VE FRAMEWORK TERMS

FRAMEWORK TERMS

Last updated: 18 December 2019

FRAMEWORK TERMS

Introduction

These Ve Framework terms and conditions ("**Framework**") govern your access to and use of the Service Offerings (as defined below) and create a legally binding agreement between Ve Global UK Limited (Company No. 10706696) whose registered office is at 77 Leadenhall Street London EC3A 3DE ("**Ve**," "**we**," "**us**," or "**our**", "**Supplier**") and you or the entity you represent ("**you**", "**Customer**", or "**Client**").

Recitals

(A) Creating an Account and signing up to this Framework

This Framework shall take effect when you create an Account with us or when you sign (or otherwise indicate your agreement to) an Order, whichever occurs first.

(B) Ordering a Service Offering

When you place an Order you will be presented with a description of the Service Offering and key commercial terms such as the price and subscription period as set out in the Order (except under a free trial as described in introductory paragraph (F) below, in which case the Order will not apply until the free trial is over). This Framework, together with each Order, Policies and/or descriptions of our Service Offerings on the Platform, creates an "**Agreement**". The Agreement shall take effect on the date that you: (i) click the "I agree to Ve's Order" (or words to that effect) button or check box presented with the Order or otherwise indicate your agreement to the Order; or (ii) on agreement of your Order via email or hard copy signature; or (iii) when you use any relevant Service Offering, whichever is the earliest ("**Effective Date**"). Each Agreement forms a separate and independent contract for the relevant Service Offering.

(C) Precedence

If there is a conflict between any part of an Agreement, the following order of precedence will apply: (i) the main body of an Order; (ii) any addendum, annex or schedule to that Order; (iii) this Framework; (iv) our Policies; and (v) descriptions of our Service Offerings on the Platform.

(D) Authority to bind

When entering into this Framework or an Agreement with us, you represent to us that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into this Framework or any Agreement on behalf of an entity, such as the company you work for, you represent to us that you have legal authority, power and right to bind that entity. If you (or, if relevant, the entity on whose behalf you are acting) do not agree to all of these terms or the terms of an Agreement (or if you do not have the right to bind the entity on whose behalf you are acting), you should not click the "Click here to accept our terms and conditions" (or words to that effect) button or check box and proceed further or start using the Service Offerings.

(E) Definitions

Please see the Appendix for definitions of certain capitalised terms used in this Framework. Capitalised terms used herein but not defined herein shall have the meanings set forth in the Order.

(F) Free Trial

If you are using a Service Offering under a trial, instead of the Order applying this paragraph F will apply and, in the event of any inconsistency, this paragraph F takes precedence over the remainder of any Agreement and in particular any warranties, promises and/or terms purporting to limit liability. You acknowledge that a trial Service Offering is (unless otherwise agreed between us in writing) provided free of charge for a trial period. Accordingly, and subject to clause 12.1, we shall not be liable to you (whether for breach of contract, negligence, misrepresentation or for any other reason) for any loss or damage whatsoever incurred or sustained by you in connection with the Agreement and/or use of a trial Service Offering whether such loss or damage is direct, indirect or consequential and including, without limitation (direct and indirect): (i) loss of profit; (ii) loss of

business; (iii) lost data; (iv) work delays; and (v) wasted staff or management time. Each trial Service Offering is provided "as is" with no warranties, undertakings, conditions or terms of any kind, whether express or implied, statutory or otherwise. In particular, no condition, warranty, representation and/or other term is given or entered into to the effect that the trial Service Offering will be of satisfactory (or other) quality, that it will be fit for any particular purpose (whether made known to us or not), that use of the trial Service Offering will be uninterrupted or error-free, or that it will perform to or operate in accordance with any particular standard. **On expiration of any free trial period, you will be automatically signed up on a fee-paying basis for that Service Offering, unless we receive notice from you in writing to the contrary prior to expiration of the free trial period.**

1. Use of our Service Offerings

1.1 Generally. You may access and use the Service Offerings in accordance with the Agreement. You will adhere to all laws, rules, and regulations applicable to your use of the Service Offerings, including the Policies.

1.2 Your Account. To access the Service Offerings, you must create an Account associated with a valid e-mail address and sign up to this Framework. Unless explicitly permitted by the Order, you may only create one Account per email address. You warrant that all information you provide to us when registering an Account is true and accurate. You must ensure your Account is updated with any relevant changes. We reserve the right in our absolute discretion to refuse to register an Account for any given prospective user. You are responsible for protecting your Account login details and all activities that occur under your Account, regardless of whether the activities are undertaken by you, your employees or a third party (including your contractors or agents) and, except to the extent caused by our breach of the Agreement, we and our affiliates are not responsible for unauthorised access to your Account or any loss or damage that may result therefrom. You will contact us immediately if you believe an unauthorised third party may be using your Account or if your Account information is lost or stolen. You may terminate your Account and any Agreement in accordance with clause 7.

1.3 Third Party Content. Third Party Content, such as software applications provided by third parties, may be made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Because we may not have tested or screened the Third-Party Content, your use of any Third Party Content is at your sole risk.

2. Changes.

2.1. To the Service Offerings. We may change, discontinue, or deprecate any of the Service Offerings (including the Service Offerings as a whole), or change or remove features or functionality of the Service Offerings from time to time. We will notify you of any material change to or discontinuation of the Service Offerings through our Platform or through other reasonable means.

2.2 **To this Framework. We may change, discontinue or add to this Framework and other documents referenced in the Agreement from time to time. When we do we will revise the "last updated" date given above. It is your responsibility to review the Framework frequently and to remain informed of any changes to it. The then-current version of the Framework will supersede all earlier versions. You agree that your continued use of our Service Offerings after such changes have been published will constitute your acceptance of such revised Framework. We will provide advance notice of this wherever practicable and will notify you of any material change to the Framework through our Platform or through other reasonable means.**

3. Security and Data.

3.1 In this Framework and each Agreement, references to "controller", "data subject", "personal data", "personal data breach", "processor" and "processing" have the meanings set out in the GDPR (and "process" and "processed" shall be construed accordingly).

3.2 Each party will comply with applicable Data Protection Legislation in relation to its respective activities under

and in connection with this Framework and each Agreement, including compliance with Article 5 GDPR (data protection principles) and all applicable data security requirements in respect of personal data that each party holds (including Article 32 GDPR).

3.3 Our Privacy Policy explains how we collect and use personal data.

3.4 Where we are, together, joint controllers with you in respect of our Service Offerings, the data sharing agreement set out at Schedule 1 below will apply.

3.5 We are, for certain purposes, a controller in our own right where we determine the purposes for which we process data, such as the use of our own data assets (which may include cookies, other online identifiers, behavioural data and other personal data collected by us via our provision of the Service Offerings, as more fully explained in our Privacy Policy) to support and/or enhance the delivery of our Service Offerings and/or for the creation of new solutions or services created for the benefit of our clients. Where we are a Controller in our own right of the data that we collect, the data sharing agreement set out at Schedule 1 below will apply.

3.6 Where we are a Processor, the data processing agreement set out in Schedule 2 below will apply. The aforementioned data processing agreement shall only apply to the extent that we are a Processor of the data that we collect for the Service Offering in question. For details of where we are a Processor, please see our guidance here.

3.7 **You agree that you are responsible for obtaining consent from the Data Subject for: (i) any cookies or similar technologies that we deposit and use to collect data from Your Website(s); and (ii) any consents necessary for marketing and advertising including without limitation unsolicited direct marketing. As such, you undertake to**:

(a) to obtain, and on reasonable request evidence, any and all marketing permissions and other consents that are required to enable us to provide the relevant Service Offerings, including (but not limited to) in respect of cookies that we use and electronic marketing that we send on your behalf, in a manner that is compliant with applicable Data Protection Legislation;

(b) to have in place and, on reasonable request evidence, in respect of Digital Properties that you operate through which we collect personal data, appropriate mechanisms, compliant with Data Protection Legislation, for obtaining any and all permissions and other consents that are required for the collection of personal data for the purposes used by us as set out in our Privacy Policy and each Agreement;

(c) to ensure, in respect of Digital Properties that you operate through which we collect personal data, that you have a privacy notice that complies with Data Protection Legislation and, in particular, expressly names Ve Global as a party for whom, and by whom, personal data is collected through your Digital Properties, including a clear link to our Privacy Policy (to help end users understand who we are and what we do); and

(d) in respect of any marketing communications that are served to data subjects in respect of our Service Offerings (including Digital Assistant and Email Remarketing solutions) to include in the marketing communication clear and visible language that makes clear Ve's involvement, including a clear link to our Privacy Policy (to help end users understand who we are and what we do).

3.8 Notwithstanding anything else in this Agreement, Ve and its group companies may use, exploit and disclose, in aggregated and/or anonymised form, data (that is not, or is no longer, personal data within the meaning of Data Protection Legislation) resulting from or generated through the provision of our Service Offerings.

4. Your Responsibilities

4.1 Your Content. Without prejudice to clause 3 in relation to personal data, you are solely responsible for the

provision, development, content, operation, maintenance, and use of Your Content. For example, you are solely responsible for: (a) the technical operation of Your Content; (b) the compliance of Your Content with the Policies and applicable law; (c) ensuring Your Content is accurate and kept up to date; (d) any claims relating to Your Content; and (e) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violates such person's rights.

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorised access and routine archiving Your Content. Your Account log-in credentials and private keys generated by the Service Offerings are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

4.3 End User Violations. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to the Agreement, Your Content or use of the Service Offerings, including by End Users. You are responsible for End Users' use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under the Agreement and that the terms of your agreement with each End User are consistent with the Agreement. If you become aware of any violation of your obligations under the Agreement by an End User, you will immediately terminate such End User's access to Your Content and the Service Offerings.

4.4 End User Support. You are responsible for providing customer service (if any) to End Users.

4.5 Traffic. You acknowledge that we do not guarantee traffic to your website and that you are solely responsible for generating traffic.

4.6 You will not, for the duration of this Framework, and for a period of 12 months following termination, directly or indirectly induce or attempt to induce any employee of ours of senior or management level who has been engaged in the provision, receipt, review or management of the Service Offerings or otherwise in connection with this Framework to leave our employment.

5. Fees and Payment

5.1 Fees. Your payment account will be managed via our Platform. We calculate and invoice Fees monthly. We may invoice you more frequently for Fees accrued if we suspect that your Account is fraudulent or at risk of non-payment. You will pay us the applicable Fees for use of the Service Offerings as described on our Platform and/or the Order (as applicable) in full and cleared funds, upon receipt of invoice, to a bank account nominated by us or using one of the payment methods we support. Fees for any new Service Offering or new feature of a Service Offering will be effective when we post updated Fees on the Platform unless we expressly state otherwise in a notice. We may increase or add new Fees annually during the Term by a percentage of no more than ten percent (10%) for any existing Service Offerings by giving you at least 30 days' written notice. If you do not notify us of your intention to terminate the affected Service Offering within 30 days of the notification of the proposed increase you will be deemed to have accepted the increase. We may charge you interest on all late payments at the rate of 4% over the then current base lending rate of the Bank of England at the date the relevant invoice was issued, commencing on the due date and continuing until fully paid, whether before or after judgment, without prejudice to any other right or remedy we may have.

