Data Processing Addendum 1

This Addendum on Data Processing (hereinafter: "Addendum") is made on the Effective Date, by and between:

Customer as defined by the SOW

– hereinafter referred to as "**Controller**" –

and

Merrill entity as defined by the SOW

– hereinafter referred to as "**Processor**" –

Hereinafter each individually referred to also as the "**Party**" and collectively as the "**Parties**"

Preamble:

(A) The Parties have entered into an Agreement which outlines the Services to be provided (definitions provided in Section 1 below). As part of the provision of Services by the Processor, Personal Data may be transferred by the Controller to the Processor.

(B) In the event of any conflict between the provisions in this Addendum and the provisions set forth in the Agreement, the provision or provisions of this Addendum will prevail. Capitalized terms not defined in this Addendum are defined in the Agreement.

(C) To ensure compliance by the Parties with Processing obligations pursuant to the Data Protection Rules, as amended from time to time, the Parties hereby agree as follows:

1. Definitions

1.1. "**Appendix**" means the appendix annexed to and forming an integral part of this Addendum;

1.2. "**Data Protection Country**" or "Data Protection Countries" means a country or countries where privacy, data protection or information security laws are in place that regulate personal or private information or Personal Data, including but not limited to the European Economic Area, Brazil, Hong Kong, Australia, Singapore, Canada, United Kingdom and Switzerland.

1.3. "**Data Protection Rules**" means the relevant national laws that apply to the Processing of Personal Data in Data Protection Countries, including but not limited to any applicable privacy and information security laws and regulations that apply from time to time;

1.4. "**Data Subject**" means an identified or identifiable natural person whose Personal Data is subject to Processing; an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity;

1.5. "**Information Security Incident**" means any transfer, access and disclosure to third parties, or Processing in breach of this Addendum or the Data Protection Rules or any event directly or indirectly affecting the confidentiality, integrity, authenticity of Personal Data;

1.6. "Agreement" means the Statement of Work and the General Terms and Conditions between the Controller and the Processor;

1.7. "**Personal Data**" means any information relating to a Data Subject contain within the Content.

1.9. "**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

1.10 "**Services**" means the provision of services as described in the Agreement and this Addendum;

1.11 "**Special Categories of Data**" means the Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data that uniquely identify a natural person, as well as Personal Data concerninghealth, sex life or sexual orientation

2. Processing Activities

The Controller shall have sole responsibility for the accuracy, quality, and legality of Processing of Personal Data, and shall comply with and is responsible for its invited Users compliance with applicable Data Protection Rules. The Processor agrees to Process the Personal Data to provide Services in accordance with this Addendum and the Agreement, pursuant to Controller's written instructions as set forth in Appendix 1 of this Addendum, and as may be communicated by the Controller from time to time. If the Processor believes that an instruction infringes applicable Data Protection Rules, it will immediately notify the Controller. The Processor undertakes to Process the Personal Data in accordance with applicable Data Protection Rules.

3. Duration and Termination of this Addendum

3.1. This Addendum is effective as of the Effective Date and shall remain in force during the term of the Agreement. This Addendum will terminate automatically with the termination or expiry of any SOW.

3.2. Notwithstanding the termination of this Addendum, the Processor and any subcontractors shall continue to be bound by their obligations of confidentiality.

4. International Transfers

The Processor undertakes to Process the Personal Data in accordance with its obligations as a Processor in the Standard Contractual Clauses incorporated into this Addendum as Appendix 3. Controller acknowledges that Processor may Process Personal Data outside the EEA, United Kingdom and United States; however, Personal Data will continued to be stored in a Data Protection Country or in the United States. The Processor will only onward transfer Personal Data in compliance with Data Protection Rules and notify Controller if it can no longer provide adequate level of protection as required by Data Protection Rules.

5. Confidentiality and Information Security Standards

5.1. The Processor shall keep Personal Data strictly confidential. The Processor shall ensure that its employees are aware of the applicable privacy and information security requirements and are held by legally binding confidentiality obligations.

