foundation.

9. **Security Breach**. Without undue delay after becoming aware, Steward will notify the Sovrin Foundation in writing of any actual Security Breach. Steward will promptly investigate any Security Breach and is obligated to expend no more than an amount mutually agreed between Sovrin Foundation and Steward. Any additional amount of required expenditure will be the obligation of Sovrin Foundation consistent with Section 13 below. Steward will provide the Sovrin Foundation with reasonable assistance to satisfy any legal obligations of the Sovrin Foundation in relation to such Security Breach (including any obligation to notify data protection authorities or data subjects). In the event of a Security Breach, the Sovrin Foundation has the right to control the breach notification process, unless the GDPR dictates otherwise.

10. **Return or Destruction of Node Data**. Upon termination or expiration of the SSA and to the extent technically feasible given the architecture of the Sovrin Network, Steward will return to the Sovrin Foundation or destroy all Node Data and all copies thereof in its possession or under its control as specified in the Steward TOPs, except to the extent that Steward is required under the GDPR to keep a copy of the Node Data.

11. **Records**. In addition to the record provided by the Sovrin Ledger, Steward will keep at its normal place of business all information relating to Steward's Processing of Node Data as described in the Steward TOPs and in this DPA pursuant to Article 28(h) of the GDPR. Steward will make such documents and all other information necessary to demonstrate compliance with its obligations in Article 28(h) of the GDPR available to the Sovrin Foundation upon request.

12. **Limitation of Liability**. Notwithstanding anything to the contrary in the SSA, a party's liability for breach of its obligations including any claims arising from this DPA or the Standard Contractual Clauses, will be limited as set forth below.

(a) EXCEPT IN THE EVENT OF EITHER PARTY'S GROSS NEGLIGENCE, WILFUL MISCONDUCT OR FRAUD, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES UNDER THIS DPA, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR DATA, OR OTHERWISE, EVEN IF THE OTHER PARTY IS EXPRESSLY ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. EXCEPT IN THE EVENT OF EITHER PARTY'S GROSS NEGLIGENCE, WILFUL MISCONDUCT OR FRAUD, IN NO EVENT SHALL EITHER PARTY'S LIABILITY UNDER THIS DPA EXCEED $250,000 USD IN THE AGGREGATE. IN THE EVENT OF EITHER PARTY'S GROSS NEGLIGENCE, SUCH PARTY'S LIABILITY UNDER THIS DPA SHALL NOT EXCEED $500,000 USD IN THE AGGREGATE. IN THE EVENT OF EITHER PARTY'S WILFUL MISCONDUCT OR FRAUD, THERE SHALL BE NO DOLLAR CAP ON SUCH PARTY'S LIABILITY UNDER THIS DPA.

(b) However, in the event of any conflict between the Standard Contractual Clauses and this Section 12, the Standard Contractual Clauses will prevail but only with respect to claims arising from the Standard Contractual Clauses.

(c) As the Sovrin Foundation is entering into this DPA on behalf of itself and the Transaction Authors, the Sovrin Foundation will secure a Transaction Author's consent to the limitation of liability set forth in this Section 12 through the Transaction Author Agreement. Therefore a Transaction Author will be considered a "party" as used in this Section 12 for the purpose of interpreting this limitation of liability.

(d) Without prejudice to Art. 82 of GDPR and for the avoidance of doubt, no controller will be jointly and severally liable with any other controller to Steward or vice versa.

13. **Assistance:** The Sovrin Foundation will make a written request to Steward for any assistance referred to in this DPA. Steward and the Sovrin Foundation will mutually agree in writing to a reasonable charge for Steward to perform such assistance or an Additional Instruction. If the parties do not mutually agree to such reasonable charge, the parties agree to reasonably cooperate to find a feasible solution.

14. **Disputes.** The parties will make good faith efforts to first resolve internally any dispute under this DPA. Neither party will seek any external remedies until thirty (30) days have elapsed from the initiation of such good faith efforts. At the conclusion of any such thirty (30) day period, each party shall be entitled as a matter of right to seek remedies for any dispute, controversy, or claim arising out of, relating to, involving, or having any connection with this DPA, including any question regarding the validity, interpretation, scope, performance, or enforceability of this dispute resolution provision, in any court of competent jurisdiction, in equity or otherwise. The rights conferred upon the parties by the preceding sentence shall not be exclusive of any other rights or remedies which each party may have at law, in equity or otherwise.

The Parties hereto have caused this DPA to be executed by their duly authorized representatives as of the Effective Date.

Sovrin Foundation

By: _____

Name: _____

Title: _____

Date: _____

Steward

By: _____

Name: _____

Title: _____

Date: _____

SCHEDULE 1 Scope of Processing

Subject Matter of Processing: The context for the Processing of Node Data is Steward's operation, maintenance and hosting of a Node under the SSA.

Duration of Processing: The Processing will begin on the effective date of the SSA and will continue through the period from expiration of the SSA until deletion of all Node Data by Steward in accordance with this DPA.

Nature and Purpose of Processing: Steward will Process Node Data solely as necessary to operate, maintain and host a Node in accordance with the SSA and the Sovrin Governance Framework.

Types of Personal Data:

Permissible Personal Data: Public DIDs, public keys, and any other Personal Data that a Transaction Author writes to the Sovrin Ledger in accordance with the Transaction Author Agreement.

Impermissible Personal Data: The Sovrin Governance Framework prohibits writing of Impermissible Personal Data to the Sovrin Ledger. If Impermissible Personal Data is written to the Sovrin Ledger, Steward has no obligation or liability with respect to such Impermissible Personal Data, except to promptly notify the Sovrin Foundation in writing.

Categories of Data Subjects: Node Data may belong to any of the following categories of data subjects:

- Transaction Authors who are natural persons

Order of precedence

The Sovrin Foundation may update the content of this Schedule 1 (Scope of Processing), including the types of Permissible Personal Data and Impermissible Personal Data, from time to time by updating the Sovrin Governance Framework.

Solely with reference to the details of the Processing of the Node Data included in this Schedule 1, in case of conflict, the Sovrin Governance Framework will prevail over the present Schedule 1.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C (2010)593

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

The Sovrin Foundation, on its own behalf and on behalf of applicable Transaction Authors who may act as independent controllers for purposes of these clauses.

(the data **exporter**)

And

The Steward named in the SSA

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of

individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be

transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer [2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the date exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses([3]). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): The Sovrin Foundation on its own behalf and on behalf of applicable Transaction Authors

On behalf of the data importer:

Name (written out in full): .....

Position: .....

Address:

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

See Schedule 1 to this DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see the Steward TOPs as set forth in the Sovrin Governance Framework.