5.2 Taxes. All Fees payable by you are exclusive of applicable taxes and duties, including VAT and applicable sales tax. You will provide us any information we reasonably request to determine whether we are obligated to collect VAT from you, including your VAT identification number. If any deduction or withholding is required by law, you will notify us and will pay us any additional amounts necessary to ensure that the net amount that we receive, after any deduction and withholding, equals the amount we would have received if no deduction or withholding had been required. Additionally, you will provide us with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

5.3 We collate details of transactions relating to our Service Offerings on the Platform, and invoice for those transactions on a monthly basis in accordance with clause 5.1. You may log into your Account at any time to review details of those transactions. If you dispute the validity of a transaction you can change its status on the Platform using your Account. Any pending transactions on the Platform invoicing section whose status is not amended within a 1-day period from the date of the conversion shall, unless otherwise agreed, be deemed automatically approved.

6. Temporary Suspension

6.1 Generally. We may suspend your or any End User's right to access or use any portion or all of the Service Offerings immediately upon notice to you if we determine:

(a) your or an End User's use of or registration for the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) may adversely impact the Service Offerings or the systems or Content of any other Ve customer, (iii) may subject us, our affiliates, or any third party to liability, or (iv) may be fraudulent;

(b) you are, or any End User is, in breach of the Agreement, including if you are late on your payment obligations for more than 15 days; or

(c) you are subject to an Insolvency Event.

6.2 Effect of Suspension. If we suspend your right to access or use any portion or all of the Service Offerings:

(a) you remain responsible for all Fees you have incurred through the date of suspension;

(b) you remain responsible for any applicable Fees for any Service Offerings to which you continue to have access; and

(c) we will not erase any of Your Content as a result of your suspension, except as specified elsewhere in the Agreement.

6.3 Our right to suspend your or any End User's right to access or use the Service Offerings is in addition to our right to terminate the Agreement pursuant to clause 7.2.

7 Term and Termination

7.1 Term. This Framework will commence on the occurrence of one of the events described in recital (A) of this Framework and shall continue indefinitely until terminated in accordance with its terms. Each Agreement shall commence on the Effective Date and shall continue indefinitely until terminated in accordance with its terms.

7.2 Termination.

(a) Termination for Convenience. Either party may terminate this Framework at any time for any reason by providing the other with written notice in accordance with the timing and notice period set out in the Order where there are no extant Agreements. Either party may terminate an Agreement at any time for any reason by providing the other with written notice in accordance with the timing and notice period set out in the Order to that effect. Termination of any one Agreement shall not affect the term of this Framework or any other Agreement(s).

(b) Termination for Cause.

(i) By Either Party. Without prejudice to any other rights or remedies to which the parties may be entitled,

either party may terminate an Agreement immediately without liability to the other if: (A) the other party commits a material breach of any of the terms of the Agreement and (if such a breach is remediable) fails to remedy that breach within 15 days of that party being notified in writing of the breach; or (B) an Insolvency Event occurs.

(ii) By Us. We may also terminate an Agreement immediately upon notice to you: (A) if you repeatedly fail to provide us assistance to enable us to carry out the Service Offerings; (B) if any act or omission by you or any End User results in a suspension described in clause 6.1; (C) if our relationship with a third party partner who provides software or other technology we use to provide the Service Offerings expires, terminates or requires us to change the way we provide the software or other technology as part of the Service Offerings; (D) if we believe providing the Service Offerings could create a substantial economic or technical burden or material security risk for us; (E) in order to comply with applicable law or requests of governmental entities or regulators, or (F) if we determine use of the Service Offerings by you or any End Users or our provision of any of the Service Offerings to you or any End Users has become impractical or unfeasible for any legal or regulatory reason.

7.3 Effect of Termination.

(a) Generally. Upon any termination of an Agreement:

(i) all your rights under the Agreement immediately terminate;
(ii) you remain responsible for all Fees you have incurred through the date of termination; and
(iii) you will immediately return or, if instructed by us, destroy all Ve Content relevant to the Agreement in your possession.

(b) On termination of an Agreement or this Framework, the accrued rights of the parties as at termination, or the continuation after termination of any provision including clauses 4.1, 4.6, 5.2, 7.3, 8 (except the license granted to you in clause 8.4), 9, 10, 11, 12, and 13 and those provisions implicitly surviving termination shall not be affected or prejudiced and will continue to apply in accordance with their terms.

8 Intellectual Property Rights and Licence

8.1 Your Licence to us. You or your licensors shall continue to own all Intellectual Property Rights in and to Your Content. Subject to the limited licence set forth herein, no Intellectual Property Rights in Your Content are transferred or assigned to us under an Agreement. You grant us and our affiliates a non-exclusive, worldwide, royalty free, transferable, sub-licensable licence to use, copy, transfer, distribute, store and modify Your Content to provide the Service Offerings and for marketing purposes.

8.2 Our Licence to you. We or our affiliates or licensors own and reserve all Intellectual Property Rights in and to the Service Offerings and Ve Content. In consideration of your payment of the Fees, we grant you a limited, revocable, non-exclusive, non-sublicensable, non-transferable licence to do the following during the Term: (i) access and use the Service Offerings solely in accordance with the Agreement; and (ii) copy and use the Ve Content solely in connection with your permitted use of the Service Offerings. Except as provided in this clause 8.2, no Intellectual Property Rights in the Service Offerings or Ve Content are transferred or assigned to you under the Agreement. You acknowledge that some Open Source Software may form part of the Service Offerings. Open Source Software is not licensed to you under the Agreement. You must comply with the terms of the applicable Open Source Software licences, a list of which is available upon request.

8.3 Licence Restrictions. Neither you nor any End User may use the Service Offerings in any manner or for any purpose other than as expressly permitted by the Agreement. Neither you nor any End User may, or may attempt to: (a) copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Service Offerings or Ve Content in any form or media or by any means; (b) (except to the extent permitted by law notwithstanding any contractual prohibition) reverse compile,

disassemble, reverse engineer or otherwise reduce to human-perceivable or source code or unlocked coding form all or any part of the Service Offerings or Ve Content; (c) access or use the Service Offerings, Ve Content or any part in order to build a product or service which competes with the Service Offerings or is in a way intended to avoid incurring Fees or exceeding usage limits or quotas; (d) attempt in any way to remove or circumvent any technical protection measures (TPMs), nor apply or manufacture for sale or hire, import, distribute, sell or let for hire, offer or expose for sale or hire, advertise for sale or hire, or have in its possession for private or commercial purposes, any means, the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of TPMs; or (e) use the Service Offerings or Ve Content to provide services to third parties or otherwise licence, sell, rent, lease, transfer, assign, distribute, display, disclose or otherwise commercially exploit or make the Service Offerings or Ve Content available to any third party. All licenses granted to you are conditional upon on your continued compliance with the Agreement and will immediately automatically terminate if you do not comply. You will use all reasonable endeavours to prevent any unauthorised access to, or use of, the Service Offerings and Ve Content and, in the event of any such unauthorised access or use, promptly notify us. During and after the Term, you will not assert, nor will you authorise, assist, or encourage any third party to assert, against us or any of our affiliates, customers, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding any Service Offerings or Ve Content you have used or had access to.

8.4 We grant you a non-exclusive, non-transferable, non-sublicensable licence to use the Ve Marks solely in connection with your use of the Service Offerings. Any goodwill arising from such use shall belong to us. You shall use the Ve Marks only in relation to the Service Offerings and in a manner, which complies with all standards and directions as to quality and mode of presentation laid down from time to time by us. In particular you shall not use the Ve Marks: (i) other than in respect of the Service Offerings; and (ii) in a manner which could affect the value or validity of the Ve Marks in any part of the world.

8.5 Suggestions. If you provide any Suggestions to us or our affiliates, we will own Intellectual Property Rights in and to the Suggestions, even if you have designated the Suggestions as confidential. We and our affiliates will be entitled to use the Suggestions without restriction. You hereby irrevocably assign to us with full title guarantee (including by way of present assignment of future rights) all Intellectual Property Rights in and to the Suggestions absolutely and agree to provide us any assistance we may require to document, perfect, and maintain our Intellectual Property Rights in the Suggestions. To the extent (if any) that the foregoing assignment is ineffective for any reason, you agree to grant and hereby grant to us a non-exclusive, perpetual, irrevocable, royalty-free, sublicensable, worldwide licence to make, have made, use, import, offer for sale, sell, reproduce, distribute, modify, adapt, prepare derivative works of, display, perform and otherwise exploit such Suggestions without restriction.

9 Indemnification.

9.1 General indemnity from you. You will fully defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives, on demand, from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable legal fees) arising out of, in connection with or relating to any third party claim concerning: (a) your or any End Users' use of the Service Offerings (including any activities under your Account and use by your employees and personnel); (b) breach of the Agreements or violation of applicable law (including Data Protection Legislation) by you or any End User; (c) Your Content or the combination of Your Content with other applications, content or processes, including any claim involving alleged infringement or misappropriation of third party rights by Your Content or by the use, development, design, production, advertising or marketing of Your Content; or (d) a dispute between you and any End User. If we or our affiliates are obligated to respond to a third-party claim, you will also reimburse us for reasonable legal fees, as well as our employees' and contractors' time and materials spent responding to the third party claim at our then-current hourly rates.

9.2 Process. We will promptly notify you of any claim subject to clause 9.1, but our failure to promptly notify you will only affect your obligations under clause 9.1 to the extent that our failure prejudices your ability to defend the

claim. You may: (a) use counsel of your own choosing (subject to our written consent) to defend against any claim; and (b) settle the claim as you deem appropriate, provided that you obtain our prior written consent before entering into any settlement. We may also assume control of the defence and settlement of the claim at any time.

9.3 Our indemnity to you. We will indemnify and hold you harmless or, at our option, defend or settle any Third Party Claim and shall be responsible for any reasonable losses, damages, costs (including legal fees) and expenses incurred by, or awarded against, you as a result of or in connection with any such Third Party Claim. The indemnity set out in this clause 9.3 shall not apply to the extent the Third Party Claim in question is attributable to or arises from: (a) possession, use, development, modification or maintenance of the Service Offerings (or any part thereof including for the avoidance of doubt incorrect installation) by you other than in accordance with the terms of the Agreement; (b) use in combination with any hardware or software not supplied or specified by us, or if the infringement would have been avoided by use not so combined; (c) your failure to use updated versions of the Service Offerings which would have avoided the infringement (provided they were made available to you in good time so as to avoid the infringement); or (d) your failure to comply with the terms of any applicable Open Source Software licence.

9.4 Process. Our indemnity in clause 9.3 is conditional upon you: (a) as soon as reasonably practicable giving written notice of the Third Party Claim to us, specifying the nature of it in reasonable detail; (b) not making any admission of liability, agreement or compromise in relation to the Third Party Claim without our prior written consent (such consent not to be unreasonably conditioned, withheld or delayed); (c) giving us and our professional advisers access at reasonable times (on reasonable prior notice) to your premises and your officers, directors, employees, agents, representatives or advisers, and to any relevant documents, so as to enable us and our professional advisers to examine them and to take copies for the purpose of assessing the Third Party Claim; (d) taking such action as we may reasonably request to avoid, dispute, compromise or defend the Third Party Claim; and (e) at our request allowing us to conduct the defence (and settlement if any) of the relevant claim. If any Third Party Claim is made, or in our reasonable opinion is likely to be made, we may at our sole option and expense (a) procure for you the right to continue using the Service Offerings in accordance with the Agreement; (b) modify the Service Offerings so that they cease to be infringing; (c) replace the Service Offerings with non-infringing works; or (d) terminate the relevant Agreement immediately on notice to you. This clause constitutes your exclusive remedy and our only liability in respect of Third Party Claims.

9.5 Our Data Indemnity to you: We agree to hold harmless and indemnify you, and keep you indemnified, from any and all costs, claims, damages, liabilities and expenses suffered or incurred by you as a result of any failure by us to comply with our obligations in clause 3. This indemnity shall not apply to the extent that any such cost, claim, damage liability or expense arises or is exacerbated as a result of your failure to comply with your obligations under this Framework and/or any Agreement. This indemnity is conditional upon you: (a) as soon as reasonably practicable giving written notice of the claim to us, specifying the nature of it in reasonable detail; (b) not making any admission of liability, agreement or compromise in relation to the claim without our prior written consent (such consent not to be unreasonably conditioned, withheld or delayed); (c) giving us and our professional advisers access at reasonable times (on reasonable prior notice) to your premises and your officers, directors, employees, agents, representatives or advisers, and to any relevant documents, so as to enable us and our professional advisers to examine them and to take copies for the purpose of assessing the claim; (d) taking such action as we may reasonably request to avoid, dispute, compromise or defend the claim; and (e) at our request allowing us to conduct the defence (and settlement if any) of the relevant claim.

10 Warranties

10.1 Mutual warranties. Each party represents and warrants to the other that: (a) it or its licensors owns all Intellectual Property Rights it requires to perform its obligations and grant any licences under the Agreement; (b) it has full power and authority to enter into the Agreement and shall secure and maintain during the Term any and all authorisations as may be necessary in respect of the performance of its obligations under the Agreement; (c) it

shall not knowingly do anything or omit to do anything which will cause the other to be in breach of any applicable law or regulation; and (d) it will not make false, misleading or disparaging representations or statements regarding the other party.

10.2 Your warranties. You further represent and warrant to us that Your Content or End Users' use of Your Content will comply with the Website Terms. If you have instructed a third party agent to represent you then you warrant to us that such third party agent has full authority to commit you to the Agreement and you remain liable for all acts and representations and agreements of such third party agent.

10.3 Specification. We warrant that the Service Offerings will perform substantially in accordance with the specification set out on the Platform and will be provided with reasonable skill and care. This warranty shall not apply to the extent of any non-conformance of use by you with the Agreement or our instructions or due to any incorrect installation of the Service Offerings. If the Service Offerings do not perform in accordance with this clause then we shall, at our expense, use all reasonable efforts to correct such non-conformance or provide alternative means of accomplishing the desired performance. Where we are able to correct or substitute within a reasonable time, such correction or substitution shall constitute your sole and exclusive remedy and our only liability in respect of the warranty breach.

11 Disclaimer

11.1 You acknowledge that the Service Offerings have not been developed to meet your individual requirements and it is your responsibility to ensure the Service Offerings meet your requirements.

11.2 You assume sole responsibility for results obtained from your use of the Service Offerings and for conclusions drawn from such use and we recommend that if you intend to use any information resulting from the Service Offerings you should not do so without carrying out proper investigation and obtaining appropriate independent professional and legal advice.

11.3 We are not liable for any damage caused by errors or omissions in any information, instructions or scripts provided to us by you in connection with the Service Offerings or any actions taken by us at your direction.

11.4 Except for those warranties in clause 10 of this Framework, we and our affiliates and licensors make no representations, warranties, conditions or other terms of any kind, whether express, implied, statutory or otherwise regarding the Service Offerings or the Third Party Content, including any warranty that the Service Offerings or Third Party Content will be uninterrupted, error free or free of harmful components, or that any content, including Your Content or the Third Party Content, will be secure or not otherwise lost or damaged and we are not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and you acknowledge that the Service Offerings may be subject to limitation, delays and other problems inherent in the use of such communications facilities.

11.5 Except to the extent prohibited by law and as expressly provided under the Agreement, we and our affiliates and licensors disclaim all warranties, conditions or other terms, including any implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, and any warranties arising out of any course of dealing or usage of trade.

12 Limitations of Liability.

12.1 Nothing in this Framework or any Agreement excludes the liability of either party for: (a) death or personal injury caused by its negligence or that of its employees or personnel; (b) for fraud or fraudulent misrepresentation; (c) for non-payment of Fees; or (d) any other liability that cannot be excluded under applicable law, even if any other term of this Agreement would suggest that this might otherwise be the case.

12.2 Exclusions. Subject to clause 12.1, neither party shall be liable whether in tort (including for negligence), breach of statutory duty, contract, misrepresentation, restitution or otherwise for any: (a) loss of profits; (b) loss of business; (c) depletion of goodwill and/or similar losses; (d) loss or corruption of data or information; or (e) for any special or indirect or consequential loss, costs, damages, charges or expenses, however arising under or in connection with this Agreement whether or not reasonably foreseeable and even if the other party had been advised of the possibility of incurring the same.

12.3 Financial cap. Subject to clauses 12.1, 12.2 and 12.4, our total aggregate liability to you in respect of any Contract Year in contract, tort (including negligence) or breach of statutory duty, misrepresentation, restitution or otherwise, arising from or in connection with the performance or contemplated performance of this Framework and each Agreement shall be limited as follows: (a) in aggregate in relation to each Agreement, to the greater of (i) an amount equal to 100% of the total amount payable to us in the previous Contract Year and (ii) £25,000; and (b) in the aggregate under this Framework, to £1,000,000, so that under no circumstances will our total aggregate liability under or in relation to this Framework (including all Agreements) in a Contract Year exceed £1,000,000. In respect of the first Contract Year of the relevant Agreement the amount in sub-clause (b) shall apply. "Contract Year" for these purposes means the relevant twelve-month period starting on the effective date set out in the relevant Order or an anniversary thereof (as appropriate). Where liability arises out of an event or series of connected events which span more than one Contract Year, all such liability shall be deemed to have occurred in the Contract Year in which the event first occurred, or in which the first of a series of connected events occurred, as appropriate.

12.4 IP and Data Financial Caps: Subject to clauses 12.1 and 12.2, our total aggregate liability to you in respect of any Contract Year in contract, tort (including negligence), breach of statutory duty, misrepresentation, restitution or otherwise, arising from or in connection with:

a) any claim that the existence and/or use of our Service Offerings infringes third party rights (including any Third Party Claim and the indemnity provided under clause 9.3) shall not exceed i) in respect of each Agreement, the greater of: A) 100% of the Fees received by us under the relevant Agreement and B) £10,000; and ii) in respect of all Agreements and the Framework Terms £50,000; and

b) breach of our data protection related warranties, obligations and other terms, including clause 3 and the indemnity at clause 9.5, shall not exceed: i) in respect of the relevant Agreement £100,000; and ii) in respect of all Agreements and the Framework Terms £500,000.

13 Miscellaneous.

13.1 Confidentiality and Publicity. Each party undertakes to keep the Confidential Information of the disclosing party strictly confidential and not publish or disclose any part of it except as strictly necessary to exercise its rights or perform its obligations under an Agreement. Each party shall apply no lesser security measures and degree of care than those which it takes in protecting its own Confidential Information and in any event no less than that which a reasonable person or business would take in protecting its own confidential information. The obligations of confidentiality will not apply to the whole or any part of the Confidential Information to the extent that it: (a) is or becomes publicly known other than through any act or omission of the receiving party; (b) was in the other party's lawful possession before the disclosure; (c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure; (d) is independently developed by the receiving party, which independent development can be shown by written evidence; or (e) is required to be disclosed by law, by any court of competent jurisdiction or by any regulatory or administrative body. The obligations of confidentiality shall continue beyond the Term until such time as the information enters the public domain other than through the act or omission of the receiving party. Each party shall promptly on request and in any event on termination of an Agreement return to the other party or cause to be deleted all materials incorporating Confidential Information in its possession or control relevant to that Agreement. You will not issue any press release or make any other

public communication with respect to an Agreement or your use of the Service Offerings. You will not misrepresent or embellish the relationship between us and you (including by expressing or implying that we support, sponsor, endorse, or contribute to you or your business endeavours), or express or imply any relationship or affiliation between us and you or any other person or entity except as expressly permitted by an Agreement.

13.2 Force Majeure. Neither us nor our affiliates nor you will be liable for any delay or failure to perform any obligation under an Agreement where the delay or failure results from any Force Majeure Event provided that the other party is notified of such an event and its expected duration.

13.3 Independent Contractors. We and you are independent contractors and this Framework and any Agreement shall not constitute a partnership, agency or joint venture between the parties.

13.4 Third Party Rights. An Agreement will not create any third-party beneficiary rights in any individual or entity that is not a party to the Agreement.

13.5 English language. If an Agreement is translated into any language other than English, the English language text will prevail.

13.6 Notice. (a) To You. We may provide any notice to you under an Agreement by: (i) posting a notice on the Ve Site, effective upon posting; or (ii) sending a message to the email address then associated with your Account, effective when we send the email. It is your responsibility to keep your email address current. You will be deemed to have received any email sent to the email address then associated with your Account when we send the email, whether or not you actually receive the email; (b) To Us. To give us notice under this Framework or an Agreement, you must contact us: (i) by email to info@ve.com (effective one Business Day after they are sent); or (ii) by personal delivery (effective immediately), overnight courier (effective one Business Day after they are sent) or registered or certified mail to Ve Global UK Limited, 77 Leadenhall Street London EC3A 3DE, England (effective three Business Days after they are sent). We may update our email or postal addresses for notices by posting a notice on the Ve Site.

13.7 Assignment. You will not, without our prior written consent, assign, transfer, charge, subcontract or deal in any other manner with all or any of your rights or obligations under this Framework or any Agreement.

13.8 No Waivers. A waiver by us of any terms of this Framework or an Agreement in a particular instance shall not be deemed or construed to be a waiver of such term or condition for the future or affect our rights in respect of any subsequent breach of the terms of this Framework or an Agreement as applicable. All rights and remedies contained in this Framework and any Agreement shall be distinct, separate and cumulative and no action or inaction by us shall operate to exclude or deprive us of any other rights allowed by law.

13.9 Severability. If any part of this Framework or an Agreement is or becomes invalid, illegal or unenforceable (including any provision excluding liability), it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant part shall be deemed deleted. Any modification to or deletion of a part shall not affect the validity and enforceability of the rest of this Framework or an Agreement as applicable. If one party gives notice to the other of the possibility that any part of this Framework or an Agreement is invalid, illegal or unenforceable, the parties shall negotiate in good faith to amend such part so that, as amended, it is legal, valid and enforceable and, to the greatest extent possible, achieves the intended commercial result of the original provision.

13.10 Entire Agreement. Each Agreement contains the entire agreement between the parties relating to its subject matter and supersedes any previous agreements, arrangements, undertakings or proposals, written or oral, between the parties in relation to such matters or any statements made by any person, including (without limitation) any employees or agents for each party. Save for fraud or fraudulent misrepresentation, the parties shall have no liability for any such representation being untrue or misleading. You acknowledge and agree that

in entering into this Framework and/or any Agreement you do not rely on any undertaking, promise, statement, representation, warranty, condition and/or other term (whether in writing or not) in relation to the subject matter of this Agreement, other than as expressly set out in this Agreement.

13.11 Governing Law and Jurisdiction. This Framework and any Agreement shall be governed and interpreted in accordance with English law and subject to clause 13.12 the parties irrevocably agree that the courts in England and Wales shall have non-exclusive jurisdiction in relation thereto.

13.12 Dispute Resolution. Any dispute arising out of or in connection with this Framework or an Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the rules of the London Court of International Arbitration ("LCIA"), which rules are deemed to be incorporated by reference into this clause. The place and seat of arbitration shall be London, England. The language to be used in the arbitration proceedings shall be English. The number of arbitrators shall be one. Notwithstanding this clause, we may bring proceedings in the courts of any state or territory which has jurisdiction for reasons other than the parties' choice, for the purpose of seeking an interim injunction, order or other non-monetary relief to protect its Intellectual Property Rights and/or rights in Confidential Information.

Please sign below. Customer's continued use of Supplier's services will be deemed to constitute acceptance of and agreement to this Agreement including the Sections, Annexes and Appendices (as applicable).

We look forward to continuing our relationship with you.

Signed for and on behalf of	Signed for and on behalf of
VE GLOBAL UK LIMITED	**Client**
Signature: 	Signature:
Print Name: Charles Delamain	Print Name
Position: CEO	Position:

APPENDIX – DEFINITIONS

"Account"	means your account to access the Service Offerings through the Platform;
“Ads”	means any advertisement and other content;
“Agreement”	is defined in the Introduction section (B);
“Business Days”	means any day which is not a Saturday, Sunday or public holiday in England;
“Confidential Information”	means (i) proprietary information (whether owned by the disclosing party or a third party to whom the disclosing party owes a non-disclosure obligation), including information relating to our technology, customers, business plans, promotional and marketing activities, finance and other business affairs, knowhow, software, including without limitation its source code, translations, compilations, partial copies and derivative works; (ii) such information which is marked as confidential at the time of disclosure to the receiving party, or if in oral form, is identified as confidential at the time of oral disclosure and reduced in writing or other tangible (including electronic) form including a prominent confidentiality notice and delivered to a receiving party within 30 days of disclosure; (iii) such information that, by the nature of the circumstances surrounding the disclosure, ought to be treated in good faith as proprietary and/or confidential;
“Content”	means software (including machine images), data, text, audio, video images or other content;
"Data Protection Legislation"	means all data protection and privacy laws, regulations, directives and rules, including GDPR and the EU Privacy and Electronic Communications Directive (2002/58/EC), each as transposed into domestic legislation of each Member State or other territory, and as amended, replaced or superseded from time to time, and including laws implementing or supplementing the GDPR and other data protection and privacy laws elsewhere in the world from time to time;
“Digital Properties”	means websites, mobile applications, media players, mobile content, and/or other any properties approved by us;
“Effective Date”	is defined in the introductory paragraph (B) of this Framework;
“End User”	means any individual or entity that directly or indirectly: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under your Account. The term “End User” does not include individuals or entities when they are accessing or using the Service Offerings or any Content under their own Account, rather than your Account;
“Fees”	means the fees payable by you to us according to the rates as referred to in the Order or Platform;
“Framework”	means this Framework, as amended by us from time to time pursuant to clause 2.2;
“Force Majeure Event”	means any cause beyond our reasonable control, including without limitation strikes, lockouts or other industrial disputes (whether involving our workforce or any other party), failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental

	order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors;
“GDPR”	means EU 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 (General Data Protection Regulation);
“Insolvency Event”	(a) an order is made or a resolution is passed for the winding up of the other party, or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order in relation to the other party; or (b) an order is made for the appointment of an administrator to manage the affairs, business and property of the other party, or documents are filed with a court of competent jurisdiction for the appointment of an administrator of the other party, or notice of intention to appoint an administrator is given by the other party or its directors or by a qualifying floating charge holder (as defined in paragraph 14 of Schedule B1 to the Insolvency Act 1986); or (c) a receiver is appointed of any of the other party's assets or undertaking, or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of the other party, or if any other person takes possession of or sells the other party's assets; or (d) the other party makes any arrangement or composition with its creditors, or makes an application to a court of competent jurisdiction for the protection of its creditors in any way; or (e) the other party ceases, or threatens to cease, to trade; or (f) the other party takes or suffers any similar or analogous action in any jurisdiction in consequence of debt;
“Intellectual Property Rights”	means all patents, rights to inventions, utility models, copyright and related rights, trademarks, service marks, trade, business and domain names, rights in trade dress or get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database rights, topography rights, moral rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications for and renewals or extensions of such rights, and all similar or equivalent rights or forms of protection in any part of the world unless otherwise stated in this Agreement;
"Open Source Software"	means software licensed under terms which require as a condition of the use, modification or distribution of such software that other software incorporated into, derived from, or distributed with such software: (a) be disclosed or distributed in source code form; (b) be licensed under terms that permit making derivative works; and/or (c) be re-distributable at no charge to subsequent licensees;
"Order"	means the purchase order or insertion order requested or placed by you for one or more of our Service Offerings which is made available through the Platform, via email and/or hard copy format;

“Platform”	means the digital platform operated, programmed and hosted by us from which you can deploy and use Service Offerings;
“Policies”	means the Website Terms, all restrictions described in the Ve Content and on the Ve Site, and any other policy or terms referenced in or incorporated into this Agreement. Policies does not include whitepapers or other marketing materials referenced on the Ve Site;
“Privacy Policy”	means our privacy policy (which includes our cookie policy), available here, as updated from time to time
“Service Offering(s):	means the services to be provided by us pursuant to an Order (which excludes Third Party Content);
“Suggestions”	means all suggested improvements to the Service Offerings that you provide to us;
“Term”	means the term of an Agreement beginning on the Effective Date;
“Territory”	means the territory or territories set out in the Order;
“Third Party Content”	means Content made available to you by any third party in conjunction with the Service Offerings;
“Third Party Claim”	means a claim or action brought by a third party alleging that the use of the Service Offerings in the Territory infringes its copyright or rights in confidential information;
“Ve”	means Ve Global UK Limited (Company No. 10706696) whose registered office is at 77 Leadenhall Street London EC3A 3DE, England;
“VeAds”	means the digital advertising services undertaken by Ve on your behalf;
“Ve Content”	means Content we or any of our affiliates make available in connection with the Service Offerings or on the Ve Site to allow access to and use of the Service Offerings;
“Ve Marks”	means the following marks and/or associated logos: Ve; and any other trademark or logo owned or licensed to Ve to which the customer has access as a result of an Agreement whether registered or unregistered anywhere in the world;
“Ve Site”	means the website at www.ve.com;
"Website Terms"	means the website terms and conditions for the Ve Site;
“Your Content”	means Content you or any End User: (a) run on the Service Offerings (which is not Ve Content); (b) submit to enable you or any End User to join the Platform; (c) cause to interface with the Service Offerings; (d) use in (or which contains) any Ads or which you or an End User submits or provides access to under the applicable Order; or (e) upload to the Service Offerings under your Account or otherwise transfer, process, use or store in connection with your Account, including without limitation the trade-marks, logos and brand identifiers used by you in connection with your business, and any information relating to the commercial objectives of your website, retail prices, data, graphics, logos, photographs, video, text, design work and any other items reasonably required by us;
“Your Website(s)”	means websites at the domains listed in the Order that are owned or operated by you

Schedule 1 - DATA SHARING AGREEEMENT

This Data Sharing Agreement ("Agreement") reflects the Supplier's services entered into between Supplier VE GLOBAL UK LIMITED and Customer with respect to the terms governing the sharing of personal data under the Framework Terms.

This Data Sharing Addendum is referred to and forms an integral part of the applicable VE Framework Terms. It is effective upon acceptance of the Framework Terms.

1. DEFINITIONS

1.1 The following definitions shall apply to this Agreement:

"Framework Terms" means the applicable Ve framework terms entered into between the Supplier and the Customer;

"Controller", "Data Protection Officer", "Data Subject", "Personal Data", "Personal Data Breach", "Processor", "Process"/"Processing"/"Processed", "Supervisory Authority" and "**appropriate technical and organisational measures**" take the meanings given to them in the Data Protection Legislation;

"Data Loss Event" means any event that results, or may result, in unauthorised or unlawful access to Personal Data held by the Supplier under this Agreement and controlled by the Controller, and/or actual or potential loss and/or destruction of, or damage to Personal Data in breach of this Agreement, including any Personal Data Breach;

"Data Protection Legislation" means all applicable data protection and privacy Laws in force from time to time (as amended) including without limitation (as applicable) the General Data Protection Regulation (*(EU) 2016/679*); the Law Enforcement Directive *(Directive (EU) 2016/680*); the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC); any other European Union Laws relating to personal data and all other Laws and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the relevant data protection or supervisory authority and applicable to a party.

"Data Subject Access Request" means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

"Law" means any law, subordinate legislation, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;

"Party" means a Party to this Agreement;

"Processed Personal Data" means the Personal Data that is Processed by the Customer and the Supplier under this Agreement;

"Protective Measures" means appropriate technical and organisational security measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;

"**Security Incident**" means: (i) accidental or unlawful destruction; (ii) accidental loss, alteration, unauthorised disclosure or access; and/or (iii) any other breach of security in relation to Processed Personal Data under this Agreement;

"Sub-processor" means any third Party appointed to process the Personal Data on behalf of the Supplier related to this Agreement; and

"Supplier Personnel" means all directors, officers, employees, agents, consultants and suppliers of the Supplier and/or of any sub-supplier engaged in the performance of its obligations under this Agreement.

1.2 References to either party in this Agreement includes a reference to that party's affiliates and group companies.

1.3 The Annexes form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the annexes.

1.4 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.5 A reference to a statue or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.6 Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

2. DATA CONTROLLER OBLIGATIONS

2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer and the Supplier are both Controllers. Supplier shall only process data: (i) in accordance with this Agreement (including Annex A) or any further instructions from Customer; and (ii) only to the extent, and in such a manner, as is necessary for the purposes of performing their obligations under this Agreement. Supplier shall only Process Personal Data strictly in accordance with Customer's written instructions and shall not use the Processed Personal Data for any other purpose.

2.2 Each Controller shall comply with the obligations that apply to it under applicable Data Protection Legislation in relation to the Processed Personal Data, and to the extent that a Controller under this Agreement is Processing Personal Data on behalf of the other party, it will Process such Personal Data in compliance with the Data Protection Legislation and the terms of this Agreement (including Annex A).

2.3 Both Parties agree to notify the other Party immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

2.4 Neither Controller will transfer Processed Personal Data outside the EEA without first entering into: (i) the Standard Contractual Clauses with the importer of the Processed Personal Data attached hereto as Annex C; or, (ii) any other permitted transfer mechanism prescribed by Data Protection Legislation.

2.5 Both Parties agree to implement and maintain Protective Measures to protect the Processed Personal Data from a Security Incident. Such measures shall have regard to 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. Such measures shall include, as appropriate those contained in Annex B.

2.6 Both Parties agree to notify the customer immediately upon becoming aware of a Security Incident involving the data that has been shared.

