# Data Protection Addendum

The customer agreeing to these terms ("***Customer***") has entered into an agreement with Blinkfire Analytics, Inc., and certain of its Affiliates (as applicable, "***Blinkfire Analytics***") under which Blinkfire Analytics has agreed to provide services to Customer, including the Order Form and online Terms of Service, as applicable (in each case as amended from time to time, collectively referred to as the "***Agreement***").

This Data Protection Addendum, including its appendices (the "***Addendum***") will be effective and replace any previously applicable data processing and security terms as of the Addendum Effective Date (as defined below). This Addendum forms part of the Agreement.

## 1. Definitions

For purposes of this Addendum, the terms below shall have the meanings set forth below. Capitalised terms that are used but not otherwise defined in this Addendum shall have the meanings set forth in the Agreement.

1.1. "***Addendum Effective Date***" means the date on which the parties agreed to this Addendum.

1.2. "***Affiliate***" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

1.3. "***Audit Reports***" has the meaning given in Section 5.4.4.

1.4. "***Customer Personal Data***" means any personal data contained within the data provided to or accessed by Blinkfire Analytics by or on behalf of Customer or Customer end users in connection with the Services.

1.5. "***EEA***" means the European Economic Area.

1.6. "***EU***" means the European Union.

1.7. "***European Data Protection Legislation***" means the GDPR and other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein and Norway and the United Kingdom, applicable to the processing of Customer Personal Data under the Agreement.

1.8. "***FADP***" means together the Federal Act on Data Protection of 19 June 1992 (FADP) and the Ordinance to the Federal Act on Data Protection dated 14 June 1993 (DPO) in force on the Effective Date as well as the revised FADP and DPO entering into force on 1 September 2023.

1.9. "***GDPR***" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.10. "***Information Security Incident***" means a breach of Blinkfire Analytics' security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data in Blinkfire Analytics' possession, custody or control. "***Information Security Incidents***" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.11. "***Model Contract Clauses***" or "***MCCs***" mean modules 2 (controller to processor) or 3 (processor to processor), as applicable, of the standard contractual clauses approved by the

European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, a copy of which are attached as Attachment 3.

1.11.1. "***Restricted Transfer***" means the disclosure, grant of access or other transfer of Customer Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "***EU Restricted Transfer***"); (ii) in the context of the Switzerland, any country or territory outside Switzerland which does not benefit from an adequacy decision from the respective government body (a "***Swiss Restricted Transfer***"); and (iii) in the context of the UK, any country or territory outside the UK which does not benefit from an adequacy decision from the UK Government (a "***UK Restricted Transfer***"), which would be prohibited without a legal basis under European Data Protection Legislation.

1.12. "***Security Documentation***" means all documents and information made available by Blinkfire Analytics under Section 5.1.

1.13. "***Security Measures***" has the meaning given in Section 5.1.1 (Blinkfire Analytics' Security Measures).

1.14. "***Services***" means the services and/or products to be provided by Blinkfire Analytics to Customer under the Agreement.

1.15. ***"Subprocessors"*** means third parties authorised under this Addendum to process Customer Personal Data in relation to the Services.

1.16. "***Term***" means the period from the Addendum Effective Date until the end of Blinkfire Analytics' provision of the Services.

1.17. "***Third Party Subprocessors***" has the meaning given in Section 9 (Subprocessors).

1.18. "***Transfer Solution(s)***" means the MCCs, UK Transfer Addendum, and/or Swiss transfer mechanism; as applicable to the relevant Restricted Transfer.

1.19. "**UK**" means the United Kingdom of Great Britain and Northern Ireland.

1.20. "***UK Transfer Addendum***" means the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the UK Mandatory Clauses included in Part 2 thereof (the "UK Mandatory Clauses").

1.21. The terms "***personal data***", "***data subject***", "***processing***", "***controller***", "***processor***" and "***supervisory authority***" as used in this Addendum have the meanings given in the GDPR, and the terms "***data importer***" and "data exporter" have the meanings given in the Model Contract Clauses.

## 2. Duration of Addendum

This Addendum will take effect on the Addendum Effective Date and, notwithstanding the expiration of the Term, will remain in effect until, and automatically expire upon, Blinkfire Analytics' deletion of all Customer Personal Data as described in this Addendum.

