

Customer EU Data Processing Addendum

This Data Processing Addendum ("**DPA**"), forms part of the Agreement between Ahoy Technologies, Inc d/b/a ahoy! ("**ahoy!**") and _____ ("**Customer**") and shall be effective on the date both parties execute this DPA ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions.

1. "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.
2. "**Agreement**" means the ahoy! Terms of Use, which governs the provision of the Services to Customer, as such terms may be updated by ahoy! from time to time.
3. "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled " shall be construed accordingly.
4. "**Customer Data**" means any Personal Data that ahoy! processes on behalf of Customer as a Data Processor in the course of providing Services.
5. "**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data by ahoy! pursuant to the Agreement, including, where applicable, EU Data Protection Law.
6. "**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.
7. "**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.
8. "**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).
9. "**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.
10. "**Group**" means any and all Affiliates that are part of an entity's corporate group.
11. "**Personal Data**" means any information relating to an identified or identifiable natural person.
12. "**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of

Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

13. **“Privacy Shield Principles”** means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).
14. **“Processing”** has the meaning given to it in the GDPR and “process”, “processes”, and “processed” will be interpreted accordingly.
15. **“Security Incident”** means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.
16. **“Services”** means any product or service provided by ahoy! to Customer pursuant to the Agreement.
17. **“Sub-processor”** means any Data Processor engaged by ahoy! or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

2. **Relationship with the Agreement.**

1. The parties agree that this DPA will replace any existing data protection addendum or similar agreement the parties may have previously entered into in connection with the Services.
2. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA will prevail to the extent of that conflict.
3. Any claims brought under or in connection with this DPA will be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.
4. Any claims against ahoy! or its Affiliates under this DPA will be brought solely against the entity that is a party to the Agreement. Customer further agrees that any regulatory penalties or other liability incurred by ahoy! in relation to the Customer Data that arise as a result of, or in connection with, Customer’s failure to comply with its obligations under this DPA or any applicable Data Protection Laws will count toward and reduce ahoy!’s liability under the Agreement as if it were liability to the Customer under the Agreement.
5. No one other than a party to this DPA, its successors and permitted assignees will have any right to enforce any of its terms.
6. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

3. **Scope and Applicability of this DPA.**

1. This DPA applies where and only to the extent that ahoy! processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data

Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

2. Part A of this DPA (Sections 4 through 8, inclusive) will apply to the processing of Customer Data within the scope of this DPA beginning on the Effective Date.
 3. Part B of this DPA (Sections 9 through 12, inclusive) will apply to the processing of Customer Data within the scope of the DPA beginning 25 May 2018. For the avoidance of doubt, Part B will apply in addition to, and not in substitution for, the terms in Part A.
4. **PART A: DATA PROTECTION OBLIGATIONS. Roles and Scope of Processing.**
1. **Role of the Parties.** As between ahoy! and Customer, Customer is the Data Controller of Customer Data, and ahoy! will process Customer Data only as a Data Processor acting on behalf of Customer.
 2. **Customer Processing of Customer Data.** Customer agrees that: (i) it will comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to ahoy!; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Data Protection Laws for ahoy! to process Customer Data and provide the Services pursuant to the Agreement and this DPA.
 3. **ahoy! Processing of Customer Data.** ahoy! will process Customer Data only for the purposes described in the DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to ahoy! in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) will require prior written agreement between Customer and ahoy!.
 4. **Details of Data Processing.**
 1. *Subject matter.* The subject matter of the data processing under this DPA is the Customer Data.
 2. *Duration:* As between ahoy! and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.
 3. *Purpose:* The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of ahoy! pursuant to the Agreement (including this DPA) or as otherwise agreed by the parties.
 4. *Nature of the processing:* ahoy! provides an email service, automation and marketing platform, and other related services, as described in the Agreement.
 5. *Categories of data subjects:* Any individual accessing and/or using the Services through the Customer's Account ("**Users**"); and any individual: (i) whose email address is included in the Customer's subscriber list(s); (ii) whose information is stored on or collected via the Services, or (iii) to

whom Users send emails or otherwise engage or communicate with via the Services (collectively, "**Subscribers**").

6. *Types of Customer Data:*

- Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (account details, payment information); employment details (employer, job title, geographic location, area of responsibility);
- Subscribers: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

5. **Legitimate Interests.** Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that ahoy! will have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, ahoy! is the Data Controller of such data and accordingly will process such data in accordance with the ahoy! Privacy Policy and Data Protection Laws.