5.2. The Processor will implement appropriate operational, technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access described in Appendix 2.

5.3. The Processor will update the technical and organizational security measures in line with reasonable technological developments as determined by Processor and provide updated documentation to the Controller on request in the form of its current ISO 27001 certification.

6. Cooperation and Notification Obligations

6.1. The Parties will co-operate with each other to promptly and effectively handle enquiries, complaints, and claims relating to the Processing of Personal Data from any government authority or Data Subjects. If a Data Subject should apply directly to the Processor to exercise his/her Personal Data rights, the Processor must forward this request to the Controller without undue delay. The Processor will notify the Controller immediately if the Personal Data is subject to a control or investigation by public authorities and will not disclose any Personal Data without the prior consent of the Controller. The Processor will provide the public authorities, upon request, with information regarding Processing under this Addendum as well as allow inspections within the scope stated in this Section 7.

6.2. The Processor will notify the Controller of an Information Security Incident that is determined to affect Controller's Personal Data without undue delay. The Processor shall provide Controller with the information to help and reasonably assist Controller as required by Data Protection Rules.

7. Controller's Audit and Inspection Rights

Upon Controller's request, Processor shall make available to Controller information necessary to demonstrate Controller's compliance with the obligations in the Addendum and Data Protection Rules and allow for and contribute to audits, including inspections conducted by Controller or an independent third party auditor mandated by Controller for the purpose of verifying the Processor's compliance with this Addendum, subject to the persons performing such audit sign a non-disclosure agreement with the Processor. All inspections shall be conducted during normal working hours and

without interfering with the course of the Processor's business.

8. Use of Subcontractors

8.1 Controller hereby acknowledges and agrees that Processor may use Subcontractors to Process Personal Data. Processor will make available to Controller its current list of Subcontractors upon request. Any Subcontractor will be permitted to Process Personal Data only to deliver the Services Processor has retained them to provide and will be contractually bound by contractual obligations no less protective than this Addendum. Processor shall be liable for the acts and omissions of any Subcontractor as if the acts or omissions were performed by Processor. The Processor will keep the Controller updated of any changes to the subcontracted Processing and provide the Controller with a copy of this subcontracting agreement upon request.

8.2 If the Processor intends to appoint or replace a Subcontractor covered by this Addendum, the Processor shall inform Controller of this advance and give Controller the opportunity to reasonably object to such changes. The Supplier shall provide Controller with all information that Controller may reasonably request to assess whether the appointment of the proposed Subcontractor complies with the Controller's obligations under this Addendum and applicable Data Protection Rules.

9. Return and Deletion of Personal Data

Upon the request of the Controller or upon termination of this Addendum, the Processor will, return or destroy all Personal Data and copies thereof. Upon the request of the Controller, the Processor will certify that this has been done.

10. Liability & Indemnification

10.1 The Liability of the Parties and the limitation thereof shall be in accordance with the Agreement.

10.2 The Controller shall indemnify Processor against all claims by any third party with regard to the processing of personal data provided to the Processor if the processing of such data was not permitted by Data Protection Rules.

Controller:	**Processor:**
By:_____	By:_____
Name/Title:_____	Name/Title:_____
Date: _____	Date:_____

Appendix 1: Processed Personal Data and Purposes

Personal Data are transferred and Processed for the **following purposes**:

- Secure online repository and data sharing for corporate due diligence, related transactions or internal business purposes.

Scope of Processing:

- As described in the Statement of Work, Processor provides virtual data room, a secure online repository for storing, managing, collaborating on and distributing data and documents.

Categories of Personal Data:

- Names, address, company email address, company phone number, national identification numbers, compensation and benefits, holiday and pension information, job titles and functions and potentially all other types of personal data embedded in the business information uploaded by Controller's Administrator onto the virtual data room.