## 3. Processing of Data

### 3.1. Roles and Regulatory Compliance; Authorization.

3.1.1. **Processor and Controller Responsibilities.** If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

(a) the subject matter and details of the processing are described in Appendix 1;

(b) Blinkfire Analytics is a processor of that Customer Personal Data under the European Data Protection Legislation;

(c) Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Legislation; and

(d) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

3.1.2. **Authorization by Third Party Controller.** If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Blinkfire Analytics that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Blinkfire Analytics as another processor, have been authorised by the relevant controller.

### 3.2. Scope of Processing.

3.2.1. **Customer's Instructions.** By entering into this Addendum, Customer instructs Blinkfire Analytics to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services; (b) as authorised by the Agreement, including this Addendum; and (c) as further documented in any other written instructions given by Customer and acknowledged in writing by Blinkfire Analytics as constituting instructions for purposes of this Addendum.

3.2.2. **Blinkfire Analytics' Compliance with Instructions.** Blinkfire Analytics will only process Customer Personal Data in accordance with Customer's instructions described in Section 3.2.1 (including with regard to data transfers) unless European Data Protection Legislation to which Blinkfire Analytics is subject requires other processing of Customer Personal Data by Blinkfire Analytics, in which case Blinkfire Analytics will notify Customer (unless that law prohibits Blinkfire Analytics from doing so on important grounds of public interest).

## 4. Data Deletion

4.1. **Deletion on Termination.** On expiry of the Term, Customer instructs Blinkfire Analytics to delete all Customer Personal Data (including existing copies) from Blinkfire Analytics' systems in accordance with applicable law as soon as reasonably practicable, unless applicable law requires otherwise.

## 5. Data Security

### 5.1. Blinkfire Analytics' Security Measures, Controls and Assistance.

5.1.1. **Blinkfire Analytics' Security Measures.** Blinkfire Analytics will implement and maintain technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Data as described in Appendix 2 (the "***Security Measures***"). Blinkfire Analytics may update or modify the Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

5.1.2. **Security Compliance by Blinkfire Analytics Staff.** Blinkfire Analytics will grant access to Customer Personal Data only to employees, contractors and Subprocessors who need such access for the scope of their performance, and are subject to appropriate confidentiality arrangements.

5.1.3. **Blinkfire Analytics' Security Assistance.** Blinkfire Analytics will (taking into account the nature of the processing of Customer Personal Data and the information available to Blinkfire Analytics) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Customer Personal Data under European Data Protection Legislation, including Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with Section 5.1.1 (Blinkfire Analytics' Security Measures);

(b) complying with the terms of Section 5.2 (Information Security Incidents); and

(c) providing Customer with the Security Documentation in accordance with Section 5.1 and the Agreement, including this Addendum.

## 5.2. Information Security Incidents

5.2.1. **Information Security Incident Notification.** If Blinkfire Analytics becomes aware of an Information Security Incident, Blinkfire Analytics will: (a) notify Customer of the Information Security Incident without undue delay after becoming aware of the Information Security Incident; and (b) take reasonable steps to identify the cause of such Information Security Incident, minimise harm and prevent a recurrence. Customer agrees that the provisions of this Section 5.2 (Information Security Incidents) satisfy the requirements under Clause 5(d)(2) of the Model Contract Clauses.

5.2.2. **Details of Information Security Incident.** Notifications made pursuant to this Section 5.2 (Information Security Incidents) will describe, to the extent known, details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Blinkfire Analytics recommends Customer take to address the Information Security Incident.

5.2.3. **Notification.** Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Information Security Incident(s).

5.2.4. **No Acknowledgement of Fault by Blinkfire Analytics.** Blinkfire Analytics' notification of or response to an Information Security Incident under this Section 5.2 (Information Security Incidents) will not be construed as an acknowledgement by Blinkfire Analytics of any fault or liability with respect to the Information Security Incident.

## 5.3. Customer's Security Responsibilities and Assessment.

5.3.1. **Customer's Security Responsibilities.** Customer agrees that, without prejudice to Blinkfire Analytics' obligations under Section 5.1 (Blinkfire Analytics' Security Measures, Controls and Assistance) and Section 5.2 (Information Security Incidents):

(a) Customer is solely responsible for its use of the Services, including:

(i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data;

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Services;

(iii) securing Customer's systems and devices Blinkfire Analytics uses to provide the Services; and

(iv) backing up its Customer Personal Data; and

(b) Blinkfire Analytics has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Blinkfire Analytics' and its Subprocessors' systems (for example, offline or on-premises storage).

