

## Data Processing Agreement

This Data Processing Addendum ("DPA") supplements our Terms of use (TOU) as updated from time to time between you (together with subsidiary(ies) and affiliated entities, collectively, "Customer") and The FIA (hereinafter collectively referred to as "Parties" and individually "Party") when the GDPR applies to the Customer's use of The FIA's Services to process Customer data.

This DPA is effective from the date the Customer agrees with the terms and conditions of the FIA nurture product. If there is any conflict between this DPA and our GDPR terms, the relevant terms of this DPA take precedence.

### 1. Definitions

1.1. "Account Data" means information about the Customer that the Customer provides to the FIA in connection with the creation or administration of one of its customers when they enter the nurture journey. The Customer shall ensure that all Account Data is current and accurate at all times during the term of the TOU.

1.2. "Authorized User" means an individual employee, agent or contractor of the Customer for whom subscriptions to Services have been granted pursuant to the terms of the TOU.

1.3. "Customer Credentials" means access passwords, keys or other credentials used by the Customer in connection with the Services.

1.4. "Customer Data" means any Personal Data that the FIA Processes on behalf of the Customer as a Data Processor in the course of providing its Services.

1.5. "Data Controller" means an entity that determines the purposes and means of the Processing of Personal Data.

1.6. "Data Processor" means an entity that Processes Personal Data on behalf of a Data Controller.

1.7. "Data Protection Laws" means all data protection and privacy laws and regulations of the EU, EEA and their member states, applicable to the Processing of Personal Data.

1.8. "Data Subject" means the identified or identifiable person to whom Personal Data relates.

1.9. "EEA" means the European Economic Area, the United Kingdom, and Switzerland.

1.10. "EU" means the European Union.

1.11. "GDPR" means the Regulation (EU) 2016/679 of the European Parliament and 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).

1.12. "Personal Data" means any information relating to an identified or identifiable natural person as defined in the GDPR.

1.13. "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. "Process", "Processes" and "Processed" shall be interpreted accordingly.

1.14. "Processor" means a natural or legal person, public authority, agency, or any other body which Processes Personal Data on behalf of the Data Controller.

1.15. "SCC" means the standard contractual clauses as approved by the European Commission.

1.16. "Services" means any product or service provided by the FIA pursuant to the FIA's TOU.

1.17. "Sub-Processor" means any third-party Processor engaged by the FIA.

## **2. Scope and Roles**

2.1. The FIA has agreed to enter into this DPA based on the Customer's belief that Customer Data may include Personal Data that originates from EU/EEA and/or that is otherwise subject to the GDPR. Accordingly, this DPA supplements the TOU and applies exclusively to the FIA's Processing of Customer Data in providing Services under the TOU to the Customer.

2.2. The FIA agrees to comply with the following provisions with respect to any Personal Data Processed for the Customer in connection with the provision of the Services.

2.3. The Parties agree that with regard to the Processing of Personal Data, the Customer is the Data Controller and The FIA is a Data Processor, acting on behalf of the Customer, as further described in Annex 1 ("*Details of Data Processing*") of this DPA. Each Party will comply with its respective obligations under EU Data Protection Law.

## **3. Customer's Processing of Personal Data**

3.1. The Customer is responsible for the control of Personal Data and must comply with its obligations as a Data Controller under Data Protection Laws, in particular for justification of any transfer of Customer Data to The FIA and its decisions and actions regarding the Processing and use of Personal Data.

3.2. The Customer agrees that it has provided notice and received all consents and rights necessary under Data Protection Laws for the FIA to Process Customer Data and provide the Services.

#### **4. The FIA's Processing of Customer Data**

4.1. By entering into this DPA, the Customer instructs the FIA to Process Customer Data to provide the Services in accordance with the features and functionality of the Services (Post Sale nurture program)

4.2. In connection with the FIA's delivery of the Services to the Customer, the FIA shall Process certain categories and types of the Customer data, only for the purposes described in this DPA and only in accordance with the Customer's documented lawful instructions, including with regard to transfers of Customer data to a third country or an international organization, unless required to do so by EU or Member State of the EU law to which the FIA is subject. In such a case, the FIA shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

4.3. The Parties agree that this DPA sets out the Customer's complete and final instructions to the FIA in relation to the Processing of Customer Data. The Processing outside the scope of these instructions shall require a prior written agreement between Customer and the FIA. Notwithstanding the foregoing, the FIA will inform the Customer promptly if it becomes aware that the Customer's instructions may violate applicable EU Data Protection Law.

