Data Protection Addendum
(Updated 24 January 2024)

Parties to this DPA

This Fresh Relevance Data Protection Addendum ("**DPA**") is between Fresh Relevance (the "**Company**" or "**Processor**") and the Customer entity which uses Fresh Relevance (either a customer of Fresh Relevance or a customer of a Fresh Relevance reseller) (the "**Customer**" or "**Controller**").

The Customer may have an applicable agreement with Fresh Relevance (Customer Terms, Reseller Agreement, or other agreement entered into between Customer and Fresh Relevance) and any associated Order Forms (collectively the "**Agreement**").

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

"CCPA"	means the California Consumer Privacy Act of 2018, along with its regulations and as amended from time to time;
"Data Protection Law"	means: (i) for Services supplied by Fresh Relevance Limited, the EU GDPR, the Data Protection Act 2018, the UK GDPR, the FDPA, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and/or any corresponding or equivalent national laws or regulations; (ii) for Services supplied by Fresh Relevance, Inc., all state and federal legislation applicable to the processing of Personal Data as contemplated under the Agreement, including but not limited to, the CCPA; (iii) specifically in relation to the Customer, all data protection and/or privacy laws in which recipient Data Subjects are contacted through the Services are located; (iv) any applicable laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;
"Data Protection Losses"	means: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; and/or (ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject;
"Data Subject"	shall have the same meaning as in Data Protection Law or means a "Consumer" as that term is defined in the CCPA;
"DPA"	means this data processing agreement together with Exhibits A and B;
"EEA"	means the European Economic Area;
"EU GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, (General Data Protection Regulation);
"FDPA"	means the Revised Swiss Federal Act on Data Protection of 25 September 2020;
"Personal Data"	shall have the same meaning as in Data Protection Law;
"Processor"	means the Company, including as applicable any "Service Provider" as that term is defined by the CCPA;

"Restricted Transfer"	means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;
"Services"	means all services and software applications and solutions provided to the Controller by the Processor under and as described in the Agreement;
"SCCs"	means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR published at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf which is an addendum to the EU SCCs in (i); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; ("**Swiss SCCs**");
"Sub-processor"	means any third party (including Processor Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services to the Controller;
"Supervisory Authority"	means a governmental or government chartered regulatory body having binding legal authority over a party;
"UK GDPR"	shall have the meaning as defined in section 3(1) of the Data Protection Act 2018 (supplemented by section 205(4)).

2. Purpose

2.1 In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

3.1 In providing the Services to the Controller, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Controller's instructions documented in the Agreement and this DPA, and any other written instructions provided by the Controller and acknowledged by the Processor as being instructions for the purposes of this DPA, as updated from time to time ("**Processing Instructions**").

3.2 The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to Personal Data does not process them except as provided by this DPA and any Data Protection Law.

4. Processor Obligations

4.1 Unless required to do otherwise by Data Protection Laws, the Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the Processing Instructions. If the Data Protection Laws requires the Processor to process Personal Data other than in accordance with the Processing Instructions, it shall notify the Controller of any such requirement before processing the Personal Data (unless the Data Protection Laws prohibit such information on important grounds of public interest).

4.2 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the Processing Instructions regarding the processing of Personal Data provided by the Controller, breach any Data Protection Law. To the maximum extent permitted by mandatory law, the Processor shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities arising from or in connection with any processing in accordance with the Controller's Processing Instructions following the Controller's receipt of that information.

4.3 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; and (ii) have received appropriate training on their responsibilities as a data processor.

4.4 The Processor shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. These measures are outlined in Exhibit B.

4.5 The Controller acknowledges and agrees that, in the course of providing the Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Services. All such access by the Processor will be limited to those purposes.

4.6 Taking into account the nature of the processing and the information available to the Processor, the Processor shall reasonably assist the Controller with the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data with respect to: (i) security of processing; (ii) data protection impact assessments (as such term is defined in Data Protection Laws); (iii) prior consultation with a Supervisory Authority regarding high risk processing; and (iv) notifications to the Supervisory Authority and/or communications to Data Subjects by the Controller in response to any Personal Data Breach.

4.7 The Processor confirms that it and/or its Affiliate(s) have appointed a data protection officer where such appointment is required by Data Protection Law. The appointed data protection officer may be contacted by email at: GDPR@FreshRelevance.com or Privacy@dotdigital.com.

4.8 The Processor may not: (i) "sell" Personal Data (as that term is defined under the CCPA); (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement.