**5.3.2. Customer's Security Assessment.**

(a) Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures and Blinkfire Analytics' commitments under this Section 5 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation.

(b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Blinkfire Analytics as set out in Section 5.1.1 (Blinkfire Analytics' Security Measures) provide a level of security appropriate to the risk in respect of the Customer Personal Data.

### 5.4. Reviews and Audits of Compliance

5.4.1. Customer may audit Blinkfire Analytics' compliance with its obligations under this Addendum up to once per year. In addition, to the extent required by European Data Protection Legislation, including where mandated by Customer's supervisory authority, Customer or Customer's supervisory authority may perform more frequent audits (including inspections). Blinkfire Analytics will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services.

5.4.2. If a third party is to conduct the audit, Blinkfire Analytics may object to the auditor if the auditor is, in Blinkfire Analytics' reasonable opinion, not suitably qualified or independent, a competitor of Blinkfire Analytics, or otherwise manifestly unsuitable. Such objection by Blinkfire Analytics will require Customer to appoint another auditor or conduct the audit itself.

5.4.3. To request an audit, Customer must submit a detailed proposed audit plan to notices@blinkfire.com addressed to the Chief Operating Officer at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Blinkfire Analytics will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Blinkfire Analytics security, privacy, employment or other relevant policies). Blinkfire Analytics will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 5.4 shall require Blinkfire Analytics to breach any duties of confidentiality.

5.4.4. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor ("***Audit Reports***") within twelve (12) months of Customer's audit request and Blinkfire Analytics confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

5.4.5. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Blinkfire Analytics' health and safety or other relevant policies, and may not unreasonably interfere with Blinkfire Analytics business activities.

5.4.6. Customer will promptly notify Blinkfire Analytics of any non-compliance discovered during the course of an audit and provide Blinkfire Analytics any audit reports generated in connection with any audit under this Section 5.4, unless prohibited by European Data Protection Legislation or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this Addendum. The audit reports are Confidential Information of the parties under the terms of the Agreement.

5.4.7. Any audits are at Customer's expense. Customer shall reimburse Blinkfire Analytics for any time expended by Blinkfire Analytics or its Third Party Subprocessors in connection with any audits or inspections under this Section 5.4 at Blinkfire Analytics' then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

5.4.8. The parties agree that this Section 5.4 shall satisfy Blinkfire Analytics' obligations under the audit requirements of the Model Contractual Clauses applied to Data Importer under Clause 5(f) and to any Sub-processors under Clause 11 and Clause 12(2). To maintain such regularity and consistency, changes or additions to these audit obligations must be made pursuant to Model Contract Clauses.

## 6. Impact Assessments and Consultations

Blinkfire Analytics will (taking into account the nature of the processing and the information available to Blinkfire Analytics) reasonably assist Customer in complying with its obligations under European Data Protection Legislation in respect of data protection impact assessments and prior consultation, including, if applicable, Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

6.1. Making available for review copies of the Audit Reports or other documentation describing relevant aspects of Blinkfire Analytics' information security program and the security measures applied in connection therewith; and

6.2. Providing the information contained in the Agreement including this Addendum.

## 7. Data Subject Rights

7.1. **Customer's Responsibility for Requests.** During the Term, if Blinkfire Analytics receives any request from a data subject in relation to Customer Personal Data, Blinkfire Analytics will advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request.

7.2. **Blinkfire Analytics' Data Subject Request Assistance.** Blinkfire Analytics will (taking into account the nature of the processing of Customer Personal Data) provide Customer with self-service functionality through the Services or other reasonable assistance as necessary for Customer to fulfil its obligation under European Data Protection Legislation to respond to requests by data subjects, including if applicable, Customer's obligation to respond to requests for exercising the data subject's rights set out in in Chapter III of the GDPR. Customer shall reimburse Blinkfire Analytics for any such assistance beyond providing self-service features included as part of the Services at Blinkfire Analytics' then-current professional services rates, which shall be made available to Customer upon request.

## 8. Data Transfers

8.1. **Data Storage and Processing Facilities.** Blinkfire Analytics may, subject to Section 8.2 (Transfers of Data Out of Europe), store and process Customer Personal Data anywhere Blinkfire Analytics or its Subprocessors maintain facilities.

### 8.2. Transfers of Data Out of Europe.

*EEA Restricted Transfers*

8.2.1. To the extent that any Processing of Customer Personal Data under this Addendum involves an EEA Restricted Transfer from Customer to Blinkfire Analytics, the Parties shall comply with their respective obligations set out in the MCCs, which are hereby attached hereto and incorporated herein as Attachment 3.

8.2.2. The Parties acknowledge and agree that where Customer acts as a controller, the Parties shall rely on the Module 2 (controller to processor) as set out in Attachment 3. Nonetheless, where Customer acts a processor, the Parties shall rely on the Module 3 (processor to processor) as set out in Attachment 3.

*UK Restricted Transfers*

8.2.3. To the extent that any Processing of Customer Personal Data under this Addendum involves a UK Restricted Transfer from Customer to Blinkfire Analytics, the Parties shall comply with their respective obligations set out in the MCCs, which are hereby deemed to be:

(a) varied to address the requirements of the UK GDPR in accordance with the UK Transfer Addendum and populated as set out in Attachment 4; and

(b) entered into by the Parties and incorporated by reference into this Addendum.

*Swiss Restricted Transfers*

8.2.4. In respect of Processing covered hereby that is subject to the FADP, for the purposes of this Addendum, the following terms are deemed to have the following substituted meanings "GDPR" means the "FADP"; and "European Union", "Union" and "Member State(s)" each means Switzerland. In particular, in respect of any Swiss Restricted Transfer, the MCCs shall be revised as follows:

(a) the competent supervisory authority for the purposes of Clause 13 of the MCCs is the Swiss Federal Data Protection and Information Commissioner;

(b) the applicable law for the purposes of Clause 17 of the MCCs shall be Swiss law; and

(c) the courts having jurisdiction under Clause 18(b) of the MCCs shall be the courts of the city of Zurich, Switzerland –

(d) furthermore, the Parties expressly agree that nothing in those MCCs applicable to a Swiss Restricted Transfer (as amended pursuant to the foregoing) should be interpreted or construed in such a way as would limit or exclude the rights of data subjects to bring legal proceedings against either Party before the courts in Switzerland where Switzerland is that data subject's place of habitual residence, and that for so long as the FADP applies in its current version until its inapplicability by 1 September 2023, the term "data subject" shall also include legal entities.

*Adoption of new transfer mechanism*

8.2.5. Blinkfire Analytics may on notice vary this Addendum and replace the relevant Transfer Solution(s) with:

(a) any new form of the relevant Transfer Solution(s) or any replacement therefor prepared and populated accordingly; or

(b) another transfer mechanism,

that enables the lawful transfer of Customer Personal Data by Customer to Vendor under this Addendum in compliance with Chapter V of the GDPR.

*Provision of full-form Transfer Solution(s)*

8.2.6. In respect of any given Restricted Transfer, if requested of Customer or Blinkfire Analytics ("Requesting Party"), the other Party shall provide the Requesting Party with an executed version of the relevant set(s) of Transfer Solution(s) (as applicable) covering Restricted Transfer(s) to Blinkfire Analytics.

*Access to Personal Data by public authorities*

8.2.7. To the extent permitted by applicable laws, each Party shall notify the other Party promptly in writing of any subpoena or other judicial or administrative order by a public authority or proceeding seeking access to or disclosure of Customer Personal Data. Such notification shall, to the extent permitted by applicable laws, include details regarding the Data Subject concerned, Personal Data requested, the requesting authority, the legal basis for the request, and any responses provided.

8.2.8. Where Blinkfire Analytics receives such request, Customer shall have the right to defend such legal challenge in lieu of and/or on behalf of Blinkfire Analytics to the extent permitted by applicable laws. Customer may, if it so chooses, seek a protective order. Blinkfire Analytics shall reasonably cooperate with Customer in such defense.

8.2.9. To the extent permitted by applicable laws, each Party shall not disclose the Personal Data requested until all reasonable challenges have been exhausted and shall provide the minimum of information permissible when responding to an order to disclose the Personal Data.

8.2.10. Where the notifying Party is prohibited from satisfying clause 8.2.7 under applicable laws, the notifying Party shall use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible.

8.2.11. Where a Party becomes aware of any direct access by public authorities to Personal Data (including the reasonable suspicion thereof), this Party shall promptly notify the other Party with all information available, unless otherwise prohibited by applicable laws.

