Data Processing Addendum

This Data Processing Addendum (including its appendices) ("DPA") forms part of and is incorporated in the Agreement between Client and Suplexed. As used herein, "Agreement" refers to an agreement or terms of service applicable to software and services provided by Suplexed LLC and/or its subsidiaries, affiliates, and/or divisions as may change from time to time (collectively, "Suplexed"). As used herein, "Client" refers to the individual or entity subject to the Agreement.

This DPA supplements the terms and conditions set forth in the Agreement (the "Terms") and supersedes any of the Terms relating to data processing and security. This DPA will be effective as of the effective date of the Agreement. To the extent of any conflict or inconsistency between this DPA and the Terms, this DPA will govern.

Definitions

1. In this DPA:

    a. "**Applicable Law**" means all laws, regulations and other legal requirements applicable to either (i) Suplexed or its affiliates in their role as service provider processing data or (ii) Client, as the case may be. Applicable Law includes all laws, regulations and other legal requirements of any jurisdiction relating to privacy, data security, communications secrecy, Personal Data Breach notification, or the Processing of Personal Data, such as, to the extent applicable, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"). For the avoidance of doubt, each party is only responsible for the Applicable Law applicable to it.

    b. "**Personal Data**" means any information relating to an identified or identifiable individual, within the meaning and applicability of the GDPR.

    c. "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

    d. "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

    e. "**Subprocessor**" means any Suplexed affiliate or subcontractor engaged by Suplexed for the Processing of Personal Data.

Scope

2. This DPA applies to the Personal Data that Suplexed receives from Client, or otherwise Processes for or on behalf of Client, in connection with the Services provided by Suplexed under the Terms. As used herein, the "Services" means providing information

and digital multi-channel distribution to buyers and sellers in the resale market for sneakers, streetwear, watches, handbags and other "wearable" personal accessories ("Covered Products").

Client Responsibilities

3. Client acknowledges that it is using the Services as the lawful owner of any Covered Products listed and/or made available for sale via the Services (and all data related thereto) and, therefore, is considered to be a "controller" under the GDPR and that Suplexed is a "processor."

4. Client will comply with all Applicable Laws, including that it will establish legal bases for its and Suplexed's Processing of Personal Data and obtain any consents required under Applicable Laws for Suplexed to provide the Services.

Client Instructions to Suplexed

5. Suplexed will Process the Personal Data only as described under the Terms, unless obligated to do otherwise by Applicable Law. In such case, Suplexed shall inform Client of that legal requirement before Processing, unless that legal requirement prohibits providing such information on important grounds of public interest. For the avoidance of doubt, the details of the Processing are as follows:

    a. Subject matter of the Processing: The subject matter of the Processing is the Personal Data Processed by Suplexed on behalf of Client. See the Terms for details.

    b. Duration of the Processing: The duration of the Processing under this DPA is the term of the Terms, subject to any applicable deletion or retention provisions. See the Terms for details.

    c. Purpose and nature of the Processing: Provision of the Services in respect of Covered Products.

    d. Type(s) of Personal Data Processed: Personal Data provided by Client to Suplexed for Processing under the Agreement, which could consist of any Personal Data associated with the purchase or resale of Covered Products.

    e. Categories of data subjects: The data subjects whose Personal Data Client provides to Suplexed for Processing under the Terms, which could consist of buyers or sellers of Covered Products.

6. The Terms and this DPA (each as may be amended from time to time), along with Client's use of any options in the Services (as Client may be able to select from time to time, depending on the Services), constitute Client's complete and final instructions to Suplexed regarding the Processing of Personal Data, including for purposes of the Standard Contractual Clauses attached as Annex B. Client shall not instruct Suplexed to Process Personal Data in violation of Applicable Law, and Suplexed shall promptly inform Client if, in Suplexed's opinion, an instruction from Client infringes Applicable

Law.

Subprocessors

7. Suplexed may subcontract the collection or other Processing of Personal Data only in compliance with Applicable Law and any additional conditions for subcontracting set forth in the Terms. Prior to a Subprocessor's Processing of Personal Data, Suplexed will impose contractual obligations on the Subprocessor that are substantially the same as those imposed on Suplexed under this DPA. Upon written request from Client to Suplexed at support@suplexed.com, Suplexed will provide a current list of Subprocessors for the services Client obtains under the Terms. Suplexed remains responsible for its Subprocessors and liable for their performance under the Terms and this DPA. This paragraph constitutes Client's consent to both Suplexed's use of the Subprocessors and its subprocessing under the Standard Contractual Clauses, as applicable.

Security

8. Suplexed will assist Client in ensuring Client's compliance with the security obligations of the GDPR and other Applicable Law, as relevant to Suplexed's role in Processing the Personal Data, taking into account the nature of Processing and the information available to Suplexed, by complying with the following paragraph and, if available in the Services, by providing configurable security options.

