

## DPA Schedule for European Union, European Economic Area, Switzerland and United Kingdom of Great Britain and Northern Ireland

The parties hereby agree to comply with this DPA Schedule for the European Union, European Economic Area, Switzerland and United Kingdom of Great Britain and Northern Ireland (including its exhibits and annexes, this “**Schedule**”) when Customer Data, Sightings Data, or Lotame Data is or includes Personal Data subject to the GDPR.

**1. Definitions.** Capitalized words used but not defined in this Schedule have the meanings given in the DPA or the Agreement.

“**DPA**” means the Data Processing Agreement currently posted at <https://www.lotame.com/privacy/dpas/dpa-msa/>.

“**GDPR Countries**” means the countries in the European Union and the European Economic Area that have implemented the EU GDPR, the United Kingdom of Great Britain and Northern Ireland, and Switzerland.

“**DPF**” means collectively the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

“**DPF Principles**” means collectively the EU-U.S. Data Privacy Framework Principles (available at <https://www.dataprivacyframework.gov/s/framework-text>) and the Swiss-U.S. Data Privacy Framework Principles (available at <https://www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3>).

“**EU SCCs**” means the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR.

“**EU-U.S. DPF**” means collectively the EU-US Data Privacy Framework (available at <https://www.dataprivacyframework.gov/s/framework-text>) and the *Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*.

“**GDPR**” means (1) the 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 (“**EU GDPR**”) and (2) the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (“**UK GDPR**”), and Switzerland’s Federal Act of 25 September 2020 on Data Protection (“**FADP**”).

“**Non-Adequate Third Country**” means a country not recognized by the European Commission, the UK, or Switzerland as providing an adequate level of protection for personal data (as described in the GDPR).

“**Supervisory Authority**” means an independent public authority which is established by an EU Member State / Switzerland / UK, as applicable, pursuant to the GDPR.

“**Swiss-U.S. DPF**” means collectively the EU-U.S. Data Privacy Framework (available at <https://www.dataprivacyframework.gov/s/framework-text>).<sup>1</sup>

“**UK**” means The United Kingdom of Great Britain and Northern Ireland.

“**UK Extension to the EU-U.S. DPF**” means collectively the EU-U.S. Data Privacy Framework (available at <https://www.dataprivacyframework.gov/s/framework-text>) and the *Data Protection (Adequacy) (United States of America) Regulations 2023* (SI 2023/1028).

**2. Scope.** This Schedule is incorporated by reference into the DPA and is applicable only when Customer Data, Sightings Data, or Lotame Data is or includes “personal data” (as defined by the GDPR) subject to the GDPR.

**3. Processing of Customer Data by Lotame as a Processor.** This Section applies when Lotame is processing Customer Data for Customer’s or its Clients own benefit.

**3.1. Roles of the Parties.** Customer is a controller that transfers Customer Data to Lotame, and Lotame is a processor that receives Customer Data for Processing. Each party will comply with their respective obligations in and will Process Customer Data in accordance with this Section 3, Section 4 of the DPA, and the provisions of the GDPR applicable to their role as specified in the previous sentence.

<sup>1</sup> As of April 19, 2024, Switzerland has not yet recognized adequacy for the Swiss-U.S. DPF and therefore, personal data cannot be received from Switzerland in reliance on the Swiss-U.S. DPF until the date of entry into force of Switzerland’s recognition of adequacy for the Swiss-U.S. DPF.

**3.2. Incorporation of EU SCCs.** With respect to the matters referred to in Articles 28(3) and 28(4) of the EU GDPR and the UK GDPR and Article 9 of the FADP, as regards to the transfer of personal data from a controller to a processor or from a processor to a sub-processor, each party will comply with their respective obligations in Module 2 (for controller-to-processor relationships) or in Module 3 (for processor-to-sub-processor relationships) of the EU SCCs applicable to their role (as specified in Section 3.2(a)), with certain clauses of Module 2 and Module 3 of the EU SCCs completed or clarified as follows:

(a) Customer is the “data exporter” and Lotame is the “data importer.”

(b) The optional Clause 7 is included.

(c) With respect to the references to documented instructions in Clauses 8.1 and 8.2, Customer acknowledges that Lotame’s platform is operated as a multi-tenant software-as-a-service where all personal data is processed in the same manner. As such, documented instructions, as referenced in Clauses 8.1 and 8.2, are handled in accordance with Section 4.8 of the DPA and that Customer is solely responsible for ensuring that those settings and its use of the Services complies with the GDPR and Module 2 of the EU SCCs.

(d) With respect to Clause 8.8, for any onward transfers of Customer Data to a Third Party Platform initiated by Customer through use of the Services, Customer acknowledges that such onward transfer is being facilitated by Lotame on Customer’s behalf and that Customer is responsible for ensuring that it or its Third Party Sources has the appropriate contractual arrangements with the Third Party Platform as required by Clause 8.8.

(e) With respect to Clause 9(a), Option 2 is selected.

(f) With respect to Clause 10(a), if a User Data Request does not identify Customer or Lotame is unable, given the information in the User Data Request, to relate the User Data Request to Customer or any of its Third Party Sources, Lotame will be unable to notify Customer of the User Data Request; however, Lotame will respond to the User Data Request in accordance with Section 4.4 of the DPA.

(g) With respect to Clause 11(a), the optional text is included.

(h) With respect to Clause 17, with Option 2 selected, (1) for data transfers from the EU/EEA, the Member State is the Republic of Ireland and (2) for data transfers from Switzerland, the Member State is Switzerland.

(i) With respect to Clause 18(b), the Member State is the Republic of Ireland.

(j) Annexes I, II, and III of Module 2 and Module 3 are deemed completed with the information set out in Annexes I, II, and III of Exhibit 1 to this Schedule.

(k) Where the Swiss Federal Act on Data Protection (FADP) applies to Processing of Personal Data, (1) references to the GDPR in the EU SCCs should be understood as references to the FADP insofar as the data transfers are subject to the FADP and the EU SCCs will also protect the data of legal entities, until the entry into force of the revised FADP and (2) the term “member state,” as used in the EU SCCs, must not be interpreted in such a way as to exclude Users in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.

**3.3-3.3. Transfers of Customer Data to the United States.** With respect to transfers of personal data to third countries or international organisations, Customer acknowledges that using the Services will require the transfer of Customer Data to the United States- and that pursuant to Article 45(1) of the EU GDPR and the UK GDPR, the United States has been determined to provide an adequate level of protection under the DPF. Lotame complies with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF as set forth by the U.S. Department of Commerce. Lotame has certified to the U.S. Department of Commerce that it adheres to the DPF Principles with regard to the processing of Personal Data received from a GDPR Country in reliance on the applicable DPF.

**3.3-3.4. Onward Transfers of Customer Data by Lotame on Behalf of Customer.** When Lotame transfers Customer Data to third-parties on behalf of and at the instruction of Customer, the Customer is responsible for ensuring the transfer to the third-party complies with the GDPR.

**3.4-3.5. Consent Policy.** Customer and its Third Party Sources shall comply with Lotame’s Consent Policy for the European Union, European Economic Area, Switzerland, and United Kingdom of Great Britain and Northern Ireland available at <https://www.lotame.com/legal/policies/eu-consent-policy/>.

#### 4. Processing of Sightings Data by Lotame.

**4.1. Roles of the Parties.** Customer is a “controller” that transfers Sightings Data to Lotame, and Lotame is a “controller” that receives Sightings Data for Processing. Each party will comply with their respective obligations in and will Process Sightings Data in

accordance with this Section 4, Section 4 of the DPA, and the provisions of the GDPR applicable to their role specified in the previous sentence.

**4.2. Transfers of Sightings Data to the United States.** Customer acknowledges that Lotame will transfer Sightings Data to the United States. Lotame complies with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF as set forth by the U.S. Department of Commerce. Lotame has certified to the U.S. Department of Commerce that it adheres to the DPF Principles with regard to the processing of Personal Data received from a GDPR Country in reliance on the applicable DPF.

**4.3. Onward Transfers of Sightings Data.** Lotame participates in and has certified its compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. In accordance with Lotame's obligation under the DPF, any transfers of Personal Data to a third-party controller will be accomplished in compliance with the GDPR and the DPF Principles.

## **5. Processing of Lotame Data by Customer.**

**5.1. Roles of the Parties.** Lotame is a “controller” that transfers Lotame Data to Customer, and Customer is a “controller” that receives (directly or indirectly) Lotame Data for Processing. Each party will comply with their respective obligations in and will Process Lotame Data in accordance with this Section 5, Section 5 of the DPA, and the provisions of the GDPR applicable to their role specified in the previous sentence.

**5.2. Onward Transfers of Lotame Data by Customer.** Lotame participates in and has certified its compliance with the DPF and in accordance with Lotame's obligations under the DPF, Customer shall (i) only process the Lotame Data for limited and specified purposes consistent with the Agreement and (ii) provide the same level of protection for the Lotame Data as is required by the DPF Principles. Customer will notify Lotame and cease processing the Lotame Data (or take other reasonable and appropriate remedial steps) if the Customer determines that it cannot provide the same level of protection for the Lotame Data as is required by the DPF Principles.

**6. IAB Europe's Transparency & Consent Framework.** Lotame participates in the IAB Europe's Transparency & Consent Framework (TCF) as a vendor and complies with its Policies and Specifications. Lotame's identification number within the TCF is 95. If Customer or any Third Party Source has implemented the TCF on any Properties, Customer and its Third Party Sources shall add Lotame as a vendor.

**7. Cooperation.** Upon a party's request, the other party shall provide the requesting party with (a) reasonable cooperation and assistance needed for the requesting party to fulfil its obligations under the GDPR to complete any required assessments related to Processing of Personal Data exchanged between the parties, to the extent the requesting party does not otherwise have access to the relevant information, and to the extent such information is available to the other party; and (b) any Supervisory Authority inquiry or investigation related to the performance under the Agreement.

## Exhibit 1

### Annex I

#### 1. LIST OF PARTIES

##### Data exporter(s):

Name: The data exporter is the entity identified as the “Customer” in the Agreement.

Address: Address of the entity identified as “Customer” in the Agreement.

Contact person’s name, position and contact details: Privacy contact identified in the Agreement, if not directly identified therein, Customer shall provide it to Lotame without undue delay.

Activities relevant to the data transferred under these Clauses: Processing of personal data for purposes and activities identified in the Agreement.

Signature and date: Signed and dated in the Agreement by the authorized person for Customer.

Module 2 Role (controller/processor): Controller

Module 3 Role (controller/processor): Processor

##### Data importer(s):

Name: The data importer is the entity identified as “Lotame” in the Agreement.

Address: Address of the entity identified as “Lotame” in the Agreement.

Contact person’s name, position and contact details: Data Protection/Privacy Contact identified in the Agreement, privacy@notice.com and address provided in the Agreement.

Activities relevant to the data transferred under these Clauses: Processing of personal data for purposes and activities identified in the Agreement.

Signature and date: Signed and dated in the Agreement by the authorized person for Lotame.

Role (controller/processor): Processor

#### 2. DESCRIPTION OF TRANSFER

##### (a) Categories of data subjects whose personal data is transferred

Persons viewing and/or interacting with the online properties (including advertisements) of the data exporter (or its Third Party Sources) which have been tagged by or on behalf of data exporter.

##### (b) Categories of personal data transferred

The personal data transferred concern the following categories of data:

- Online identifiers (for example, cookie ID, mobile device advertising ID (e.g., Apple IDFA, Google AD ID));
- Hashed or raw email, if provided by the data exporter or its Third Party Sources;
- URLs, attributes, preferences, interests, and other characteristics of an individual or inferred about an individual (for example, individual’s non-precise location, intent data, socio-demographic data, purchase data, browsing data) (referred to as “behaviors”), as determined by the data exporter or its Third Party Sources; and
- Browser information (user agent/client hints).

##### (c) 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.

The data exporter (nor its Third Party Sources) will not send sensitive data to the data importer.

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

The transfer of personal data will be on a continuous basis.

**(e) Nature of the processing**

Same as purposes below.

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

The transfer is made for the following purposes:

- As identified in the Agreement

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

The retention for the personal data transferred is:

- Behaviours – 13 months from the date of its collection
- Pseudonymous IDs and hashed emails – 90 days after the Pseudonymous ID or hashed email is no longer associated with any Behaviours.
- Internet log data and event data – 12 weeks

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

Same as data importer.

**3. COMPETENT SUPERVISORY AUTHORITY**

The competent supervisory authority is supervisory authority in the country of data exporter's residence in the EU, as indicated in Annex I.A. above. In case data exporter falls into one of the other categories under Clause 13, it shall notify data importer without undue delay of the competent supervisory authority in accordance with clause 13 of Clauses.

For the purposes of transfers of Swiss personal data, parallel supervision should apply. FDPIC, insofar as the data transfer is governed by the Swiss FADP; EU authority insofar as the data transfer is governed by the GDPR (whilst the criteria of Clause 13 for the selection of the competent authority must be observed).

**Annex II**

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

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

- 1. Systems' Access Controls.** Lotame maintains appropriate technical and organizational policies, procedures and safeguards to limit access to its platform and services to only those individuals that require access, including protection against unauthorized processing, loss, or unauthorized disclosure of or access to Customer Data. Access to Customer Data within Lotame's platform is governed by role-based access control (RBAC) and can be configured to define granular access privileges, including distinct read/write privileges. These privileges are packaged into reusable and customizable roles to support various permission levels for employees and users (owner, admin, agent, end-user, etc.). Individual users are granted any number of roles, thus providing the capability to control specific responsibilities and access levels within Lotame's organization. Lotame's information security management system is ISO/IEC 27001:2013 certified and is audited annually by an independent third party. Lotame's ISO/IEC 27001:2013 certificate is available upon request.
- 2. Physical & Environmental Controls – Hosting Infrastructure.** Lotame's production infrastructure is hosted by Amazon Web Services (AWS). Lotame does not maintain any physical access to the AWS facilities, and remote access is restricted to named operations staff on an as needed basis. For more information about AWS security, refer to <https://aws.amazon.com/security/>.
- 3. Physical & Environmental Controls – Corporate Offices.** While Customer Data is not hosted at Lotame's corporate offices, its technical, administrative, and physical controls for its corporate offices are covered by its ISO/IEC 27001:2013 certification and include, but are not limited to, the following:
  - Physical access to the corporate offices are controlled at office ingress points;

- Badge access is required for all personnel and badge privileges are reviewed regularly;
  - Visitors are required to be escorted by employees; and
  - Cameras.
- 4. Data Transmission and Storage.** All Customer Data in transit is encrypted using TLS 1.2 or better. Customer Data is also encrypted at rest.
- 5. Development Practices.** Lotame utilizes industry-standard source code, build, and deployment processes and systems to manage the introduction of new code into its platform and services. Access to the code repositories is granted on an as needed basis only to employees within Lotame's technology and engineering organizations. A member of Lotame's privacy team is also part of product and service development to ensure privacy by design and default considerations are taken into account.
- 6. Configuration Management.** Lotame utilizes automated configuration management tools to manage application runtimes and configuration parameters across its infrastructure, with access restricted to employees that support releases and operations. Within the configuration management information architecture, credentials used by automated systems (e.g., database logins) are isolated from general application configuration parameters to further limit access to such credentials
- 7. Data Minimization and Pseudonymization.** Lotame's services do not monitor Customer to limit what personal data is collected by Lotame's code or sent to us via a file – Customer is responsible for determining what behaviors are collected. Lotame's platform will process all data regardless of its nature as long as it fits the predefined characteristics that allow it to be processed. Lotame does not make any data-based decisions other than following customers' instructions as they configure Lotame's data collection tools to perform their desired operations. Customer Data may associated with pseudonymous IDs assigned by Lotame or device-based pseudonymous IDs. If Customer Data includes un-hashed deterministic identifiers (for example, email addresses), Lotame tokenizes such deterministic identifiers and segregates them from all other data, and uses technical and organizational measures and controls to maintain that separation, prevent use of those deterministic identifiers during processing within the platform, and prevent access and viewing of deterministic identifiers except by limited operations leadership for troubleshooting purposes and compliance with applicable laws.
- 9. Confidentiality.** All Lotame employees and contractors enter into customary confidentiality agreements that governs the access, use and treatment of all Customer Data that we process.
- 10. Personal Data Incident Notifications and Mitigation.** Lotame maintains data incident management policies and procedures that it tests annually. Lotame will, without undue delay and in accordance with the timelines required by applicable Data Protection and Privacy Laws, notify data exporter of any incidents that result in the unauthorized or illegal destruction, loss, alteration, disclosure of, or access to, their Customer Data. Lotame will take prompt action to mitigate continued harm to data exporter or personal data.
- 11. Vulnerability Detection and Management.**
- Anti-Virus and Vulnerability Detection: Lotame leverages threat detection tools to monitor and alert it to suspicious activities, potential malware, viruses and/or malicious computer code.
  - Penetration Testing and Vulnerability Detection: Lotame engages an independent third party to conduct penetration tests of its platform and services annually.
  - Vulnerability Management: Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Platform and Services.

### **Annex III**

#### **LIST OF PROCESSORS**

The list of Lotame's processors engaged by Lotame are currently posted at <https://www.lotame.com/Privacy-and-Data-Protection>.