8.2.12. Blinkfire Analytics represents and warrants that:

(a) Blinkfire Analytics has not purposefully created 'backdoors' or similar programming designed to, or that could, be used to access its systems used to store or otherwise Process Customer Personal Data;

(b) Blinkfire Analytics has not purposefully created or changed its business processes in a manner that facilitates access to its relevant systems or to Customer Personal Data by any governmental authority, law enforcement agency, public body or judicial body and shall not voluntarily cooperate with any such authorities, agencies or bodies in relation to the same; and

(c) no applicable law or government policy to which Blinkfire Analytics is subject requires Blinkfire Analytics to create or maintain 'backdoors' or to otherwise enable or facilitate access to Customer Personal Data or systems.

## 9. Subprocessors

9.1. **Consent to Subprocessor Engagement.** Customer specifically authorises the engagement of Blinkfire Analytics' Affiliates as Subprocessors. In addition, Customer generally authorises the engagement of any other third parties as Subprocessors ("***Third Party Subprocessors***"). If Customer has entered into Model Contract Clauses as described in Section 9.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Blinkfire Analytics of the processing of Customer Personal Data if such consent is required under the Model Contract Clauses. and Customer agrees that such consent agrees satisfies the requirements under Clauses 5(h) and 11.1of the Model Contract Clauses.

9.2. **Information about Subprocessors.** Information about Subprocessors, including their functions and locations, is available at https://www.blinkfire.com/subprocessors (as may be updated by Blinkfire Analytics from time to time in accordance with this Addendum).

9.3. **Requirements for Subprocessor Engagement.** When engaging any Subprocessor, Blinkfire Analytics will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in the Agreement (including this Addendum) with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Subprocessor. Blinkfire Analytics shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor. Upon Customer's written request, Blinkfire Analytics shall allow Customer to examine the data protection provisions of agreements between Blinkfire Analytics and its subcontractors that access Customer Personal Data, provided that such agreements shall remain Blinkfire Analytics' Confidential Information. Customer agrees that this section 9.3 satisfies the requirements under Clause 5(j) of the Model Contract Clauses.

### 9.4. Opportunity to Object to Subprocessor Changes.

When any new Third Party Subprocessor is engaged during the Term, Blinkfire Analytics will, at least 30 days before the new Third Party Subprocessor processes any Customer Personal Data, notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform).

Customer may object to any new Third Party Subprocessor by providing written notice to Blinkfire Analytics within ten (10) business days of being informed of the engagement of the Third Party Subprocessor as described above. In the event Customer objects to a new Third Party Subprocessor, Customer and Blinkfire Analytics will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to Blinkfire Analytics.

## 10. Processing Records

10.1. **Blinkfire Analytics' Processing Records.** Customer acknowledges that Blinkfire Analytics is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Blinkfire Analytics is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to Blinkfire Analytics, and will ensure that all information provided is kept accurate and up-to-date.

## 11. Liability

11.1. **Liability Cap.** The total combined liability of either party and its Affiliates towards the other party and its Affiliates, whether in contract, tort or any other theory of liability, under or in connection with the Agreement, this Addendum, and the Model Contract Clauses if entered into as described in Section 8.2 (Transfers of Data Out of the EEA) combined will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement, subject to Section 11.2 (Liability Cap Exclusions).

11.2. **Liability Cap Exclusions.** Nothing in Section 11.1 (Liability Cap) will affect any party's liability to data subjects under the third party beneficiary provisions of the Model Contract Clauses to the extent limitation of such rights is prohibited by the European Data Protection Legislation.

## 12. Third Party Beneficiary

Notwithstanding anything to the contrary in the Agreement, where Blinkfire Analytics is not a party to the Agreement, Blinkfire Analytics will be a third party beneficiary of Section 5.4 (Reviews and Audits of Compliance), Section 9.1 (Consent to Subprocessor Engagement) and Section 11 (Liability) of this Addendum.

## 13. Analytics

Customer acknowledges and agrees that Blinkfire Analytics may create and derive from processing related to the Services anonymised and/or aggregated data that does not identify Customer or any natural person, and use, publicise or share with third parties such data to improve Blinkfire Analytics' products and services and for its other legitimate business purposes.

## 14. Notices

Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Blinkfire Analytics to Customer may be given (a) in accordance with the notice clause of the Agreement; (b) to Blinkfire Analytics' primary points of contact with Customer; and/or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

## 15. Effect of These Terms

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between this Addendum and the remaining terms of the Agreement, this Addendum will govern. In the event of any conflict or inconsistency between any Transfer Solution(s) and this Addendum and/or the Agreement, those Transfer Solution(s) (as applicable) shall prevail to the extent of any such conflict or inconsistency.