2.7 Both Parties agree to provide such assistance as is reasonably requested to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation.

3 DATA PROTECTION WARRANTIES, INDEMNITIES AND SURVIVAL

3.1 Notwithstanding any other provision of this Agreement, the Parties warrant that, upon receipt of Personal Data, each shall duly observe all its obligations as a Data Controller under Data Protection Legislation, which arise in connection with the Processing and the performance of its respective rights and obligations under this Agreement.

3.2 No variation of this Agreement shall be effective unless it is in writing and signed by both parties. No failure or delay to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

3.3 Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

3.4 Each party shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may reasonably be required for the purpose of giving full effect to this Agreement.

3.5 The provisions of this Agreement are expressly agreed by the Parties to survive any termination of this Agreement, howsoever arising.

Annex A

DESCRIPTION OF THE DATA SHARING

Client to Ve Global

Ve Global embeds JavaScript code, and uses both local storage and cookies in order to collect data from client's website users. Ve Global uses this data to track the user and provide services such as advertising and marketing. The client shares this data with Ve global.

Ve Global to Client

Additionally, where Ve Global drives traffic to clients websites, due to users clicking on adverts, Ve Global shares some of this data with clients.

Data Subjects

1. End users who visit client's websites.
2. Ve's employee contact details, in the course of running the business activities.

Purposes of the transfer

The purpose of this is to assist clients with advertising and selling their merchandise. This can be through advertising and marketing

Categories of Data

- email addresses and/or telephone numbers, if voluntarily entered into a Client Site (e.g. to buy a product or service, become a registered user, or sign up for marketing communications) ("**Contact Details**");
- data relating to browsing activity through the use of cookies, web beacons and pixel tags and similar technologies deployed on Client Sites or via emails sent by Ve Global on behalf of Clients ("**Behavioural Data**"); including:
    - IP (internet protocol) address; referring site URL (website address) where a session started, and details about a device, including type (e.g. mobile or tablet), brand, model, operating system name and version, browser name, version, language and protocol, and other unique numbers assigned to a device (e.g. IDFA on iPhone, Google adID on Android);
    - details about the pages of Client Sites visited and activities on Client Sites (e.g. products viewed or purchased, including details of purchases made and the time and duration of visits to pages of the Client's Site), page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page;
    - using an IP address, geolocation (e.g. postcode);

- events relating to ads served, such as the number of ads displayed and whether an end user clicked on an ad; and

- mailing address, age and/or date of birth, gender, marital status, number of children, nationality and/or country or city of residency, telephone number and first name, in each case if input into a Client Site ("**Profile Data**").

Annex B

SECURITY DECLARATION

1. INTRODUCTION

This policy sets set out a framework of governance and accountability for Information Security Management across the organisation. It forms the basis of the Information Security Management System (ISMS) and incorporates all policies and procedures that are required to protect company information by maintaining:

Confidentiality: protecting information from unauthorised access and disclosure.

Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion.

Availability: ensuring that information and associated services are available to authorised users whenever and wherever required.

This policy framework aims to develop a positive culture of information security throughout VE.

1.1 Document Definition

This document is a **Policy**.

For a complete list of all permitted document labels see *VE-PR-XX-IS-0002-Document Management Procedure* document. Please note these are the labels are permitted for document assets.

Policies, Standards and Procedures are the primary way in which the Information Security Steering Committee's (ISSC) direction and expectations are translated into specific, measurable, and testable goals and objectives. They are a critical component of governance at Ve Global (Ve) as they provide the structure and rules around which the organisation must operate. The Information Security Governance Committee (ISGC) has been established to create, maintain, and govern Information Security (IS) Policies, Standards and Procedures. The ISGC is responsible for communicating these documents to all applicable partners, joint ventures and subsidiaries, as well as distributing them and/or making them accessible to Ve's Employees (including consultants, contractors, and other applicable 3rd party vendors and partners).

1.2 Objective

The main objectives of this Policy are as follows:

1. Implement good practice in accordance with ISO 27001;
2. Protect against the potential consequences of security breaches;
3. Make certain that users are aware of and comply with all current and relevant legislation;
4. Increase security awareness and understanding across the organisation on the need for good information management, and of the direct responsibilities of every member for protecting data;
5. Promote information security practices that enhance the reputation of the organisation as a trustworthy, open, honest and ethical organisation;
6. Protect Ve Global from liability or damage through the misuse of data managed within the organisation.

In addition, the aim of the Ve's Information Security Policy Framework is to provide the foundation for all documentation and operational processes developed to protect information or data assets (used interchangeably from this point forward) owned by, or in the custody of, Ve from:

(a) Unauthorised disclosure – loss of CONFIDENTIALITY;

(b) Unauthorised or unintended modification – loss of INTEGRITY;

(c) Unintended loss of availability – loss of AVAILABILITY.

The Ve's Information Security Program supports the ISSC's objectives by providing the guidance and means to protect data assets. The Information Security Program includes maintaining Policies, Standards, and Procedures in areas including (but not limited to), internal and external risk management, threat and vulnerability management, logical and physical security, and mapping of Information Security (IS) responsibilities.

1.3 Scope

Applicability to Employees

Ve refers to Ve Global as well as its applicable partners, joint ventures and subsidiaries (where applicable). This Policy applies to all Employees, members of the Board of Directors, and all consultants and contractors.

Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

Applicability to Assets

This Policy applies to all information assets globally owned by Ve, or where Ve has custodial responsibilities.

2. POLICY STATEMENTS

2.1 Protection of Data

It is the Policy of Ve that information in all its forms: written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

2.2 Requirement for Policy Documentation

All supporting Policies, Standards, and Procedures must be documented and must be made available to individuals responsible for their implementation and compliance. All activities identified by the Policies, Standards and Procedures must also be documented.

2.3 Regional Variances

Where appropriate, regional variances to this Policy can be permitted to address all local legal and regulatory requirements. All such Policies, Standards, and Procedures are subordinate to, and must be consistent with, this Policy, and must be approved by the ISGC and signed off by the CEO.

See section 2.8 2.8 Policy **Exceptions** for more information.

2.4 Compliance with Policy Provisions

All processes and systems implemented after the effective date of these policies are expected to comply with the provisions of this Policy. Existing systems are expected to be brought into compliance as soon as practical.

2.5 Policy & Standard Review Period

All documentation must be reviewed at least yearly, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape. Alternative review timings to be determined by the ISGC where applicable.

2.6 Independent Review of the Information Security Program

The ISGC or the ISSC must initiate and independent review of all relevant aspects of the Ve Information Security Program at least annually, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape to ensure the continuing suitability, adequacy and effectiveness of the organisation's approach to managing inherent risks.

The review must:

a) Assess opportunities for improvement and the need for changes to the approach to security, including the Policy, Standards and/or control objectives;

b) Be carried out by individuals independent of the area under review. These individuals can be internal or third parties, but must demonstrate that they have appropriate skills and experience;

c) Be recorded and reported to the ISGC or the ISSC as appropriate. These records must be maintained, and;

d) Provide recommendations for corrective actions.

2.7 Information Security Roles & Responsibilities

All employees, members of the Board of Directors, and all consultants and contractors (where applicable) have responsibilities towards Ve Information Security that they must abide by.

To better establish Ve's Information Security Management System (ISMS), specific Information Security responsibilities are segregated between the ISSC and the ISGC.

The ISSC consists of top management and heads of departments who review and set key Information Security objectives in accordance to legislation, regulations, best practice and contractual obligations.

The ISGC consists of key points of contact from each department that are responsible for implementing controls and strategies to ensure that Information Security objectives are met and adhered to by the business.

For a comprehensive structure of Ve's Information Security responsibilities, refer to the Information Security Roles and Responsibilities standard.

2.8 Policy Exceptions

In the event that a business area or department is unable to comply with an approved Policy or Standard, an exception may be requested and submitted to the Policy Coordinator for initial review and onward presentation with recommendations to the ISGC and other interested parties.

An exception also allows for non-compliance with a Policy or Standard for either an approved period, or indefinitely. This can be caused by technical limitations within an application or system or may be a result of a fundamental change to a business process or be in-line with specific business goals. In the case of an exception, a member of the ISSC must formally accept the risk and retain accountability for non-compliance.

Refer to the policy exception procedure for further information.

2.9 Change Management

Any changes to the organisation, business processes, information processing facilities or systems that affect information security must be controlled.

The following change controls must be in place for any major change requests:

- description of change including designation of importance (e.g. minor, or major change);
- planning and testing of change(s);
- assessment of the potential impacts, including information security impacts, of such changes;
- formal approval procedure;
- verification that information security requirements have been met;
- communication of change details to all relevant persons;
- fail-back procedure or equivalent, and;
- description of audit capability and audit trail retention.

All relevant documentation must be updated as a result of any changes to Ve's systems.

2.10 Capacity Management

A documented capacity management plan must be documented for critical information systems.

The plan should include:

- System tuning and monitoring parameters;
- Detective controls to alert on threats to production systems;
- Projections of future capacity requirements.

2.11 Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of Ve's assets.

Where this is not possible, detailed mitigating controls must be prepared and approved as a Policy Exception by Ve's Information Security Team (IST).

Where practical, the initiation of an event should be separate from the authorisation.

The possibility of collusion must be considered in the design and implementation of information security controls.

2.12 Information Security in Project Management

Information security must be built into the Ve project management method to ensure that information security risks are identified and addressed as part of each project as a company-wide practice.

The following requirements will be integral to all project plans:

- Information security objectives are included;
- An information security risk assessment is conducted;
- Information security is part of all phases;
- Information security implications should be reviewed regularly in all projects, and;
- Responsibilities for information security should be defined and allocated to specified roles defined in the project management method.

2.13 Delegation of Information Security Tasking

Any individual with information security responsibilities may delegate to others, but the overarching accountability must reside with the original individual.

Where data that is classified higher than **Restricted** may be at risk, permission to delegate must be received from the Data Owner.

3. POLICY COMPLIANCE

3.1 Compliance Measures

Compliance with this Policy Framework is enforced through the validation of Compliance Measures relevant to each individual Policy and Standard derived from it.

3.2 Enforcement

As noted above, this Policy applies to all Ve Global Members, members of the Board of Directors, and all consultants, third parties and contractors (where deemed necessary). Violations of this Policy may result in disciplinary action, up to and including termination of employment and / or legal action.

Annex C

STANDARD CONTRACTUAL CLAUSES – CONTROLLER TO CONTROLLER

SECTION 1

Standard Contractual Clauses – Ve as Exporter – transferring data to clients as Importer **located outside the EEA** where advertising services are taken, or when taking email services where paid by a CPA, and data being used for invoicing.

COMMISSION DECISION

of 27 December 2004

amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries

(notified under document number C(2004) 5271)

(Text with EEA relevance)

(2004/915/EC)

ANNEX

‘

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

Ve Global UK (Company No. 10706696) whose registered office is at 77 Leadenhall Street London EC3A 3DE, England

hereinafter “data exporter”

and

Client

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

(a)“personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October

1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) “the data exporter” shall mean the controller who transfers the personal data;

(c)“the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

(d)“clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a)The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b)It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c)It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d)It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e)It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a)It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b)It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c)It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d)It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e)It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or

if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions (1) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data (2), or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects:

Initials of data importer:_;

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

(Annex A)

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

(Annex B)

DESCRIPTION OF THE TRANSFER

Ve Global provides advertising services to it's clients. To the extent that a user clicks on one of Ve's adverts selling a client's products and services, and gets diverted to the clients website, Ve is regarded as transferring that data to the client. The data that would be transferred would at a minimum be the referring URL. Additionally, Ve causes and facilitates the collection of data by the client, as by diverting the user to the cleints website, and to the extent that the client has technology to collect the data, the client has the opportunity to learn more about the user; IP address, device information, location data, and sometimes profiles can be inferred.