9. To protect the Personal Data Suplexed shall implement appropriate technical and organizational measures that comply with Annex B, without prejudice to Suplexed's right to make future updates to the measures that do not lower the level of protection of Personal Data.

10. Client is solely responsible for reviewing the available security documentation and evaluating for itself whether the Services and related security will meet Client's needs, including Client's security obligations under Applicable Law. Client agrees that the security commitments in this DPA will provide a level of security appropriate to the risk in respect of the Personal Data.

11. Suplexed will ensure that the persons Suplexed authorizes to Process the Personal Data are subject to a written confidentiality agreement covering such data or are under an appropriate statutory obligation of confidentiality.

Personal Data Breach Notification

12. Suplexed will comply with the Personal Data Breach-related obligations directly applicable to it under the GDPR and other Applicable Law. Taking into account the nature of Processing and the information available to Suplexed, Suplexed will assist Client in complying with those obligations applicable to Client by informing Client of a confirmed Personal Data Breach without undue delay.

Assistance Responding to Data Subjects

13. Taking into account the nature of the Processing, Suplexed will assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Client's obligation to honor requests by individuals (or their representatives) to exercise their rights under the GDPR and other Applicable Law (such as rights to access their Personal Data).

Assistance with DPIAs and Consultation with Supervisory Authorities

14. Taking into account the nature of the Processing and the information available to Suplexed, Suplexed will provide reasonable assistance to and cooperation with Client for Client's performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving Suplexed and related consultation with supervisory authorities by providing Client with access to documentation for the Services. Additional support for data protection impact assessments or relations with regulators is available at Client expense and will require a statement of work and mutual agreement on fees, the scope of Suplexed's involvement, and any other terms that the parties deem appropriate.

Data Transfers

15. Client agrees and will ensure that Client and its affiliates are entitled to transfer the Personal Data to Suplexed so that Suplexed and its Subprocessors may lawfully Process the Personal Data in accordance with the Terms and this DPA.

16. Client authorizes Suplexed and its Subprocessors to make international transfers of the Personal Data in accordance with Applicable Law and this DPA.

17. The Standard Contractual Clauses attached hereto as Annex A form part of this DPA, and take precedence over the rest of this DPA to the extent of any conflict, with respect to Personal Data that is transferred outside the European Economic Area ("**EEA**"), either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data. The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA.

18. To the extent the Standard Contractual Clauses apply, Client shall be the "data exporter" and Suplexed shall be the "data importer."

Return or Destruction

19. Suplexed will, at the choice of Client, return to Client and/or destroy all Personal Data after the end of the provision of services relating to Processing except to the extent Applicable Law requires storage of the Personal Data.

20. Nothing will oblige Suplexed to delete Personal Data from files created for security, backup and business continuity purposes sooner than required by Suplexed's data retention processes. If Client requires earlier deletion of such Personal Data, and such deletion is commercially feasible, Client must first pay Suplexed's reasonable charges for such deletion, which may include costs for business interruptions associated with

such a request.

Audits

21. Suplexed will allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client, as follows:

    a. If the requested audit scope is addressed in an ISO or similar audit report issued by a third party auditor within the prior twelve (12) months and Suplexed provides such report to Client confirming there are no known material changes in the controls audited, Client agrees to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

    b. In the event an audit report is not provided, any audit, whether by Client or a third party, must be limited to no more than once per twelve (12) month period, and Client will (i) conduct the audit only on an agreed date during normal business hours (9:00 am - 5:00 pm local time); (ii) limit its audit to only one business day; and (iii) pay Suplexed's then-current audit fee.

    c. If a third party is to conduct the audit, Client will provide at least thirty (30) days' advance notice. The third-party auditor must be mutually agreed to by the parties (without prejudice to any governmental authority's audit power). Suplexed will not unreasonably withhold its consent to a third-party auditor requested by Client, unless such third-party auditor is a competitor or another customer of Suplexed's Any third-party auditor must execute a written confidentiality agreement acceptable to Suplexed.

    d. Client must promptly provide Suplexed with the results of any audit, including any third-party audit report. All such results and reports, and any other information obtained during the audit (other than Client's Personal Data) is confidential information of Suplexed.

    e. Nothing herein will require Suplexed to disclose or make available:

        i. any data of any other customer of Suplexed;

        ii. Suplexed's internal accounting or financial information;

        iii. any trade secret of Suplexed;

        iv. any information that, in Suplexed's reasonable opinion, could (i) compromise the security of Suplexed systems or premises; or (ii) cause Suplexed to breach its obligations under Applicable Law or its security and/or privacy obligations to Client or any third party; or

        v. any information sought for any reason other than the good faith fulfilment of Client's obligations under the Standard Contractual Clauses or Applicable Law.

22. In addition, to the extent required by Applicable Law, including where mandated by Client's Supervisory Authority, Client or Client's Supervisory Authority may perform, at Client's expense, a broader audit, including inspections of the data center facility that Processes Personal Data. Suplexed will contribute to such audits by providing Client or Client's Supervisory Authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Services.

23. Client must provide Suplexed with any audit reports generated in connection with this DPA, unless prohibited by Applicable Law. Client may use the audit reports only for the purposes of meeting Client's regulatory audit requirements and/or confirming compliance with the terms of this DPA.

24. Client agrees that any audit conducted in accordance with Sections 21-23 above satisfies Suplexed's audit obligations under Clause 5 of the Standard Contractual Clauses.

Annex A

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;

Client (as a "data exporter" and as defined in the Data Processing Addendum to which this Annex A is annexed) and Suplexed LLC (as a "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;

(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 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[1]

[1] 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

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:

(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;

---

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.

(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[2]. 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.

---

[2] 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.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. By signing the Clauses, the parties also are signing this Appendix 1. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly activities relevant to the transfer):

The data exporter is the entity identified as "Client" in the DPA.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

The data importer is Suplexed, which is a provider of information and data management services.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The categories of data subjects are set forth in Section 5 of the DPA.

Categories of data

The personal data transferred concern the following categories of data (please specify):

The categories of personal data are set forth in Section 5 of the DPA.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Not applicable.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing operations are set forth in Section 5 of the DPA.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. By signing the Clauses, the parties also are signing this Appendix 2.

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):

See Annex B to the DPA, below.

Annex B

1. Suplexed has agreed to employ appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data ("Information Security Program").

2. Suplexed's Information Security Program includes specific security requirements for its personnel and all subcontractors or agents who have access to Client Personal Data ("Data Personnel"). Suplexed's security requirements covers the following areas:

    a. Information Security Policies and Standards. Suplexed will maintain information security policies, standards and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Client Personal Data. These policies, standards, and procedures shall be designed and implemented to:

        i. Prevent unauthorized persons from gaining physical access to Client Personal Data Processing systems (e.g. physical access controls);

        ii. Prevent Client Personal Data Processing systems from being used without authorization (e.g. logical access control);

        iii. Ensure that Data Personnel gain access only to such Client Personal Data as they are entitled to access (e.g. in accordance with their access rights) and that, in the course of Processing or use and after storage, Client Personal Data cannot be read, copied, modified or deleted without authorization (e.g. data access controls);

        iv. Ensure that Client Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the recipients of any transfer of Client Personal Data by means of data transmission facilities can be established and verified (e.g. data transfer controls); and

        v. Ensure that all systems that Process Client Personal Data are the subject of a vulnerability management program that includes without limitation internal and external vulnerability scanning with risk rating findings and formal remediation plans to address any identified vulnerabilities.

    b. Physical Security. Suplexed will maintain commercially reasonable security systems at all Suplexed sites at which an information system that uses or stores Client Personal Data is located ("Processing Locations") and will reasonably restrict access to such Processing Locations.

    c. Organizational Security. Suplexed will maintain information security policies and procedures addressing:

i. Data Disposal. Procedures for when media are to be disposed or reused have been implemented to prevent any subsequent retrieval of any Client Personal Data stored on media before they are withdrawn from the Suplexed's inventory or control.

ii. Data Minimization. Procedures for when media are to leave the premises at which the files are located as a result of maintenance operations have been implemented to prevent undue retrieval of Client Personal Data stored on media.

iii. Data Classification. Policies and procedures to classify sensitive information assets, clarify security responsibilities, and promote awareness for all employees have been implemented and are maintained.

iv. Incident Response. All Client Personal Data security incidents are managed in accordance with appropriate incident response procedures.

d. Network Security. Suplexed maintains commercially reasonable information security policies and procedures addressing network security.

e. Access Control (Governance).

i. Suplexed governs access to information systems that Process Client Personal Data.

ii. Only authorized Suplexed staff can grant, modify or revoke access to an information system that Processes Client Personal Data.

iii. Suplexed implements commercially reasonable physical and technical safeguards to create and protect passwords.

f. Virus and Malware Controls. Suplexed protects Client Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Client Personal Data.

g. Personnel.

i. Suplexed has implemented and maintains a security awareness program to train all employees about their security obligations. This program includes training about data classification obligations, physical security controls, security practices, and security incident reporting.

ii. Data Personnel strictly follow established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.

iii. Suplexed shall take reasonable steps to ensure the reliability of any

employee, agent or contractor who may Process Client Personal Data.

h. Business Continuity. Suplexed implements disaster recovery and business resumption plans. Business continuity plans are tested and updated regularly to ensure that they are up to date and effective.