5. Controller Obligations

5.1 The Controller represents and warrants that: (i) it shall comply with this DPA and its obligations under Data Protection Law in connection with the processing of Personal Data, use of the Services and the exercise and performance of its respective rights and obligations under this DPA, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; (ii) it has obtained any, and all, necessary permissions and authorisations necessary to permit the Processor, its Affiliates and Sub-processors, to execute their rights or perform their obligations under this DPA; (iii) all Affiliates of the

Controller who use the Services shall comply with the obligations of the Controller set out in this DPA; (iv) all data sourced by the Controller for use in connection with the Services shall comply in all respects, including in terms of its collection, storage and processing (which shall include the Controller providing all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws; and (v) all instructions given by the Controller to the Processor in respect of Personal Data shall at all times be in accordance with Data Protection Laws.

5.2 The Controller shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5.3 The Controller shall not unreasonably withhold, delay or condition its agreement to any change or amendment requested by the Processor in order to ensure the Services and the Controller (and each Sub-Processor) can comply with Data Protection Laws.

5.4 The Controller acknowledges and agrees that some instructions from the Controller including the Processor assisting with audits, inspections or providing any assistance under this DPA, may result in additional fees. In such case the Processor shall notify the Controller of its fees for providing such assistance in advance and shall be entitled to charge the Controller for its reasonable costs and expenses in providing such assistance, unless agreed otherwise in writing.

6. Sub-processors

6.1 The Controller acknowledges and agrees that: (i) Affiliates of the Processor may be used as Sub-processors; and (ii) the Processor and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services.

6.2 The Controller authorises the Processor to use the Sub-processors at https://www.freshrelevance.com/legal/third-party-sub-processor/ to process the Personal Data. During the term of this DPA, the Processor shall provide the Controller with 30 days prior notification, via email, of any changes to the list of Sub-processors before authorising any new or replacement Sub-processor to process Personal Data in connection with provision of the Services.

6.3 The Controller may object (on reasonable grounds and only relating to data protection) to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within fourteen (14) days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-processor: (i) the Processor shall work with the Controller in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-Processor; (ii) Where such a change cannot be made within 14 days of the Processor's receipt of the Controller's notice, the Controller may by written notice to the Processor, with immediate effect terminate the Agreement with respect to those Services which cannot be provided by the Processor without the use of the new or replacement Sub-processor. This termination right is Client's sole and exclusive remedy to Client's objection of any Sub-Processor appointed by the Processor during the Term.

6.4 The Processor shall ensure (i) via a written contract that the Sub-Processor only accesses and processes Personal Data to perform the obligations subcontracted to it and does so in

accordance with the measures contained in this DPA, and (ii) remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

6.5 The Controller agrees that the Processor and its Sub-processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement. The Processor confirms that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or (ii) have entered into the applicable SCCs with the Processor; or (iii) have other recognised appropriate safeguards in place.

7. Restricted Transfers

7.1 The parties agree that, when the transfer of Personal Data from the Controller to the Processor or from the Processor to a Sub-processor is a Restricted Transfer, it shall be subject to the applicable SCCs.

7.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

(i) Module Three (Processor to Processor) shall apply where the Company is a Processor of Customer Data and the Company uses a Sub-processor to process the Customer Data;

(ii) Module Four (Processor to Controller) shall apply where Personal Data is transferred from the Company to the Controller which processes it;

(iii) In Clause 7 of the EU SCCs, the optional docking clause will not apply;

(iv) In Clause 9 of the EU SCCs Option 2 applies, and the time period for giving notice of Sub-processor changes shall be as set out in clause 6.3 of this DPA;

(v) In Clause 11 of the EU SCCs, the optional language shall not apply;

(vi) In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by the laws of Netherlands;

(vii) In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Netherlands;

(viii) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A of this DPA;

(ix) Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B of this DPA.

7.3 The parties agree that the EU SCCs as amended in clause 7.2 above, shall be adjusted as set out below where the FDPA applies to any Restricted Transfer:

(i) The Swiss Federal Data Protection and Information Commissioner (“FDPIC”) shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FDPA;

(ii) Restricted Transfers subject to both the FDPA and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Exhibit A of this DPA;

(iii) The term ’member state’ must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;

(iv) Where Restricted Transfers are exclusively subject to the FDPA, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA;

(v) Where Restricted Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA insofar as the Restricted Transfers are subject to the FDPA;

(vi) The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the revised FDPA.

7.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), completed as follows:

(i) Appendix 1 of the UK SCCs shall be deemed completed with the information set out in Exhibit A of this DPA; and

(ii) Appendix 2 of the UK SCCs shall be deemed completed with the information set out in Exhibit B of this DPA.

7.5 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.