Special Categories of Data (if applicable):

The Personal Data concerns the following Special Categories of Data (please specify):

- None, unless otherwise identified by Controller

Data Subjects:

The Personal Data concerns the following categories of Data Subjects:

- Business information that may include owner, employee, customer, contractor and vendor data.

Appendix 2: Information Security Measures

Appendix 2 includes:

Section I: Processor's General Data Security Plan
Section II: Processor's Information Security Procedure/Process

I. General Data Security Plan

The Processor undertakes to institute and maintain the following data protection measures:

	Security Requirement	How the Processor implements the specific information security measure
	Please describe the access control (physical) measures in your company to prevent unauthorized persons from gaining access to Processing systems within which Personal Data are Processed or used (If your company has several subsidiaries or branches please distinguish the differences between the locations).	All data centers hold ISO 27001:2013 and SOC 2 Type 2 certifications. A perimeter of multiple security controls are in place for all data centers which include multiple require authentication methods in order to gain access.
2.	Please describe the admission control measures taken in your company to prevent Processing systems from being used without authorization.	Authorized users are based on business requirements and require management role identification and approval. Time out features, strong authentication requirements and access rights are implemented and trackable.
3.	Please describe the access control (virtual) measures taken in your company to ensure that persons entitled to use a Processing system have access only to Personal Data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorizations in the course of Processing or use and after storage.	Authorized user access is managed through a formal registration and de-registration procedure for granting and revoking access to all systems and services based on job role. Audit reporting allows for the accurate monitoring of user activity and access controls are in place to protect data integrity and confidentiality.
4.	Describe the transmission control measures taken in your company to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities are envisaged.	Processor has removable media policy with the appropriate technical controls in place to protect data integrity and confidentiality and prohibit unauthorized Personal Data transfer. Remote access is controlled using multifactor authentication. Data is encrypted at rest and in-transit using government approved encryption technologies.

5.	Describe the measures of input control to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into Processing systems, modified or removed.	Processor is agnostic to the data the client chooses to upload. All user actions with respect to data integrity and confidentiality are tracked and reportable. Controller has sole determination on what data is provided to Processor.
6.	Describe the assignment control measures in your company to ensure that, in the case of commissioned Processing, the Personal Data are Processed strictly in accordance with the instructions.	Audits are conducted annually as part of ISO 27001 Certification and SOC 2 Type 2 Report to ensure compliance requirements are being met. Authorized users complete Training and acknowledge compliance with company code of conduct and policies annually. All employees and contractors are required to sign NDA.
7.	Describe the availability control measures your company takes to ensure that Personal Data are protected from accidental destruction or loss.	Processor has redundancy with each platform and maintains logs of system availability. In addition, redundancy allows for continuous system backups. Processor has Disaster Recovery and Business Continuity Plans that are reviewed, updated and tested annually.
8.	Describe the separation control measures your company has taken to ensure that Personal Data collected for different purposes can be Processed separately.	Logical separation is maintained within the same multi-tenant database. Authorized users are restricted to the project to which they are authenticated. Processor maintains a 3-tiered application with separation of data; development, test and production.

II. Processor's Information Security Procedure/Process

The Processor implements and follows the following standards, processes, and procedures:

Merrill operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope: The management of information security applies to processes for the protection of client information regarding the global services of financial transactions and reporting, marketing and communications for regulatory industries, and customer content and collaborations.

Appendix 3: Standard Contractual Clauses

For the purposes of applicable Data Protection Laws 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: Customer as defined by the SOW, unless otherwise identified below:

Address:

Tel.:…….. E-mail:…….

(the data **exporter**)

And

Name of the data importing organisation: DATASITE LLC.

Address: 733 S. Marquette Ave, Suite 600 Minneapolis, MN 55402,

Tel.: US 888 867 0309, EMEA +44 203 928 0400 E-mail: service@datasite.com

(collectively "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

[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.

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 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;

(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:

---

[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.

(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 data 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 of 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

Subprocessing

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 subprocessor 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 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.

---

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