Data Protection Addendum
(Updated April 12 2022)

Parties to this DPA

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

The Customer entity (or "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**") between Fresh Relevance and the Customer.

Does this DPA apply?

I. If there is already a DPA between the Customer and Fresh Relevance, for example because an Agreement between the Customer entity and Fresh Relevance includes one, then that DPA applies.
II. Otherwise, if Fresh Relevance is doing work for the Customer but there is no DPA, the Customer can choose to sign this one. In that case, if the Customer signs, then this DPA applies to the work, and if there's an agreement between Fresh Relevance and the Customer then this DPA is supplemental to it.
III. If the situation is as in II, and privacy legislation requires a contract to govern it*, then the Customer must sign this one*.
IV. Otherwise, **this DPA does not apply** - *it is ignored and is not legally binding*.

If you are signing this DPA

This DPA has been pre-signed on behalf of the Processor. To sign it, Customer must sign all the places indicated and return a copy of the countersigned DPA to *GDPR@freshrelevance.com*. Upon receipt of the validly completed DPA by Fresh Relevance at this email address, this DPA will become legally binding.

1. Definitions

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

"**Affiliate**"	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
"Agreement"	means the agreement between the Controller and the Processor for the provision of the Services;
"CCPA"	means the California Consumer Privacy Act of 2018, along with its regulations and as amended from time to time;
"Controller"	means the Customer;
"Data Protection Law"	means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the FDPA, the UK Data Protection Act 2018, the CCPA and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
"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 Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; FDPA) and as amended from time to time;
"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"	means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2. Purpose

2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. 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 pursuant to the terms of the Agreement, 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, as updated from time to time.

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 on the instructions from the Controller unless required to do so by any Data Protection Law.

4. Processor Obligations

4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA.

4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the documented instructions of the Controller.

4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any Data Protection Law.

4.4 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; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

4.5 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.

4.6 The Processor 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.

4.7 The technical and organisational measures defined in Exhibit B shall at all times be adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures defined in Exhibit B and appropriate pursuant to the Processor's obligations in clauses 4.5 and 4.6 above.

4.8 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.

4.9 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

4.10 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

4.11 The Processor may not: (i) sell Personal Data; (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; (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; and (iii) all Affiliates of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.

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 acknowledges and agrees that some instructions from the Controller including the Processor assisting with audits, inspections, DPIAs 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 All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.

6.3 The Controller authorises the Processor to use the Sub-processors at https://www.freshrelevance.com/images/uploads/blog/GDPR_Data_Processing_Addendum_Subprocessors.pdf 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.

6.4 The Controller may object to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's

notice. If the Controller objects to a new or replacement Sub-processor, the Controller may 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. The Processor will refund the Controller any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination with respect to such terminated Services.

6.5 All Sub-processors who process Personal Data shall comply with the obligations of the Processor set out in this DPA. The Processor shall prior to the relevant Sub-processor carrying out any processing activities in respect of the Personal Data: (i) appoint each Sub-processor under a written contract containing materially the same obligations to those of the processor in this DPA enforceable by the Processor; and (ii) ensure each such Sub-processor complies with all such obligations.

6.6 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 legally 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 Irish law;

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

(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) notify the Controller on receiving the 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.

9. Audit

9.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

9.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which shall be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.

9.3 This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

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 48 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.

10.3 Upon confirmation of any vulnerability or breach of the Processor's security affecting the Controller Personal Data in the Processor's custody and control, The Processor will modify its processes and security program as necessary to mitigate the effects of the vulnerability or breach upon such the Controller Personal Data.

10.4 Notification(s) of Security Breaches, if any, will be delivered to one or more of the Controller's administrators by any means The Processor selects, including via email. It is the Controller's sole responsibility to ensure the Controller's authorised administrators maintain accurate contact information on The Processor Platform

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 Processor shall reasonably assist the Controller in meeting the Controller's obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to the Processor.

11.4 The Controller shall notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the Processor is unable to accommodate necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

11.5 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 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

12.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

12.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.

12.4 The Controller shall not be entitled to recover more than once in respect of the same loss.

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 Controller may export Personal Data from the Fresh Relevance Platform at any time during the term of the Agreement, using the Fresh Relevance Platform's then existing features and functionality, at no additional charge. The Processor's obligations to return Personal Data upon termination of the Agreement may be fulfilled by permitting the Controller to export Personal Data as specified above. The Processor will delete the Personal Data within the Fresh Relevance Platform within 60 days of termination or expiration of the Agreement. The Processor is not obligated to delete copies of Personal Data retained in automated backup copies generated by The Processor, which The Processor may retain for up to 12 months from their creation. Such backup copies will remain subject to this DPA until the copy, or the Personal Data in the copy, is destroyed.

15. General

15.1 This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

15.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

15.3 Subject to any provision of the SCCs to the contrary, this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

12.4 The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Signed on behalf of the parties

DATA EXPORTER

Name: ……..

Authorised Signature ……...

DATA IMPORTER

Name: Mr Peter Richard John Austin

Authorised Signature 

Exhibit A

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

MODULE THREE: PROCESSOR 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 personalization 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 Irish Data Protection Authority

supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	(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 FOUR: PROCESSOR TO CONTROLLER

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. 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 personalization 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 Irish Data Protection Authority

supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	(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 in the "Fresh Relevance Security Policy" which is available to Customer on request.

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