Information necessary to prove invoices where Ve Global has provided services on a cost per click or purchase basis, may be necessary to share to verify the invoices.

Data Subjects

1. End users who click on adverts and get diverted to the client's website.

2. Ve's employee contact details, in the course of running the business activities.

Purposes of the transfer

The purpose of this is to provide the user with the opportunity to buy the goods that they have shown interest in, from the provider that is selling the goods and services, on the website belonging to the advertiser, and for this to be tracked to allow the parties involved with spending money on placing adverts, to be paid for their achievements when a sale is realised.

Ve's transfer of data is one initiated by the user but facilitated (caused) by Ve Global placing the advert. If the user clicks on an advert, they will be directed to website of the advertising client. The client then has the opportunity to collect information by their own cookies and similar technologies or permit other third parties to collect information if they have deposited cookies on the website of the client.

Once a sale is agreed / message displayed, Ve may be paid on a cost per click / view/ display or purchase basis, and the information is retained for invoicing and may need to be transferred to verify the charges on invoices. This part is not just for adverts, but also onsite experiences where Ve Global is paid via number of messages/interactions

Categories of Data - Emails and on-site messaging services (non adverts), that will be used to support CPA sales, and data used to prove the transactions for invoicing.

- email addresses and/or telephone numbers, if voluntarily entered into a Client Site by an end user (e.g. to buy a product or service, become a registered user, or sign up for marketing communications) ("**Contact Details**");
- data relating to an end user's browsing activity through the use of cookies, web beacons and pixel tags and similar technologies deployed on Client Sites or via emails sent by Ve on behalf of Clients ("**Behavioural Data**"), including:
    - IP (internet protocol) address; referring site URL (website address) where a session started, and details about devices, including type (e.g. mobile or tablet), brand, model, operating system name and

version, browser name, version, language and protocol, and other unique numbers assigned to a device (e.g. IDFA on iPhone, Google adID on Android);

- details about the pages of Client Sites visited and activities on Client Sites (e.g. products viewed or purchased, including details of purchases made and the time and duration of visits to pages of the Client's Site), page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page;
- using an end users IP address, your geolocation (e.g. postcode);
- events relating to ads served on an end user, such as the number of ads displayed to them and whether they clicked on an ad; and

- mailing address, age and/or date of birth, gender, marital status, number of children, nationality and/or country or city of residency, telephone number and first name, in each case if input into a Client Site ("**Profile Data**").

Recipients of the Data

The client as detailed in this agreement.

Categories of Data – Programmatic Advertising services

This is where Ve Global causes and facilitiates the transfer of data to the clients/customer website (directs traffic to clients website):

- data relating to your end users browsing activity through the use of cookies, web beacons and pixel tags and similar technologies deployed on Client Sites;
- ("**Behavioural Data**"), including:
  - IP (internet protocol) address; referring site URL (website address) where a session started, and details about a device, including type (e.g. mobile or tablet), brand, model, operating system name and version, browser name, version, language and protocol, and other unique numbers assigned to a device (e.g. IDFA on iPhone, Google adID on Android);
  - events relating to ads served on your end users, such as the number of ads displayed to your end users and whether you clicked on an ad; and
- Inferences (not actual data), but conclusions drawn by the client using it's own technologies to deduce profiles of customers, for example, if the end user clicks on an expensive pink pair of shoes, the client may deduct that the clients income is substantial, and they like pink shoes.

Recipients of the Data

Ve Group Members (covered by a group data sharing agreement).

Ve Global UK Limited

Privacy@ve.com

Contact Point – Importer (Client)

See Insertion Order

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be agreed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Client Privacy Policy.

SECTION 2

Standard Contractual Clauses – Client/Customer (Exporter) – transferring data to Ve Global UK (Importer)

COMMISSION DECISION

of 27 December 2004

amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries

(notified under document number C(2004) 5271)

(Text with EEA relevance)

(2004/915/EC)

ANNEX

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

Client

hereinafter “data exporter”

and

Ve Global UK Limited (Company No. 10706696) whose registered office is at 77 Leadenhall Street London EC3A 3DE, England

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

(a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) “the data exporter” shall mean the controller who transfers the personal data;

(c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

(d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or

supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions [(1)] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data [(2)], or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects:

Initials of data importer:_;

(i) It will not disclose or transfer the personal data to a third-party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third-party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third-party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third-party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third-party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

(Annex A)

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

(Annex B)

DESCRIPTION OF THE TRANSFER

Ve Global embeds is JavaScript code, and uses both local storage and cookies in order to collect data from client's website users. Ve then uses this data to track the user and provide services such as advertising and emails.

Data Subjects

1. End users who visit client's websites.
2. Ve's employee contact details, in the course of running the business activities.

Purposes of the transfer

The purpose of this is to assist clients with advertising and selling their merchandise. This can be through advertising, email services, and onsite messaging and interactions.

Categories of Data

- email addresses and/or telephone numbers, if voluntarily entered into a Client Site (e.g. to buy a product or service, become a registered user, or sign up for marketing communications) ("**Contact Details**");
- data relating to browsing activity through the use of cookies, web beacons and pixel tags and similar technologies deployed on Client Sites or via emails sent by Ve on behalf of Clients ("**Behavioural Data**"); including:
    - IP (internet protocol) address; referring site URL (website address) where a session started, and details about a device, including type (e.g. mobile or tablet), brand, model, operating system name and version, browser name, version, language and protocol, and other unique numbers assigned to a device (e.g. IDFA on iPhone, Google adID on Android);
    - details about the pages of Client Sites visited and activities on Client Sites (e.g. products viewed or purchased, including details of purchases made and the time and duration of visits to pages of the Client's Site), page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page;
    - using an IP address, geolocation (e.g. postcode);
    - events relating to ads served, such as the number of ads displayed and whether an end user clicked on an ad; and
- mailing address, age and/or date of birth, gender, marital status, number of children, nationality and/or country or city of residency, telephone number and first name, in each case if input into a Client Site ("**Profile Data**").

Recipients or categories of recipients of the Data

Processors

- Microsoft Azure - Infrastructure and hosting
- Google – Infrastructure and hosting
- Freshworks – CRM ticketing system
- Ve Group Members – processing of data to enable the business to run efficiently
- Hubspot – CRM system
- Juice Tactics – CRM system
- Plain Concepts – CRM system
- Converygtics – Analytics
- Cloud Technology Solutions Ltd – Analytics
- Ve Global Group Members (where acting as a Processor)

Controllers

- Ve Global Group Members (covered by a Group Data Sharing Agreement)

Contact Points – Exporter Client

See Insertion Order

Contact Points – Importer VE Global Group Member

Privacy@ve.com

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be agreed by the parties.

Description of the technical and organisational security measures implemented by the data importer (this appendix if for use when Client/Customer transfers data to Ve Global UK)in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. INTRODUCTION

This policy sets set out a framework of governance and accountability for Information Security Management across the organisation. It forms the basis of the Information Security Management System (ISMS) and incorporates all policies and procedures that are required to protect company information by maintaining:

Confidentiality: protecting information from unauthorised access and disclosure.

Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion.

Availability: ensuring that information and associated services are available to authorised users whenever and wherever required.

This policy framework aims to develop a positive culture of information security throughout VE.

1.1 Document Definition

This document is a **Policy**.

For a complete list of all permitted document labels see *VE-PR-XX-IS-0002-Document Management Procedure* document. Please note these are the labels are permitted for document assets.

Policies, Standards and Procedures are the primary way in which the Information Security Steering Committee's (ISSC) direction and expectations are translated into specific, measurable, and testable goals and objectives. They are a critical component of governance at Ve Global (Ve) as they provide the structure and rules around which the organisation must operate. The Information Security Governance Committee (ISGC) has been established to create, maintain, and govern Information Security (IS) Policies, Standards and Procedures. The ISGC is responsible for communicating these documents to all applicable partners, joint ventures and subsidiaries, as well as distributing them and/or making them accessible to Ve's Employees (including consultants, contractors, and other applicable 3rd party vendors and partners).

1.2 Objective

The main objectives of this Policy are as follows:

1. Implement good practice in accordance with ISO 27001;
2. Protect against the potential consequences of security breaches;
3. Make certain that users are aware of and comply with all current and relevant legislation;
4. Increase security awareness and understanding across the organisation on the need for good information management, and of the direct responsibilities of every member for protecting data;
5. Promote information security practices that enhance the reputation of the organisation as a trustworthy, open, honest and ethical organisation;
6. Protect Ve Global from liability or damage through the misuse of data managed within the organisation.

In addition, the aim of the Ve's Information Security Policy Framework is to provide the foundation for all documentation and operational processes developed to protect information or data assets (used interchangeably from this point forward) owned by, or in the custody of, Ve from:

(a) Unauthorised disclosure – loss of CONFIDENTIALITY;

(b) Unauthorised or unintended modification – loss of INTEGRITY;

(c) Unintended loss of availability – loss of AVAILABILITY.

The Ve's Information Security Program supports the ISSC's objectives by providing the guidance and means to protect data assets. The Information Security Program includes maintaining Policies, Standards, and Procedures in areas including (but not limited to), internal and external risk management, threat and vulnerability management, logical and physical security, and mapping of Information Security (IS) responsibilities.

1.3 Scope

Applicability to Employees

Ve refers to Ve Global as well as its applicable partners, joint ventures and subsidiaries (where applicable). This Policy applies to all Employees, members of the Board of Directors, and all consultants and contractors.

Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

Applicability to Assets

This Policy applies to all information assets globally owned by Ve, or where Ve has custodial responsibilities.

2. POLICY STATEMENTS

2.1 Protection of Data

It is the Policy of Ve that information in all its forms: written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

2.2 Requirement for Policy Documentation

All supporting Policies, Standards, and Procedures must be documented and must be made available to individuals responsible for their implementation and compliance. All activities identified by the Policies, Standards and Procedures must also be documented.

2.3 Regional Variances

Where appropriate, regional variances to this Policy can be permitted to address all local legal and regulatory requirements. All such Policies, Standards, and Procedures are subordinate to, and must be consistent with, this Policy, and must be approved by the ISGC and signed off by the CEO.

See section 2.8 2.8 Policy **Exceptions** for more information.

2.4 Compliance with Policy Provisions

All processes and systems implemented after the effective date of these policies are expected to comply with the provisions of this Policy. Existing systems are expected to be brought into compliance as soon as practical.

2.5 Policy & Standard Review Period

All documentation must be reviewed at least yearly, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape. Alternative review timings to be determined by the ISGC where applicable.

2.6 Independent Review of the Information Security Program

The ISGC or the ISSC must initiate and independent review of all relevant aspects of the Ve Information Security Program at least annually, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape to ensure the continuing suitability, adequacy and effectiveness of the organisation's approach to managing inherent risks.