6. **Tracking Technologies.** Customer acknowledges that in connection with the performance of the Services, ahoy! employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Customer will maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable ahoy! to deploy Tracking Technologies lawfully on, and collect data from, the devices of Subscribers in accordance with and as described in the ahoy! Privacy Policy.

5. **Subprocessing.**

1. Authorized Sub-processors. Customer agrees that ahoy! may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors engaged by ahoy! and authorized by Customer as of the Effective Date are listed at
2. Sub-processor Obligations. ahoy! will: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause ahoy! to breach any of its obligations under this DPA.

6. **Security.**

1. **Security Policy.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, ahoy! will implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with ahoy!'s security standards described at: ("**Security Policy**").
2. **Updates to Security Measures.** Customer is responsible for reviewing the information made available by ahoy! relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Policy is subject to technical progress and development and that ahoy! may update or modify the Security Policy from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.
3. **Customer Responsibilities.** Notwithstanding the above, Customer agrees that except to the extent expressly provided in this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

7. **Security Reports and Audits.**

1. ahoy! is regularly audited by independent third party auditors. Upon request, ahoy! will supply a summary copy of its audit report(s) ("**Report**") to Customer, so that Customer can verify ahoy!'s compliance with the audit standards against which it has been assessed, and this DPA. Such Reports, as well as any conclusions or findings specified therein, are ahoy!'s Confidential Information.
2. ahoy! will also provide written responses to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm ahoy!'s compliance with this DPA, provided that Customer will not exercise this right more than once per year. Such responses are ahoy!'s Confidential Information.

8. **International Transfers.**

1. **Processing Locations.** ahoy! may transfer and process Customer Data anywhere in the world where ahoy!, its Affiliates or its Sub-processors maintain data processing operations. ahoy! will at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.
2. **Privacy Shield.** To the extent that ahoy! processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as

providing an adequate level of protection for Personal Data, the parties acknowledge that ahoy! will be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by virtue of having self-certified its compliance with Privacy Shield. ahoy! agrees to protect such Personal Data in accordance with the requirements of the Privacy Shield Principles. If ahoy! is unable to comply with this requirement, ahoy! will inform Customer.

3. **Alternative Transfer Mechanism.** The parties agree that the data export solution identified in Section 8.2 will not apply if and to the extent ahoy! adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under EU Data Protection Laws) outside of the EEA (“Alternative Transfer Mechanism”), in which event, the Alternative Transfer Mechanism will apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

9. PART B: GDPR OBLIGATIONS: Additional Security.

1. **Confidentiality of Processing.** ahoy! will ensure that any person who is authorized by ahoy! to process Customer Data (including its staff, agents and subcontractors) will be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).
2. **Security Incident Response.** Upon becoming aware of a Security Incident, ahoy! will notify Customer without undue delay and will provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

10. Changes to Sub-processors.

1. ahoy! will (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email will suffice) if it adds a Sub-processors at least ten (10) days prior to any such changes.
2. Customer may object in writing to ahoy!’s appointment of a new Sub-processor within five (5) days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If a resolution is not achieved within a reasonable amount of time, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

11. **Return or Deletion of Data.** Upon termination or expiration of the Agreement, ahoy! will (at Customer’s election) delete or return to Customer all Customer Data (including copies) in its possession or control, save that this requirement will not apply to the extent ahoy! is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data ahoy! will securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Cooperation.

1. **Data Subject Requests.** The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete, or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR including, for example, its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent Customer is unable to independently access the relevant Customer Data within the Services, ahoy! will (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event any such request is made directly to ahoy!, ahoy! will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If ahoy! is required to respond to such a request, ahoy! will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.
2. **Records of Processing.** Upon request from Customer, ahoy! will make available in a timely manner such information as is required by Customer to demonstrate ahoy!'s compliance with its obligations under EU Data Protection Law and under this DPA.
3. **Government Requests.** If a law enforcement agency sends ahoy! a demand for Customer Data (for example, through a subpoena or court order), ahoy! will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, ahoy! may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then ahoy! will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless ahoy! is legally prohibited from doing so.
4. **Data Protection Impact Assessments.** To the extent ahoy! is required under EU Data Protection Law, ahoy! will (at Customer's expense to the extent legally permitted) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

Ahoy Technologies, Inc d/b/a ahoy!

Customer

By:

By:

Name:

Name:

Title:

Title:

Date:

Date: