



36 Crafts Street, Newton, MA 02458
TEL: 617.965.4500 FAX: 617.965.4551
www.freshaddress.com

Data Processing Addendum (GDPR and Standard Contractual Clauses) (Revised October 2019)

This Data Processing Addendum (“DPA”) supplements the Email List Services Agreement or other Agreement (the “Agreement”) between FreshAddress, LLC (successor in interest to FreshAddress, Inc.) (VENDOR) and CUSTOMER (together, the “Parties”) to reflect the parties’ agreement with regard to the Processing of Personal Data. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer and, where applicable, to Customer’s Affiliates pursuant to the Agreement, Vendor may Process Personal Data on behalf of Customer. Vendor agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Services and Processed by or for Vendor using the Services.

By signing to the Agreement, Customer enters into this DPA on its own behalf and on behalf of its Affiliates, if and to the extent Vendor Processes Personal Data for which such Affiliates qualify as Controller.

In consideration of the Parties’ mutual rights and obligations set out in the Agreement and this DPA, the Parties agree as follows:

1. DEFINITIONS

- 1.1. **“Affiliate”** shall mean, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity.
- 1.2. **“GDPR”** means the EU General Data Protection Regulation ((EU) 2016/679)) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- 1.3. **“Controller”** shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.
- 1.4. **“Customer Personal Information”** shall mean the Personal Data which Vendor is Processing as Processor on behalf of Customer in order to provide the Services.
- 1.5. **“Data Protection Laws”** shall mean all data protection and privacy laws applicable to the respective party in its role in the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.
- 1.6. **“EU Data Protection Law”** shall mean (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of

personal data and on the free movement of such data (“Directive”), (ii) on or after 25 May 2018, the GDPR, and any equivalent or replacement law in any Member State and all and any regulations made under those acts or regulations; (iii) the guidelines, recommendations, best practice opinions, directions, decisions, and codes of conduct issued, adopted or approved by the European Commission, the European Data Protection Board, and/or any supervisory authority or data protection authority from time to time in relation to the Directive or the GDPR; and (iii) any judgments of any relevant court of law relating to the processing of personal data, data privacy, and data security.

- 1.7. **“EU Standard Contractual Clauses”** shall mean the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries set forth in the Commission Decision 2010/87/EC of 5 February 2010, as well as under any new laws, rules, regulations, and/or contracts that that replace, supersede, or are required to be implemented in connection with the Standard Contractual Clauses.
- 1.8. **“Member State”** shall mean a country that is a member of the European Union or of the European Economic Area.
- 1.9. **“Personal Data”** shall mean any information relating to an identified or identifiable natural person (“Data Subject”), which information is subject to Data Protection Legislation; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier such as an IP or MAC Address or Mobile ID, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 1.10. **“Personal Data Breach”** shall mean a suspected or actual breach of the Vendor Security Standards leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
- 1.11. **“Process”** or **“Processing”** shall mean the collection, recording, organization, alteration, use, access, disclosure, copying, transfer, storage, deletion, combination, destruction, disposal or other use of Personal Data by the Processor on behalf of Customer.
- 1.12. **“Processor”** shall mean a natural or legal person, public authority, agency or other body which processes Personal Information on behalf of the Controller.
- 1.13. **“Services”** shall mean the services provided by Vendor as described in the Agreement.
- 1.14. **“Sub-processor”** means any subcontractor engaged by Vendor for the Processing of Customer Personal Data in accordance with Section 8.1.
- 1.15. **“Supervisory Authority”** shall mean an independent public authority which is established by a Member State pursuant to Data Protection Legislation.
- 1.16. **“Transfer”** shall mean the access by, transfer or delivery to, or disclosure of Personal Data to a person, entity or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.
- 1.17. **“Vendor Security Standards”** means the security standards attached to the Agreement, of in none are attached to the Agreement, attached to this Addendum as Annex 1.