The review must:

a) Assess opportunities for improvement and the need for changes to the approach to security, including the Policy, Standards and/or control objectives;

b) Be carried out by individuals independent of the area under review. These individuals can be internal or third parties, but must demonstrate that they have appropriate skills and experience;

c) Be recorded and reported to the ISGC or the ISSC as appropriate. These records must be maintained, and;

d) Provide recommendations for corrective actions.

2.7 Information Security Roles & Responsibilities

All employees, members of the Board of Directors, and all consultants and contractors (where applicable) have responsibilities towards Ve Information Security that they must abide by.

To better establish Ve's Information Security Management System (ISMS), specific Information Security responsibilities are segregated between the ISSC and the ISGC.

The ISSC consists of top management and heads of departments who review and set key Information Security objectives in accordance to legislation, regulations, best practice and contractual obligations.

The ISGC consists of key points of contact from each department that are responsible for implementing controls and strategies to ensure that Information Security objectives are met and adhered to by the business.

For a comprehensive structure of Ve's Information Security responsibilities, refer to the Information Security Roles and Responsibilities standard.

2.8 Policy Exceptions

In the event that a business area or department is unable to comply with an approved Policy or Standard, an exception may be requested and submitted to the Policy Coordinator for initial review and onward presentation with recommendations to the ISGC and other interested parties.

An exception also allows for non-compliance with a Policy or Standard for either an approved period, or indefinitely. This can be caused by technical limitations within an application or system or may be a result of a fundamental change to a business process or be in-line with specific business goals. In the case of an exception, a member of the ISSC must formally accept the risk and retain accountability for non-compliance.

Refer to the policy exception procedure for further information.

2.9 Change Management

Any changes to the organisation, business processes, information processing facilities or systems that affect information security must be controlled.

The following change controls must be in place for any major change requests:

- description of change including designation of importance (e.g. minor, or major change);
- planning and testing of change(s);
- assessment of the potential impacts, including information security impacts, of such changes;
- formal approval procedure;
- verification that information security requirements have been met;
- communication of change details to all relevant persons;
- fail-back procedure or equivalent, and;
- description of audit capability and audit trail retention.

All relevant documentation must be updated as a result of any changes to Ve's systems.

2.10 Capacity Management

A documented capacity management plan must be documented for critical information systems.

The plan should include:

- System tuning and monitoring parameters;
- Detective controls to alert on threats to production systems;
- Projections of future capacity requirements.

2.11 Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of Ve's assets.

Where this is not possible, detailed mitigating controls must be prepared and approved as a Policy Exception by Ve's Information Security Team (IST).

Where practical, the initiation of an event should be separate from the authorisation.

The possibility of collusion must be considered in the design and implementation of information security controls.

2.12 Information Security in Project Management

Information security must be built into the Ve project management method to ensure that information security risks are identified and addressed as part of each project as a company-wide practice.

The following requirements will be integral to all project plans:

- Information security objectives are included;
- An information security risk assessment is conducted;
- Information security is part of all phases;
- Information security implications should be reviewed regularly in all projects, and;
- Responsibilities for information security should be defined and allocated to specified roles defined in the project management method.

2.13 Delegation of Information Security Tasking

Any individual with information security responsibilities may delegate to others, but the overarching accountability must reside with the original individual.

Where data that is classified higher than **Restricted** may be at risk, permission to delegate must be received from the Data Owner.

3. Policy Compliance

3.1 Compliance Measures

Compliance with this Policy Framework is enforced through the validation of Compliance Measures relevant to each individual Policy and Standard derived from it.

3.2 Enforcement

As noted above, this Policy applies to all Ve Global Members, members of the Board of Directors, and all consultants, third parties and contractors (where deemed necessary). Violations of this Policy may result in disciplinary action, up to and including termination of employment and / or legal action.

Schedule 2

DATA PROCESSING AGREEMENT

This Data Protection Addendum ("Agreement") reflects the Supplier's services entered into between Supplier Ve Global UK Limited and Customer; with respect to the terms governing the processing of personal data under the Framework Terms.

This Data Protection Addendum is referred to and forms an integral part of the applicable Ve Global UK Limited Framework Terms. It is effective upon acceptance of the Framework Terms.

Where personal data processed under the Framework Terms is subject to Applicable Data Protection Law, Clients/Customers may enter into this Data Protection Addendum (which incorporates the European Commission's 2010/87/EU Standard Contractual Clauses attached hereto as Annex C): (i) to protect the personal data in accordance with the requirements of Applicable Data Protection Law; and (ii) to provide appropriate safeguards with respect to personal data which may be processed outside of the European Territories.

1. DEFINITIONS

1.1 The following definitions shall apply to this Agreement:

"Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer" take the meaning given in the GDPR;

"Data Loss Event" means any event that results, or may result, in unauthorised or unlawful access to Personal Data held by the Supplier under this Agreement and controlled by the Controller, and/or actual or potential loss and/or destruction of, or damage to Personal Data in breach of this Agreement, including any Personal Data Breach;

"Data Protection Impact Assessment" means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

"Data Protection Legislation" means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 subject to royal consent to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;

"Data Subject Access Request" means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data to the extent that such Personal Data controlled by the Controller;

"DPA 2018" means Data Protection Act 2018;

"Framework Terms" means the applicable Ve framework terms entered into between the Supplier and the Customer;

"Law" means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the a Party (as applicable) is bound to comply;

"LED" means Law Enforcement Directive (Directive (EU) 2016/680);

"Party" means a Party to this Agreement;

“Protective Measures” means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it; and

“Sub-processor” means any third Party appointed to process Personal Data on behalf of the Supplier related to this Agreement.

“Supplier Personnel” means all directors, officers, employees, agents, consultants and suppliers of the Supplier and/or of any sub-supplier engaged in the performance of its obligations under this Agreement;

2. DATA CONTROLLER OBLIGATIONS

2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor. Supplier shall only process data: (i) in accordance with this Agreement (including Annex A) or any further instructions from Customer; and (ii) only to the extent, and in such a manner, as is necessary for the purposes of this Agreement and/or the Framework Terms. The Supplier shall not have the right to determine the processing.

2.2 The Supplier shall notify the Customer if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

2.3 The Supplier shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:

2.3.1 a systematic description of the envisaged processing operations and the purpose of the processing;

2.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

2.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

2.4 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

2.4.1 process that Personal Data only in accordance with this Agreement (including Annex A) or any further instructions from Customer, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;

2.4.2 ensure that it has in place Protective Measures, to protect against a Data Loss Event having taken account of the:

(a) nature of the data to be protected;
(b) harm that might result from a Data Loss Event;
(c) state of technological development; and
(d) cost of implementing any measures;

2.4.3 ensure that:

(a) the Supplier Personnel do not process Personal Data except in accordance with this Agreement (and in particular Annex A) or any further instructions from Customer;
(b) it takes reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:

i. are aware of and comply with the Supplier's duties under this clause 2;
ii. are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
iii. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Agreement; and
iv. have undergone adequate training in the use, care, protection and handling of Personal Data

2.4.4 at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Framework Terms unless the Supplier is required by Law to retain the Personal Data.

2.5 Subject to clause 2.6, the Supplier shall notify the Customer if it:

2.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

2.5.2 receives a request to rectify, block or erase any Personal Data;

2.5.3 becomes aware of a Data Loss Event.

2.6 The Supplier's obligation to notify under clause 2.5 shall include the provision of further information to the Customer in phases, as details become available.

2.7 Taking into account the nature of the processing, the Supplier shall provide the Customer with reasonable assistance where necessary in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 2.5 (and insofar as possible within the timescales reasonably required by the Customer) including by providing:

2.7.1 the Customer with full details and copies of the complaint, communication or request;

2.7.2 such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

2.7.3 the Customer, at its reasonable request, with any Personal Data it holds in relation to a Data Subject;

2.7.4 assistance as reasonably requested by the Customer following any Data Loss Event; and

2.7.5 assistance as reasonably requested by the Customer with respect to any request received by Customer from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.

2.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this clause 2 and shall make available to Customer all information necessary to demonstrate compliance with Article 28 of the GDPR. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

2.7.6 the Customer determines that the processing is not occasional;

2.7.7 the Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

2.7.8 the Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

2.8 The Supplier shall allow for audits of its Data Processing activity by the Customer or the Customer's designated auditor.

2.9 The Supplier shall designate a data protection officer if required by the Data Protection Legislation.

2.10 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Supplier must:

2.10.1 notify the Customer in writing of the intended Sub-processor and processing;

2.10.2 obtain the written consent of the Customer;

2.10.3 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this clause 2 (such that they apply to the Sub-processor); and

2.11 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

2.12 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. Either Party may on not less than 30 Working Days' notice to the other Party amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

2.13 The Supplier shall not transfer the personal data outside the European Economic Area without:

2.13.1 the prior written consent of Customer, which can be withheld at the sole discretion of Customer, and subject to any additional Customer requirements (which may include entering into or procuring that the relevant Sub processor enter into the standard contractual clauses attached hereto as Annex C for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU in their entirety for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection; or

2.13.2 any other permitted measure as described in article 46 of regulation EU 2016/679

3. DATA PROTECTION WARRANTIES, INDEMNITIES AND SURVIVAL

3.1 Notwithstanding any other provision of this Agreement, the Parties warrant that, upon receipt of Personal Data, each shall duly observe all its obligations as a Data Controller and/or Data Processor under the DPA 2018 and the GDPR, which arise in connection with the Processing and the performance of its respective rights and obligations under this Agreement.

3.2 The provisions of this Agreement are expressly agreed by the Parties to survive any termination of this Agreement, howsoever arising.

3.3 The terms contained in this Agreement shall be governed by the laws of England and the parties hereby submit to the exclusive jurisdiction of the English Courts.

Annex A – PUX Products

Details of Data Processing

1. The Supplier shall comply with any further written instructions with respect to processing of personal data.
2. Any such further instructions shall be incorporated into this Annex.

Description	Details
Subject matter of the processing	To provide onsite technology via first party cookies to personalise an end users' online experiences.
Duration of the processing	Usually no more than 90 days.
Nature and purposes of the processing	Tracking a user's behaviour online, in order to customise the web page to suit their interests. This involves collecting data via cookies and similar technologies.
Type of Personal Data	Data relating to your end users' browsing activity through the use of cookies and similar technologies deployed on Client Sites ("Behavioural Data"), including: IP (internet protocol) address; and details about devices, including type (e.g. mobile or tablet), brand, model, operating system name and version, browser name, version, language and protocol, and other unique numbers assigned to a device (e.g. IDFA on iPhone, Google adID on Android); and Details about the pages of Client Site visited and activities on Client Site (e.g. products viewed or purchased, including details of purchases made and the time and duration of visits to pages of the Client's Site), page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.
Categories of Data Subject	End users who visit your website. Employee contact details in the context of our contact with you.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Within 90 days of the contract termination, or sooner if requested.

Annex B

Email Remarketing (Basket Abandonment & other emails and onsite messaging and interactions sent on your behalf)

Details of Data Processing

1. The Supplier shall comply with any further written instructions with respect to processing of personal data.
2. Any such further instructions shall be incorporated into this Annex.