8. Data Subject Access Requests

8.1 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Controller acknowledges and agrees that the Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

8.2 If the Processor receives a request from a Data Subject to invoke their rights under Applicable Data Protection Law, including access to, or deletion of that person's Personal Data, the Processor shall (a) refer such request to the Controller within three (3) Business Days of receipt of such request, (b) provide the Controller with reasonable co-operation and assistance taking in to account the nature of the Services and ability of the Controller to comply with its obligations towards Data Subjects directly, and (c) not disclose the Personal Data to any Data Subject or to a third party other than at the request of the Controller provided that the Processor shall be authorised to communicated with the Data Subject to acknowledge receipt of the request and provide progress updates as may be necessary. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable. Further to the above and notwithstanding anything to the contrary in the Agreement, the Processor reserves the right to disclose the identity of the Controller to any relevant Data Subject following any such request from a Data Subject.

9. Records, Information and Audit

9.1 The Processor shall maintain, in accordance with Data Protection Laws binding on the Processor, written records of all categories of processing activities carried out on behalf of the Controller.

9.2 The Processor shall, in accordance with Data Protection Laws, make available to the Controller such information as is reasonably necessary to demonstrate the Processor's compliance with the obligations of data processors under Data Protection Laws, and allow for and contribute to audits, including inspections, by the Controller (or another auditor mandated by the Controller) for this purpose, subject to the Controller: (i) Giving the Processor reasonable prior notice of such information request, audit and/or inspection being required by the Controller; (ii) Ensuring that all information obtained or generated by the Controller or its auditor(s) in connection with such information requests, inspections and audits are kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Data Protection Laws); (iii) Ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to the Processor's business and the business of other customers of the Controller; and (iv) Paying the Processor reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits on-site, calculated on a time & materials basis.

10. Personal Data Breach

10.1 The Processor will notify the Controller of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Controller Personal Data in the Processor's possession or under its control (a "Security Breach") within 24 hours of the Processor's confirmation of the nature and extent of the same or when required by applicable law, whichever is earlier and The Processor will take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Breach.

10.2 The Processor and the Controller will reasonably cooperate with each other with respect to the investigation and resolution of any Security Breach including, in the case of the Processor, within a reasonably practicable timeframe, the provision of the following, to the extent then known to The Processor (i) the possible cause and consequences of the Security Breach; (ii) the categories of the Controller Personal Data involved; (iii) a summary of the possible consequences for the affected Data Subjects (iv) a summary of the unauthorised recipients of the Controller Personal Data; and (v) the measures taken by The Processor to mitigate any damage.

11. Compliance, Cooperation and Response

11.1 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.

11.2 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

11.3 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

12. Liability

12.1 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set out in the Agreement.

12.2 Notwithstanding the foregoing, the limitations specified in clause 12.1 above shall not apply to Data Protection Losses. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

12.3 Any Data Protection Losses incurred by one party arising from or in connection with the other's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall be considered a liability to the non-compliant party.

13. Term and Termination

13.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

14. Deletion and Return of Personal Data

14.1 The Processor shall at the Controller's written request, delete or provide facilities for the Client to either delete, or return all the Personal Data to the Controller in such form as the Controller reasonably requests within a reasonable time after the earlier of: (i) the end of the provision of the relevant Services related to processing; or (ii) once processing by the Controller of any Personal Data is no longer required for the purpose of the Processor's performance of its relevant obligations under the Agreement, and delete existing copies (unless storage of any data is required by Data Protection Law or applicable law and, if so, the Processor shall inform the Controller of any such requirement).

15. Government Requests

15.1 The Processor does not, as a matter of course, voluntarily supply government authorities, agencies or law enforcement access to or information relating to Fresh Relevance accounts or Personal Data. If the Processor receives a compulsory request (whether via court order, warrant, or other valid legal process) from any government authority, agency or law enforcement for access to or information relating to a customer account (including Personal Data) belonging to a customer (hereafter, a "**Government Request**"), the Processor shall take all such reasonable steps as necessary to confirm the validity of such a request.

15.2 In the event that the Processor satisfies itself that a Government Request is valid, the Processor shall: (i) inform the government authority, agency or law enforcement that the Processor is a processor of the Personal Data; (ii) attempt to redirect the government

authority, agency or law enforcement to request the data directly from the Controller; and (iii) notify the Controller via email of the Government Request to allow the Controller to seek their own appropriate remedy, whereby the Processor may provide the Controller's contact information.

15.3 The Processor shall not be required to comply with the provisions of clauses 15.1 or 15.2 above if: (i) the Controller is legally prohibited from doing so; or (ii) the Controller has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, the safety of the public, or the Processor's Services or property.