Accepted and agreed to by the authorised representative of each party:

**CUSTOMER**

[Customer name]

By: ____________________________________

Name:

Title:

Date:

**Blinkfire Analytics**

By: ______________________________________

Name:

Title:

Date:

## APPENDIX 1

## Subject Matter and Details of the Data Processing

| | |
|---|---|
| **Duration of the Processing (period for which the personal data will be retained)** | **Where Customer acts as a controller (Module 2):** The Term plus the period from the expiry of the Term until deletion of all Customer Personal Data by Blinkfire Analytics in accordance with the Addendum.<br>**Where Customer acts as a processor (Module 3):** Same as above |
| **Nature of the Processing** | **Where Customer acts as a controller (Module 2):** Blinkfire Analytics will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Addendum.<br>**Where Customer acts as a processor (Module 3):** Same as above |
| **Purpose of the Processing** | **Where Customer acts as a controller (Module 2):** Blinkfire Analytics' provision of the Services to Customer<br>**Where Customer acts as a processor (Module 3):** Same as above |
| **Categories of Data** | **Where Customer acts as a controller (Module 2):** Navigation information (IP address, time) of customer's representatives, customer's representatives business contact details (name, family name, position)<br>**Where Customer acts as a processor (Module 3):** Same as above |
| **Categories of Sensitive Data** | **Where Customer acts as a controller (Module 2):** N/A<br>**Where Customer acts as a processor (Module 3):** N/A |
| **Additional Safeguards for Sensitive Data** | **Where Customer acts as a controller (Module 2):** N/A<br>**Where Customer acts as a processor (Module 3):** N/A |
| **Data Subjects** | **Where Customer acts as a controller (Module 2):** Data subjects include customer's representatives<br>**Where Customer acts as a processor (Module 3):** Same as above |
| **The Frequency of the Processing/Transfer** | **Where Customer acts as a controller (Module 2):** Ongoing processing / transfer<br>**Where Customer acts as a processor (Module 3):** Same as above |

| | |
|---|---|
| **Processing to (Sub-) Processors (specify subject matter, nature and duration of the processing)** | **Where Customer acts as a controller (Module 2):**<br>• **Google Cloud**:<br>○ Subject Matter: provides cloud computing services<br>○ Nature: Storage<br>• **Quickbooks**:<br>○ Subject Matter: provides accounting services<br>○ Nature: Accounting services and invoicing<br>**Where Customer acts as a processor (Module 3):** Same as above |

## APPENDIX 2

## Security Measures

As from the Addendum Effective Date, Blinkfire Analytics will implement and maintain the Security Measures set out in this Appendix 2, which are part of Blinkfire Analytics Data and Security Guidelines. Blinkfire Analytics may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

### Hosting environment

All data is kept in Google Cloud Platform servers. Their security whitepaper is here: https://cloud.google.com/security/overview/whitepaper

### Data Storage

All data is kept in the cloud in the Google Cloud Platform in the us-central region (Iowa) https://cloud.google.com/compute/docs/regions-zones. However, web pages and APIs are served with geo-redundancy to CDNs closest to our customers, and some data may be cached in other regions of the world in a transient manner for performance reasons.

All customer access keys are kept in a database separate from the code, which can only be accessed from within the application.

### Penetration testing

We currently use Google Cloud Scanner https://cloud.google.com/security-command-center/docs/how-to-web-security-scanner-custom-scans to perform daily automated penetration testing against https://www.blinkfire.com and all public APIs, as we as our staging environments.

Any vulnerabilities introduced by code or third party libraries are dealt with as Priority 1 issues and are solved as soon as possible.

### Blinkfire.com user accounts

Blinkfire does not allow login through username or passwords, but only through third party login mechanisms of Facebook, Twitter, Google, or Microsoft. We rely on your security policies with those platforms to protect your login to Blinkfire.com

Blinkfire Analytics supports 2 Factor Authentication, though it is not required. It is recommended that all customers require their users of Blinkfire to turn on 2 Factor Authentication.

Blinkfire.com does not store any user passwords.

### Blinkfire Analytics Employee Policies

All systems used by Blinkfire Analytics are required to support 2 Factor Authentication, and all employees are required to use 2 Factor Authentication for all logins at all times.