2. DATA PROCESSING

- 2.1** This DPA applies if and to the extent Vendor is Processing Customer Personal Information. In this context, Vendor will act as a “Processor” to the Customer, who will act as “Controller” with respect to Customer Personal Data.
- 2.2** Annex 3 (Processing Details) sets out:
- (a) the nature, purposes, and subject matter of the Processing;
 - (b) the duration of the Processing;
 - (c) the categories of Data Subjects; and
 - (d) the types of Customer Personal Data.
- 2.3** Vendor will Process Customer’s Personal Data for the sole purpose of providing the Services according to Customer’s written instructions. The Parties agree that the Agreement and this DPA constitute Customer’s complete and final documented instructions to Vendor in relation to the Processing of Personal Data. Additional instructions outside the scope of the Agreement or this DPA (if any) require prior written agreement between Vendor and Customer, including agreement on any additional fees payable by Customer for carrying out such instructions. Customer shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to Customer’s Personal Data, and that the Processing of Customer’s Personal Data in accordance with Customer’s instructions will not cause Vendor to be in breach of the GDPR.
- 2.4** Vendor will not access or use Customer’s Personal Data, except as necessary to maintain or provide the Services, or as necessary to comply with the law or a binding order of a governmental body.
- 2.5** Customer agrees that (i) it will comply with its obligations under Data Protection Laws in respect of its Processing of Customer’s Personal Data, including any obligations specific to its role as a Controller and/or Processor (as applicable); and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Data Protection Laws for Vendor to Process Customer’s Personal Data and provide the Services pursuant to the Agreement and this DPA. If Customer is itself a Processor, Customer warrants to Vendor that Customer’s instructions and actions with respect to that Customer Personal Data, including its appointment of Vendor as another Processor, have been authorized by the relevant Controller.

3. TECHNICAL AND ORGANIZATIONAL MEASURES

- 3.1.** Vendor will implement and maintain technical and organizational measures to ensure a level of security appropriate to the risk as set out in Annex 1.
- 3.2.** Customer is responsible for reviewing the information made available by Vendor relating to data security and making an independent determination as to whether the technical and organizational measures implemented by Vendor meet Customer’s requirements and legal obligations under GDPR. Customer acknowledges that the Vendor Security Standards are subject to technical progress and further development and that Vendor may update or modify the Vendor Security Standards from time to time provided that such updates and modifications do not result in a material degradation of the overall security of the Services provided to Customer under the Agreement.

- 3.3.** Customer agrees that, without prejudice to Vendor's obligations under Section 3.1: (a) Customer is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Customer's Personal Data, securing its account authentication credentials, managing its data back-up strategies, and protecting the security of Customer's Personal Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer's Personal Data uploaded to the Services; and (b) Vendor has no obligation to protect Customer's Personal Data that Customer elects to store or transfer outside of Vendor's and its Sub-processors' systems (for example, offline or on premise storage).

4. DATA SUBJECT RIGHTS AND REQUESTS

- 4.1** Vendor shall rectify, erase, allow the portability of or otherwise Process Customer's Personal Data and take any other measures in relation to requests from Data Subjects in relation to their rights under applicable EU Data Protection Law only in accordance with and subject to Customer's written instructions.
- 4.2** To the extent permitted by applicable Data Protection Legislation, Vendor will inform Customer without undue delay of requests from Data Subjects exercising their rights thereunder that are addressed directly to Vendor regarding Customer's Personal Data. If Customer is obliged to provide information regarding Customer's Personal Data to third parties (e.g., Data Subjects or any Supervisory Authority), Vendor shall use best efforts to assist Customer in doing so by providing all required information.
- 4.3** Customer agrees that, without prejudice to Vendor's obligations under Sections 4.1 and 4.2 above, Customer is solely responsible for dealing with Data Subject requests.
- 4.4** If a law enforcement agency sends Vendor a demand for Customer's Personal Data (e.g., a subpoena or court order), Vendor will redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Vendor may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer's Personal Data to a law enforcement agency, then Vendor will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Vendor is legally permitted to do so.
- 4.5** Customer acknowledges that Vendor is required under the GDPR to: (a) collect and maintain written records of certain information, including the name and contact details of each Processor and/or Controller on behalf of which Vendor is acting and, where applicable, of such Processor's or Controller's local representative and data protection officer. and (b) make such information available to the Supervisory Authorities. Accordingly, if GDPR applies to the Processing of Customer's Personal Data, Customer will, where requested, provide such information to Vendor via the Services or other means provided by Vendor, and will ensure that all information provided is kept accurate and up-to-date.