#### **5. Customer Responsibilities and Restrictions**

5.1. Without limiting its responsibilities under the TOU, the Customer is solely responsible for: (a) Account Data, Customer Data and Customer Credentials (including activities conducted with Customer Credentials), subject to the FIA's Processing obligations under the TOU and this DPA; (b) providing any notices required by EU Data Protection Law to, and receiving any required consents and authorizations required by EU Data Protection Law from, persons whose Personal Data may be included in Account Data, Customer Data or Customer Credentials; and (c) ensuring no Personal Data relating to criminal convictions and offenses (GDPR Article 10) are submitted for Processing by the Services.

#### **6. Security**

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, the FIA shall in relation to Customer Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk (including those outlined in Annex 2, "*Security Measures*"). In assessing the appropriate level of security, the FIA shall take into account the risks that are presented by Processing Customer Data including, in particular, the risks presented by a Customer Data Breach (as defined in Section 10). The FIA

may make such changes to the Security Measures as the FIA deems necessary or appropriate from time to time, including without limitation to comply with applicable law, but no such changes will reduce the overall level of protection for Customer Data. The FIA will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-Processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to Process Customer Data have agreed to appropriate obligations of confidentiality.

6.2. The Parties shall take steps to ensure that any natural person acting under the authority of the Customer or the FIA who has access to Personal Data does not Process them except on instructions from the Customer, unless he or she is required to do so by EU or EU Member State law.

6.3. The Customer is responsible for reviewing the information made available by the FIA relating to its data security and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations under Data Protection Laws. The Customer acknowledges that the FIA may update or modify the FIA's security standards from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

6.4. The Customer agrees it is responsible for its secure use of the Services, including securing its Customer Credentials, protecting the security of Customer Data when in transit to and from the Services, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

## **7. Sub-Processors**

7.1. The Customer acknowledges and agrees that the FIA may engage third-party Sub-Processors in connection with the provision of Services, and hereby consents to the FIA's use of Sub-Processors. As a condition to permitting a third-party Sub-Processor to Process Customer Data, the FIA will enter into a written agreement with the Sub-Processor containing data protection obligations no less protective than those in this DPA with respect to Customer Data. The FIA will restrict its Sub-Processors' access to only what is necessary to maintain the Services or to provide the Services to Customers. Subject to this Section 7, the FIA reserves the right to engage and substitute Sub-Processors as it deems appropriate, but shall: (a) remain responsible to the Customer for the provision of the Services and (b) be liable for the actions and omissions of its Sub-Processors undertaken in connection with the FIA's performance of this DPA to the same extent the FIA would be liable if performing the Services directly.

7.2. Upon the Customer's request by email to [email@thefia.co.uk](mailto:email@thefia.co.uk), the FIA will provide the Customer with a list of then-current third-party Sub-Processors and the nature of the services they provide. The Customer can find an up-to-date list of Sub-Processors in Annex 3 of this DPA. The Customer may object to any new Sub-Processor on reasonable legal grounds (the "Objection Notice") relating to the protection of the Customer Data, in which case the FIA shall have the right to satisfy the objection through one of the following:

- (a) the FIA will cancel its plans to use the Sub-Processor with regard to Customer Data or will offer an alternative to provide the Services without such Sub-Processor;
- (b) the FIA will take the corrective steps requested by the Customer in its Objection Notice (which removes the Customer's objection) and proceed to use the Sub-Processor with regard to Customer Data; or
- (c) the FIA may cease to provide, or the Customer may agree not to use (temporarily or permanently), the particular aspect of the Services that would involve the use of such Sub-Processor with regard to Personal Data, subject to a mutual agreement of the Parties to adjust the remuneration for the Services considering their reduced scope.

7.3. All Objection Notices under Section 7.2 must be submitted by email to the FIA at [email@thefia.co.uk](mailto:email@thefia.co.uk). If none of the options outlined in Clause (a), (b) or (c) of Section 7.2 are reasonably available and Customer's objection has not been resolved to the Parties' mutual satisfaction within 30 days of the FIA's receipt of the Objection Notice, either Party may terminate the affected Services and the FIA will refund to the Customer a pro rata share of any unused amounts prepaid by the Customer. The refund will be calculated in proportion to what Services have been provided until the time the Customer has informed the FIA on terminating the Services. the FIA does not provide any refunds if the Objection Notice does not have reasonable legal grounds.

## **8. Data Subject Rights**

8.1. If the FIA receives a request from a Data Subject in relation to the Customer Data then, to the extent legally permissible, the FIA will advise the Data Subject to submit their request to the Customer and the Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services. The Customer hereby agrees that the FIA may confirm to a Data Subject that his or her requests relate to the Customer. To the extent the Customer is unable through its use of the Services to address a particular Data Subject request, the FIA will, upon the Customer's request and taking into account the nature of Customer Data Processed, provide reasonable assistance in addressing the Data Subject request (provided the FIA is legally permitted to do so and that the Data Subject request was made in accordance with EU Data Protection Law).

To the extent permitted by applicable law, the Customer shall be responsible for any costs arising from the FIA's provision of such assistance.

## **9. Deletion Upon Expiration**

9.1. Upon termination of the TOU and/or DPA, the FIA will initiate a process upon the Customer's written request that deletes Customer Data in its possession or control. This requirement shall not apply to the extent the FIA is required by the applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data the FIA shall securely isolate and protect from any further processing, except to the extent required by applicable law.

## **10. Customer Data Breach Management**

10.1. the FIA will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach with respect to Customer Data transmitted, stored or otherwise Processed by the FIA or its Sub-Processors (a "*Customer Data Breach*"). Such notice may be provided (1) by posting a notice in the Services; (2) by sending an email to the email address from which the account of Authorized User was created; and/or (3) pursuant to the notice provisions of the TOU. The Customer shall ensure that its contact information is current and accurate at all times during the terms of this DPA. the FIA will promptly take all actions relating to its Security Measures (and those of its Sub-Processors) that it deems necessary and advisable to identify and remediate the cause of a Customer Data Breach. In addition, the FIA will promptly provide the Customer with: (i) reasonable cooperation and assistance with regard to the Customer Data Breach, (ii) reasonable information in the FIA's possession concerning the Customer Data Breach insofar as it affects the Customer, including remediation efforts and any notification to Supervisory Authorities and, (iii) to the extent known: (a) the possible cause of the Customer Data Breach; (b) the categories of Customer Data involved; and (c) the possible consequences to Data Subjects. the FIA's notification of or response to a Customer Data Breach under this Section will not constitute an acknowledgment of fault or liability with respect to the Customer Data Breach, and the obligations herein shall not apply to Personal Data Breaches that are caused by the Customer, Authorized Users or providers of Customer components (such as systems, platforms, services, software, devices, etc.). If the Customer decides to notify a Supervisory Authority, Data Subjects or the public of a Customer Data Breach, the Customer will provide the FIA with advance copies of the proposed notices and, subject to applicable law (including any mandated deadlines under EU Data Protection Law), allow the FIA an opportunity to provide any clarifications or corrections to those notices. Subject to applicable

law, the FIA will not reference the Customer in any public filings, notices or press releases associated with the Customer Data Breach without the Customer's prior consent.

## **11. Compliance and Reviews**

11.1. Upon request, the FIA shall supply, on a confidential basis, a copy of its audit reports (if any) to the Customer, so that the Customer can verify the FIA compliance with the audit standards and this DPA.

11.2. the FIA shall also provide written responses, on a confidential basis, to all the Customer's reasonable requests for information to confirm the FIA's compliance with this DPA.

11.3. Where required by EU Data Protection Law, the FIA will allow the Customer (directly or through a third-party auditor subject to written confidentiality obligations) to conduct an audit of the FIA's procedures relevant to the protection of Customer Data to verify the FIA's compliance with its obligations under this DPA. In such case:

(a) The Customer shall: (i) provide the FIA at least 30 days' prior written notice of any proposed audit; (ii) undertake an audit no more than once in any 12-month period, except where required by a competent Supervisory Authority or where an audit is required due to a Customer Data Breach; and (iii) conduct any audit in a manner designed to minimize disruption of the FIA's normal business operations. To that end and before the commencement of any such audit, the Customer and the FIA shall mutually agree upon any reimbursement of expenses for which the Customer shall be responsible as well as audit's participants, schedule and scope, which shall in no event permit the Customer or its third-party auditor to access the Services' hosting sites, underlying systems or infrastructure.

(b) Representatives of the Customer performing an audit shall protect the confidentiality of all information obtained through such audits in accordance with the TOU, may be required to execute an enhanced mutually agreeable nondisclosure agreement and shall abide by the FIA's security policies while on the FIA's premises. Upon completion of an audit, the Customer agrees to promptly furnish to the FIA any written audit report or, if no written report is prepared, to promptly notify the FIA of any non-compliance discovered during the course of the audit.

## **12. Impact Assessment and Additional Information**

12.1. the FIA will provide the Customer with reasonable cooperation, information and assistance as needed to fulfill the Customer's obligation under EU Data Protection Law, including as needed to carry out a data protection impact assessment related to the Customer's use of the Services (in each case to the extent the Customer does not otherwise have access to the relevant information, and such information is in the FIA's control). Without

limiting the foregoing, the FIA shall provide reasonable assistance to the Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section to the extent required by EU Data Protection Law.

### **13. International Transfers**

13.1. the FIA shall at all times provide an adequate level of protection (within the meaning of Data Protection Laws) for the Customer Data Processed, in accordance with the requirements of Data Protection Laws. In the case of a transfer of Customer Personal data to a country not providing an adequate level of protection pursuant to the Data Protection Laws, the parties shall cooperate to ensure compliance with the applicable Data Protection Laws.

13.2. Sub-Processors used by the FIA to Process any Customer Data protected by Data Protection Laws and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) will provide an adequate level of protection for Personal Data and have SCC integrated in their Data Processing Agreements.

13.3. The parties further agree that the SCC (if applicable) will apply to Customer Data that is transferred via the Service from Europe to outside Europe, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Law). the FIA agrees to abide by and process Personal Data that originates from the EU in compliance with the SCC, which are incorporated in full by reference and form an integral part of this DPA for the SCC purposes:

13.3.1. the FIA agrees that it is the "data importer" and Customer is the "data exporter" under the SCC;

13.3.2. Annexes 1 and 2 of this DPA shall replace Appendixes 1 and 2 of the SCC, respectively.

### **14. Processing as Controller**

14.1. The Parties believe the FIA's role is as a Processor with respect to Customer Data. In relation to the Processing of Account Data, and to the extent (if any) that the FIA may be considered a Controller in relation to certain Processing of Customer Personal Data, each Party will comply with its obligations as a Controller and agrees to provide reasonable assistance as is necessary: (a) to each other to enable each Party to comply with any Data Subject access requests and to respond to any other queries or complaints from Data Subjects in accordance with the EU Data Protection Law; and (b) to each other to facilitate the handling of any Personal Data Breach as required under EU Data Protection Law.

## **15. Limitation of Liability and Applicable Law**

15.1. Each Party's liability taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the TOU.

## **16. Miscellaneous Provisions**

16.1. Any claims brought under or in connection with this DPA are subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the TOU.

16.2. No one other than a Party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

16.3. Any claims against the FIA under this DPA shall be brought solely against the entity that is a Party to the DPA. In no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. The Customer further agrees that any regulatory penalties incurred by the FIA in relation to the Customer Data that arise as a result of, or in connection with, the Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the FIA's liability under the DPA.

16.4. This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the TOU, unless required otherwise by applicable Data Protection Laws.

16.5. The Customer ensures that the decision to agree with the terms and conditions of this DPA was made lawfully by the Customer, in case the Customer is a natural person, or, by the Customer's director, authorized representative or other person having signatory powers, in case the Customer is a legal person.