### Engineering Policies

Engineering policies are stricter and require hardware key fob authentication for accessing code and Google Cloud environments.

Blinkfire engineers are only allowed to keep code on company purchased machines.

# ATTACHMENT 3

## Standard Contractual Clauses (Modules 2 and 3)

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

## MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

## MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

## SECTION I

1.

### Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

2.

## Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

3.

## Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module Two: Clause 8.1(b), Clause 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4.

## Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

5.

### Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

6.

### Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

7.

### Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II - OBLIGATIONS OF THE PARTIES

8.

### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**MODULE TWO: Transfer controller to processor**

**8.1. Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3. **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### 8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9. **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

**MODULE THREE: Transfer processor to processor**

**8.1. Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[3].

8.2. **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.3. **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4. **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5. **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8. **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

### 8.9. **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## 9.

## Use of sub-processors

**MODULE TWO: Transfer controller to processor**

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[5] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to

[5] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby — in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**MODULE THREE: Transfer processor to processor**

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[6] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**10.**

## Data subject rights

**MODULE TWO: Transfer controller to processor**

[6] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

**MODULE THREE: Transfer processor to processor**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

**11.**

## Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**12.**

## Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

**13.**

## Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

**14.**

### Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[7];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

[7] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [For Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [For Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## 15.

## Obligations of the data importer in case of access by public authorities

### 15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

For Module Three: The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). For Module Three: The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. For Module Three: The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV - FINAL PROVISIONS

**16.**

### Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [For Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**17.**

## Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the laws of Spain

**18.**

## Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Spain..

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

## APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

# ANNEX I

## A. LIST OF PARTIES

**Data exporter(s)**:

Name: [Please complete]

Address: [Please complete]

Contact person's name, position and contact details: [Please complete]

Activities relevant to the data transferred under these Clauses: [Please complete]

Signature and date: [Please complete]

Role (controller/processor): [Please complete]

**Data importer(s)**:

Name: Blinkfire Analytics Inc.

Address: 560 W Washington Blvd, Chicago, IL 60661, United States

Contact person's name, position and contact details: [Please complete]

Activities relevant to the data transferred under these Clauses: [Please complete]

Signature and date: [Please complete]

Role (controller/processor): Processor

## B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

As set out in Appendix 1 of the Addendum.

*Categories of personal data transferred*

As set out in Appendix 1 of the Addendum.

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*

Categories of sensitive data

As set out in Appendix 1 of the Addendum.

Additional safeguards for sensitive data

As set out in Appendix 1 of the Addendum.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)*

As set out in Appendix 1 of the Addendum.

*Nature of the processing*

As set out in Appendix 1 of the Addendum.

*Purpose(s) of the data transfer and further processing*

As set out in Appendix 1 of the Addendum.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

As set out in Appendix 1 of the Addendum.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

As set out in Appendix 1 of the Addendum.

## C. COMPETENT SUPERVISORY AUTHORITY

*Identify the competent supervisory authority/ies in accordance with Clause 13:* Agencia Española de Protección de Datos (Spanish supervisory authority).

# ANNEX II

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

Information Security: please refer to the Security Measures determined by and set out in Appendix 2 (Security Measures) of the Addendum, to which these Clauses are attached.

# ATTACHMENT 4

## UK TRANSFER ADDENDUM

1. Where relevant in accordance with Paragraph 8.2.2. of the Addendum, the MCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum in the manner described below –

   (a) *Part 1 to the UK Transfer Addendum*. The Parties agree:

      (i) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Appendix 1 and Attachment 3 (subject to the variations effected by the UK Mandatory Clauses described in (b) below); and

      (ii) Table 4 to the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked.

   (b) *Part 2 to the UK Transfer Addendum*. The Parties agree to be bound by the UK Mandatory Clauses of the UK Transfer Addendum.

2. As permitted by Section 17 of the UK Mandatory Clauses, the Parties agree to the presentation of the information required by 'Part 1: Tables' of the UK Transfer Addendum in the manner set out in Paragraph 1 of this Attachment 4; **provided that** the Parties further agree that nothing in the manner of that presentation shall operate or be construed so as to reduce the Appropriate Safeguards (as defined in Section 3 of the UK Mandatory Clauses).

In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the Addendum to the MCCs, shall be read as a reference to those MCCs as varied in the manner set out in Paragraph 1 of this Attachment 4.