5. CONFIDENTIALITY

- 5.1** Without prejudice to any existing contractual arrangements between the Parties, Vendor shall treat all Customers' Personal Data as strictly confidential and shall inform all its employees, agents and/or approved Sub-processors engaged in Processing the Customer's Personal Data of

the confidential nature of the data. Vendor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

- 5.2 Vendor will not disclose Customer's Personal Data to any third party, unless authorized by Customer or required by mandatory law. If a government or Supervisory Authority demands access to Customer's Personal Data, Vendor will notify Customer prior to disclosure unless prohibited by law.

6. INFORMATION AND AUDIT

- 6.1 Customer acknowledges that Vendor is regularly audited by independent third-party auditors and/or internal auditors against the standards specified in the Vendor Security Standards, as described in Annex 1. Upon request, Vendor shall supply (on a confidential basis) a summary copy of its audit report(s) to Customer, so that Customer can verify Vendor's compliance with the audit standards against which it has been assessed, and this DPA. If the Agreement does not include a provision protecting Vendor's confidential information, then any audit report(s) will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering those reports.
- 6.2 Vendor shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer's Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Vendor's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.
- 6.3 Customer agrees to exercise any right it may have to conduct an audit or inspection of Vendor's technical and organization measures, including under the EU Standard Contractual Clauses if they apply, by instructing Vendor to carry out such audit.

7. RETURNING OR DELETING CUSTOMER'S PERSONAL DATA

- 7.1 Upon termination or expiration of the Agreement, or anytime upon Customer's written request, Vendor shall promptly return or delete all copies of Customer's Personal Data. Vendor shall not be required to return or delete Customer's Personal Data to the extent (i) Vendor is required by applicable law or order of a governmental or regulatory body to retain all or some of Customer's Personal Data, or (ii) Customer has not paid all amounts due under the Agreement.

8. SUB-PROCESSORS

- 8.1 Customer agrees that Vendor may engage Sub-processors to Process Customer's Personal Data on Customer's behalf. Customer hereby consents to Vendor continuing to use any of Vendor's Affiliates and all Sub-processors already engaged by Vendor as at the date of this DPA (a full list is available on request [by contacting the Vendor's data privacy manager]). Customer shall promptly take any reasonable action required or appropriate to facilitate or support any transfer of Customer's Personal Data to approved Sub-processors (e.g. updating registrations with Supervisory Authorities).
- 8.2 Vendor shall notify Customer of any new Sub-processor Vendor wishes to appoint to carry out Processing activities on behalf of Customer. If, within two (2) weeks of receipt of any such notice, Customer notifies Vendor in writing of any objections to the proposed appointment

for legitimate reasons, Vendor shall work with Customer in good faith to take reasonable measures to address the objections raised by Customer, and where such measures cannot be agreed within three (3) weeks from Vendor's receipt of Customer's notice, Customer may by written notice to vendor with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor. "Legitimate reasons" shall be deemed given if there is an indication based on objective facts which reasonably support the assumption that the engagement of the Sub-processor would breach applicable law or this DPA.

- 8.3** Where Vendor engages a Sub-processor to carry out specific Processing activities on behalf of Customer, Vendor shall enter into a written agreement with the Sub-processor which includes terms which offer the same level of protection for Customer's Personal Data as those set out in this DPA.
- 8.4** Notwithstanding any approval by Customer within the meaning of Section 8.1, Vendor shall remain fully liable vis-à-vis Customer for the performance of any such Sub-processor that fails to fulfil its data protection obligations under this DPA and/or any applicable Data Protection Laws.

9. TRANSFERS of PERSONAL INFORMATION

- 9.1.** To the extent that Vendor Processes any Customer's Personal Data in a country that is neither a Member State nor considered by the European Commission to have adequate level of protection for personal information, Vendor will (i) enter into EU Standard Contractual Clauses with Customer (see Annex 2),
- 9.2.** To the extent that Customer or Vendor are relying on a specific statutory mechanism to normalize international Personal Data Transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, Customer and Vendor agree to cooperate in good faith to promptly terminate the Transfer or to pursue a suitable alternative mechanism that can lawfully support the transfer.
- 9.3.** For the purposes of Section 9.2, Vendor and Customer agree that incorporation of the EU Standard Contractual Clauses into this DPA shall act as a legally-binding execution.