16.6. This DPA replaces any previous DPAs concluded between the FIA and the Customer.

16.7. This DPA enters into force:

16.7.1. from the day you agreed with our Terms of Use and continues for an indefinite period of time; or

16.7.2. on October 20, 2020 if you have become our client before October 9, 2020 and continues for an indefinite period of time.

## **Annex 1**

### **Details of Data Processing**

1. Subject matter: The subject matter of the data Processing under this DPA is the Customer Data.

2. Duration of Processing: the FIA will Process Customer Data for the duration of the Services, as described in the TOU.

3. Nature of the Processing: the FIA provides email marketing and automation software as a service and other related services, as described in the TOU.

4. Purpose of the Processing: The purpose of the data Processing under this DPA is the provision of the Services.

5. Categories of Data subjects:

5.1. "Users" - any individual accessing and/or using the Services through the Customer's account;

5.2. "Subscribers" - any individual whose email address is included in the Customer's distribution list / whose information is stored on or collected via the Services / to whom Users send emails or otherwise engage or communicate with via the Services.

6. Types of Customer Data:

6.1. Users: identification and contact data (name, contact details, including email address, username); billing information (credit card details, account details, payment information); organization information (name, address, geographic location, area of responsibility, VAT code), IT information (IP address, usage data, cookies data, online navigation data, location data, browser data, access device information);

6.2. Subscribers: identification and contact data (name, date of birth, gender, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences, and publicly available social media profile information); IT information (IP address, usage data, cookies data, online navigation data, location data, browser data, access device information) and/or any other information the Customer provides to the FIA.

7. The Customer acknowledges that the FIA shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development or other. To the extent any such data is considered Personal Data under Data Protection Laws, the FIA is the Data Controller of such data and accordingly shall process such data in accordance with the FIA's Privacy Policy and Data Protection Laws.

8. The Customer acknowledges that in connection with the performance of the Services, the FIA employs the use of cookies, unique identifiers, web beacons and similar tracking technologies. The Customer shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable the FIA to deploy previously mentioned tracking technologies lawfully on and collect data from the devices of Subscribers. The Customer may use this statement about the FIA in the Customer's Privacy Policy:

*"We use the FIA to manage our nurture programme for properties that we deem to have exchanged contracts and will complete. The FIA will send SMS*

*text messages, emails and greeting cards through the postal service. The FIA uses a third-party provider, which may collect and process your data using industry standard technologies to help us to stay in touch with our customers. The FIA's Privacy Policy is available at <https://www.thefia.co.uk/privacy-policy/>*

*You can unsubscribe from our SMS service directly from any SMS message that is sent to you. You can also unsubscribe from receiving our annual greeting card by using the QR code on the card itself.*

## **Annex 2**

### **Security Measures**

Certain of The FIA's Security Measures as of the date of this DPA:

#### **1. Access Control and Employees Education**

1.1. The FIA restricts access to Customer Data to employees with a defined need-to-know or a role requiring such access.

1.2. The FIA's employees are introduced with the best security practices which allow them to identify Customer Data Breach and take any actions needed.

#### **2. Business Continuity**

2.1. The FIA maintains business continuity and backup plans in order to minimize the loss of service and comply with applicable laws.

2.2. The Backup plan addresses threats to the Services and any dependencies, and has an established procedure for resuming access to, and use of, the Services.

2.3. The Backup plan is tested at regular intervals.

#### **3. Change Control**

3.1. The FIA maintains policies and procedures for applying changes to the Services, including underlying infrastructure and system components, to ensure quality standards are being met.

3.2. The FIA undergoes a penetration test of its network and Services on an annual basis. Any vulnerabilities found during this testing will be remediated in accordance with The FIA's procedures.

#### **4. Data Security**

4.1. The FIA maintains technical safeguards and other security measures to ensure the security and confidentiality of Customer Data.

### **Annex 3**

List of The FIA Sub-Processors.

The FIA uses Autopilot HQ for the trigger of delivery of SMS text messages.

The FIA uses Zapier to trigger the delivery of some data

The FIA uses Stannp for the delivery of greeting cards

The FIA uses Twilio for the actual distribution of SMS messages