Description	Details
Subject matter of the processing	To provide onsite collection of personal data for customers that enter items in their basket but do not actually buy and submit.
Duration of the processing	Usually no more than 90 days.
Nature and purposes of the processing	Tracking a user's behaviour online in order to customise the web page to suit their interests. This involves collecting data via cookies and similar technologies.
Type of Personal Data	Data relating to your end users browsing activity through the use of cookies and similar technologies deployed on Client Sites ("Behavioural Data"), including: IP (internet protocol) address; and details about their devices, including type (e.g. mobile or tablet), brand, model, operating system name and version, browser name, version, language and protocol, and other unique numbers assigned to a device (e.g. IDFA on iPhone, Google adID on Android); Details about the pages of Client Site visited and activities on Client Site (e.g. products viewed or purchased, including details of purchases made and the time and duration of visits to pages of the Client's Site), page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page; Email addresses and/or telephone numbers, name and address, if voluntarily entered into a Client Site (e.g. to buy a product or service, become a registered user, or sign up for marketing communications) ("**Contact Details**"); and Age and/or date of birth, gender, marital status, number of children, nationality and/or country or city of residency.
Categories of Data Subject	End users who visit your website. Employee contact details in the nature of our contact with you.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under	Within 90 days of the contract termination, or sooner if requested.

union or member state law to preserve that type of data	

ANNEX C

Standard Contractual Clauses – Controller to Processor (to be signed if the contracting Ve Group Member (Importer) is outside the EEA, or is the UK when planning for Bexit and the UK as a third country)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Client

(the data exporter)

And

(the data importer)

Ve Global UK Limited, 77 Leadenhall Street London EC3A 3DE

Privacy@ve.com 020 3137 5730

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

CLAUSE 1: DEFINITIONS

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [(1)];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data

exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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, namely …

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: SUB-PROCESSING

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses [3]. Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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, namely …

4. The data exporter shall keep a list of sub-processing 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 sub-processor 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 sub-processor 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.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

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

Data collected by cookies and similar technologies for the provision of one or both of the following services:

1. PUX
2. Email services and onsite messages and interactions

Data importer

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

To process the data to provide the services above

Data subjects

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

1. End users who visit websites
2. Employees as part of providing the services

Categories of data

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

Data relating to your browsing activity through the use of cookies and similar technologies deployed on Client Sites ("**Behavioural Data**"), including:

IP (internet protocol) address and details about an end user's device, including type (e.g. mobile or tablet), brand, model, operating system name and version, browser name, version, language and protocol, and other unique numbers assigned to a device (e.g. IDFA on iPhone, Google adID on Android); and

Details about the pages of Client Site visited and activities on Client Site (e.g. products viewed or purchased, including details of purchases made and the time and duration of visits to pages of the Client's Site), page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.

<u>Email services only</u>

Email addresses and/or telephone numbers, name and address, if voluntarily entered into a Client Site by an end user (e.g. to buy a product or service, become a registered user, or sign up for marketing communications) ("**Contact Details**");

Processing operations

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

Collection of the data by way of it being transferred to the importer by cookies and similar technologies, including JavaScript, and processing the data to deliver onsite experiences to the end user, or emails to the user based on visits to the website.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. INTRODUCTION

This policy sets set out a framework of governance and accountability for Information Security Management across the organisation. It forms the basis of the Information Security Management System (ISMS) and incorporates all policies and procedures that are required to protect company information by maintaining:

Confidentiality: protecting information from unauthorised access and disclosure.

Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion.

Availability: ensuring that information and associated services are available to authorised users whenever and wherever required.

This policy framework aims to develop a positive culture of information security throughout VE.

1.1 Document Definition

This document is a **Policy**.

For a complete list of all permitted document labels see *VE-PR-XX-IS-0002-Document Management Procedure* document. Please note these are the labels are permitted for document assets.

Policies, Standards and Procedures are the primary way in which the Information Security Steering Committee's (ISSC) direction and expectations are translated into specific, measurable, and testable goals and objectives. They are a critical component of governance at Ve Global (Ve) as they provide the structure and rules around which the organisation must operate. The Information Security Governance Committee (ISGC) has been established to create, maintain, and govern Information Security (IS) Policies, Standards and Procedures. The ISGC is responsible for communicating these documents to all applicable partners, joint ventures and subsidiaries, as well as distributing them and/or making them accessible to Ve's Employees (including consultants, contractors, and other applicable 3rd party vendors and partners).

1.2 Objective

The main objectives of this Policy are as follows:

1. Implement good practice in accordance with ISO 27001;
2. Protect against the potential consequences of security breaches;
3. Make certain that users are aware of and comply with all current and relevant legislation;
4. Increase security awareness and understanding across the organisation on the need for good information management, and of the direct responsibilities of every member for protecting data;
5. Promote information security practices that enhance the reputation of the organisation as a trustworthy, open, honest and ethical organisation;
6. Protect Ve Global from liability or damage through the misuse of data managed within the organisation.

In addition, the aim of the Ve's Information Security Policy Framework is to provide the foundation for all documentation and operational processes developed to protect information or data assets (used interchangeably from this point forward) owned by, or in the custody of, Ve from:

(a) Unauthorised disclosure – loss of CONFIDENTIALITY;

(b) Unauthorised or unintended modification – loss of INTEGRITY;

(c) Unintended loss of availability – loss of AVAILABILITY.

The Ve's Information Security Program supports the ISSC's objectives by providing the guidance and means to protect data assets. The Information Security Program includes maintaining Policies, Standards, and Procedures in areas including (but not limited to), internal and external risk management, threat and vulnerability management, logical and physical security, and mapping of Information Security (IS) responsibilities.

1.3 Scope

Applicability to Employees

Ve refers to Ve Global as well as its applicable partners, joint ventures and subsidiaries (where applicable). This Policy applies to all Employees, members of the Board of Directors, and all consultants and contractors.

Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

Applicability to Assets

This Policy applies to all information assets globally owned by Ve, or where Ve has custodial responsibilities.

2. POLICY STATEMENTS

2.1 Protection of Data

It is the Policy of Ve that information in all its forms: written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

2.2 Requirement for Policy Documentation

All supporting Policies, Standards, and Procedures must be documented and must be made available to individuals responsible for their implementation and compliance. All activities identified by the Policies, Standards and Procedures must also be documented.

2.3 Regional Variances

Where appropriate, regional variances to this Policy can be permitted to address all local legal and regulatory requirements. All such Policies, Standards, and Procedures are subordinate to, and must be consistent with, this Policy, and must be approved by the ISGC and signed off by the CEO.

See section 2.8 2.8 Policy **Exceptions** for more information.

2.4 Compliance with Policy Provisions

All processes and systems implemented after the effective date of these policies are expected to comply with the provisions of this Policy. Existing systems are expected to be brought into compliance as soon as practical.

2.5 Policy & Standard Review Period

All documentation must be reviewed at least yearly, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape. Alternative review timings to be determined by the ISGC where applicable.

2.6 Independent Review of the Information Security Program

The ISGC or the ISSC must initiate and independent review of all relevant aspects of the Ve Information Security Program at least annually, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape to ensure the continuing suitability, adequacy and effectiveness of the organisation's approach to managing inherent risks.

The review must:

a) Assess opportunities for improvement and the need for changes to the approach to security, including the Policy, Standards and/or control objectives;

b) Be carried out by individuals independent of the area under review. These individuals can be internal or third parties, but must demonstrate that they have appropriate skills and experience;

c) Be recorded and reported to the ISGC or the ISSC as appropriate. These records must be maintained, and;

d) Provide recommendations for corrective actions.

2.7 Information Security Roles & Responsibilities

All employees, members of the Board of Directors, and all consultants and contractors (where applicable) have responsibilities towards Ve Information Security that they must abide by.

To better establish Ve's Information Security Management System (ISMS), specific Information Security responsibilities are segregated between the ISSC and the ISGC.

The ISSC consists of top management and heads of departments who review and set key Information Security objectives in accordance to legislation, regulations, best practice and contractual obligations.

The ISGC consists of key points of contact from each department that are responsible for implementing controls and strategies to ensure that Information Security objectives are met and adhered to by the business.

For a comprehensive structure of Ve's Information Security responsibilities, refer to the Information Security Roles and Responsibilities standard.

2.8 Policy Exceptions

In the event that a business area or department is unable to comply with an approved Policy or Standard, an exception may be requested and submitted to the Policy Coordinator for initial review and onward presentation with recommendations to the ISGC and other interested parties.

An exception also allows for non-compliance with a Policy or Standard for either an approved period, or indefinitely. This can be caused by technical limitations within an application or system or may be a result of a fundamental change to a business process or be in-line with specific business goals. In the case of an exception, a member of the ISSC must formally accept the risk and retain accountability for non-compliance.

Refer to the policy exception procedure for further information.

2.9 Change Management

Any changes to the organisation, business processes, information processing facilities or systems that affect information security must be controlled.

The following change controls must be in place for any major change requests:

- description of change including designation of importance (e.g. minor, or major change);
- planning and testing of change(s);
- assessment of the potential impacts, including information security impacts, of such changes;
- formal approval procedure;
- verification that information security requirements have been met;
- communication of change details to all relevant persons;
- fail-back procedure or equivalent, and;
- description of audit capability and audit trail retention.

All relevant documentation must be updated as a result of any changes to Ve's systems.

2.10 Capacity Management

A documented capacity management plan must be documented for critical information systems.

The plan should include:

- System tuning and monitoring parameters;
- Detective controls to alert on threats to production systems;
- Projections of future capacity requirements.

2.11 Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of Ve's assets.

Where this is not possible, detailed mitigating controls must be prepared and approved as a Policy Exception by Ve's Information Security Team (IST).

Where practical, the initiation of an event should be separate from the authorisation.

The possibility of collusion must be considered in the design and implementation of information security controls.

2.12 Information Security in Project Management

Information security must be built into the Ve project management method to ensure that information security risks are identified and addressed as part of each project as a company-wide practice.

The following requirements will be integral to all project plans:

- Information security objectives are included;
- An information security risk assessment is conducted;
- Information security is part of all phases;
- Information security implications should be reviewed regularly in all projects, and;
- Responsibilities for information security should be defined and allocated to specified roles defined in the project management method.

2.13 Delegation of Information Security Tasking

Any individual with information security responsibilities may delegate to others, but the overarching accountability must reside with the original individual.

Where data that is classified higher than **Restricted** may be at risk, permission to delegate must be received from the Data Owner.

3. Policy Compliance

3.1 Compliance Measures

Compliance with this Policy Framework is enforced through the validation of Compliance Measures relevant to each individual Policy and Standard derived from it.

3.2 Enforcement

As noted above, this Policy applies to all Ve Global Members, members of the Board of Directors, and all consultants, third parties and contractors (where deemed necessary). Violations of this Policy may result in disciplinary action, up to and including termination of employment and / or legal action.

ANNEX D – LIST OF APPROVED SUB PROCESSORS

- Microsoft Azure - Infrastructure and hosting
- Google – Infrastructure and hosting
- Freshworks – CRM ticketing system
- Ve Group Members – processing of data to enable the business to run efficiently
- Hubspot – CRM system (ending early 2020)(
- Juice Tactics – CRM system
- Plain Concepts – CRM system
- Converygtics – Analytics
- Cloud Technology Solutions Ltd – Analytics
- Praect – Microsoft Dynamics (Jan 2020)

An updated list to be provided online as part of our guidance (link to be provided shortly)