Exhibit A

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

MODULE TWO: CONTROLLER TO PROCESSOR

A. LIST OF PARTIES

The Data Exporter: is the Company.

The Data Importers: are the Sub-processors named in the Sub-processor list which contains the name, address, contact details and activities relevant to the data transferred to each Data Importer.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of Data Subjects:	In outline, users of the Controller's website and people subscribed to receive the Controller's emails. They may be the following… Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons). Users, Affiliates and other participants authorised by the Controller to access or use the Services in accordance with the terms of the Agreement. Prospects, customers, clients, business partners and vendors of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media. Employees or contact persons of Controller's prospects, customers, clients, business partners and vendors. Suppliers and service providers of the Controller. Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.
Categories of Personal Data:	In outline, data about users of the Controller's website and people subscribed to receive the Controller's emails, including personal details, what they did, and what happened to them… The Personal Data may include the following: • Personal details, names, email addresses, personal addresses. • Unique identifiers such as username, account number or password. • Personal Data derived from a user's use of the Services such as what pages they have seen and what products they have seen, carted, or purchased. • Personal Data within email and messaging content which identifies or may reasonably be used to identify, Data Subjects. • Meta data including sent, to, from, date, time, subject, which

	may include Personal Data. • location based upon IP address, but not IP address. • Information about preferences, such as categories of favourite categories of products. • Purchases made.
Sensitive Data: (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the Sensitive Data, restrictions for onward transfers or additional security measures:	No sensitive data is stored unless this is specifically requested by the Controller. Sensitive data will correspond to the business category of the Controller - for example if they sell medicines then data might include information about shopping behaviour that might allow a data subject's medical condition to be guessed.
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	Processing operations include but are not limited to personalisation and triggering so that Data Subjects see marketing that is tailored to them.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Unless agreed otherwise in writing, for the duration of the Agreement, subject to clause 14 of the DPA.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-processor list accessed via "GDPR Data Processing Addendum: Approved Sub-processors" on https://www.freshrelevance.com/legal/legal-documents sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent	Where the EU GDPR applies, the Netherlands Data Protection

supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Authority (Data Protection Commission). Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

MODULE THREE: PROCESSOR TO PROCESSOR

A. LIST OF PARTIES

The Data Exporter: is the Company.

The Data Importer: is the Controller.

This is only relevant when the Controller is based in a third country. In this case it applies for scenarios including when Personal Data is exported from the Company for (a) backup by the Controller, or (b) subsequent use by a third-party processor chosen by the Controller.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of Data Subjects:	In outline, users of the Controller's website and people subscribed to receive the Controller's emails. They may be the following… Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons). Users, Affiliates and other participants authorised by the Controller to access or use the Services in accordance with the terms of the Agreement. Prospects, customers, clients, business partners and vendors of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media. Employees or contact persons of Controller's prospects, customers, clients, business partners and vendors. Suppliers and service providers of the Controller. Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.
Categories of Personal Data:	In outline, data about users of the Controller's website and people subscribed to receive the Controller's emails, including personal details, what they did, and what happened to them… The Personal Data may include the following: • Personal details, names, email addresses, personal addresses. • Unique identifiers such as username, account number or password. • Personal Data derived from a user's use of the Services such as what pages they have seen and what products they have seen, carted, or purchased. • Personal Data within email and messaging content which identifies or may reasonably be used to identify, Data Subjects. • Meta data including sent, to, from, date, time, subject, which

	may include Personal Data. • Geolocation based upon IP address, but not IP address. • Information about preferences, such as categories of favourite categories of products. • Purchases made.
Sensitive Data: (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the Sensitive Data, restrictions for onward transfers or additional security measures:	No sensitive data is stored unless this is specifically requested by the Controller.
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	Processing operations include but are not limited to personalisation and triggering so that Data Subjects see marketing that is tailored to them.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Unless agreed otherwise in writing, for the duration of the Agreement, subject to clause 14 of the DPA.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-processor list accessed via "GDPR Data Processing Addendum: Approved Sub-processors" on https://www.freshrelevance.com/legal/legal-documents sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent	Where the EU GDPR applies, the Netherlands Data Protection

supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Authority (Data Protection Commission). Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

Exhibit B

Technical and Organisational Security Measures
(Including Technical and Organisational Measures to Ensure the Security of Data)

Below is the location of the technical and organisational measures implemented by the Processor (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Details of the Processor's technical and organisational security measures used to protect Personal Data are available at https://dotdigital.com/trust-center/technical-and-organizational-security-measures/.

Where applicable this Exhibit B will serve as Annex II to the SCCs.