10. INFORMATION OBLIGATIONS AND PERSONAL DATA BREACH

- 10.1** If Vendor becomes aware of a Personal Data Breach that impacts the Processing of the Customer's Personal Data that is the subject of the Agreement and is reasonably likely to require a data breach notification by Customer under the GDPR, Vendor will without undue delay: (a) notify Customer of the Personal Data Breach; and (b) take reasonable steps to minimize any damage resulting from the Personal Data Breach.
- 10.2** To assist Customer in relation to any Personal Data Breach notifications Customer is required to make under the GDPR, Vendor will include in the notification under Section 10.1(a) such information about the Personal Data Breach as Vendor is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Vendor, and any restrictions on disclosing the information, such as confidentiality.

10.3 Customer agrees that:

- (a) An unsuccessful Personal Data Breach will not be subject to this Section 10. An unsuccessful Personal Data Breach is one that results in no unauthorized access to Customer's Personal Data or to any of Vendor's equipment or facilities storing Customer's Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and
- (b) Vendor's obligation to report or respond to a Personal Data Breach under this Section 10 is not and will not be construed as an acknowledgment by Vendor of any fault or liability of Vendor with respect to the Personal Data Breach.

10.4 Notification of Personal Data Breaches, if any, will be delivered to one or more of Customer's administrators by any means Vendor selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on Vendor's systems, and secure transmission at all times.

10.5 Customer acknowledges that Vendor will not assess the contents of Customer's Personal Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with the data breach notification obligations applicable to Customer under the GDPR and fulfilling any third-party notification obligations related to any Personal Data Breach.

11. LIABILITY

11.1 The liability of each Party under this Addendum shall be subject to the exclusions and limitations of liability set out in the Agreement. Customer agrees that any regulatory penalties incurred by Vendor in relation to the Customer's Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this Addendum and the GDPR shall count towards and reduce Vendor's liability under the Agreement as if it were liability to Customer under the Agreement.

12. GENERAL

12.1 If any provision of this DPA is ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith.

12.2 In the event of any inconsistency between the provisions of this DPA and the provisions of the Agreement, the provisions of this Agreement shall prevail.

12.3 This DPA will be governed and construed in accordance with the governing law and applicable jurisdiction provisions of the Agreement, unless required by applicable Data Protection Law.

Except as otherwise detailed herein, the terms and conditions of the Agreement shall remain unchanged and in full force and effect.

The Effective Date of this DPA is May 25, 2018

FreshAddress, LLC

CUSTOMER

Craig Marcellus

(Authorized Signature)

(Authorized Signature)

Craig Marcellus

(Name)

(Name)

Director of Data Systems and Security

(Title)

(Title)

July 25, 2018

(Date)

(Date)

Please your signed DPA to security@freshaddress.com or fax to the number above.

Annex 1 Vendor Security Standards

Notwithstanding any additional measures agreed to in the Agreement, Vendor ensures that at least the following technical and organizational measures are ensured:

- 1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)**
 - Physical Access Control

No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems

- **Electronic Access Control**

No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media

- **Internal Access Control (permissions for user rights of access to and amendment of data)**

No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events

- **Isolation Control**

The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing

- **Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)**

The processing of personal data in such a method/way, that the data cannot be associated with a specific data subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- **Data Transfer Control**

No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature

- **Data Entry Control**

Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- **Availability Control**

Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning

- **Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR)**

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- **Data Protection Management**

- **Incident Response Management**

- **Data Protection by Design and Default (Article 25 Paragraph 2 GDPR)**

- Order or Contract Control
No third party data processing as per Article 28 GDPR without corresponding instructions from the Controller, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

Annex 2 – EU Standard Contractual Clauses



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:

Address:

(the data **exporter**)

And

Name of the data importing organisation: FreshAddress, LLC

e-mail contact: cmarcellus@freshaddress.com

(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 data¹;
- (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

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;
 - (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 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

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 Clauses². 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.

On behalf of the data exporter:

Name :

Position:

Email Address:

Signature.....

On behalf of the data importer:

Name: Craig Marcellus

Position: Director of Data Systems and Security

Email Address: cmarcellus@freshaddress.com

Signature...*Craig Marcellus*.....

Annex 3 – Processing Details

1. Nature, purpose and subject matter of the Processing

-
The type and purpose of processing is for performance of the email validation and data quality services as defined in the Service Agreement

2. Duration of the Processing

- This DPA will be in place for the duration of our agreement and beyond.

3. Categories of Data Subjects

All data processed under this agreement is considered Personal Data.

4. Types of Customer's Personal Data

Email Addresses

5. Special Categories of Personal Data

N/A