

CUSTOMER DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) amends and forms part of the written agreement between Ivory Consulting Corporation (“**Company**”) and you (“**Customer**”) titled Terms of Use, or an otherwise written agreement between Company and Customer (the “**Agreement**”). This DPA prevails over any conflicting term of the Agreement but does not otherwise modify the Agreement.

1. Definitions

1.1. In this DPA:

- a) “**Controller**”, “**Data Subject**”, “**Personal Data**”, “**Personal Data Breach**”, “**Processing**”, and “**Supervisory Authority**” have the meaning given to them in Data Protection Law. “**Data Subject**” includes “**Consumer**” as that term is defined under U.S. Privacy Laws;
- b) “**Customer Personal Data**” means Personal Data Processed by Company as a Processor on behalf of Customer or Third Party Controller;
- c) “**Data Protection Law**” means U.S. Privacy Laws, the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), their national implementations in the European Economic Area (“**EEA**”), including the European Union, and all other data protection laws of the EEA, the United Kingdom (“**UK**”), and Switzerland, each as applicable, and as may be amended or replaced from time to time;
- d) “**Data Subject Rights**” means Data Subjects’ rights to information, access, rectification, erasure, restriction, portability, objection, the right to withdraw consent, and the right not to be subject to automated individual decision-making in accordance with Data Protection Law;
- e) “**International Data Transfer**” means any disclosure of Customer Personal Data by an organization subject to Data Protection Law to another organization located outside the EEA, the UK, or Switzerland;
- f) “**Processor**” means “**Processor**,” “**Service Provider**,” or “**Contractor**” as those terms are defined in Data Protection Law.
- g) “**Sale**” and “**Selling**” have the meaning defined in the U.S. Privacy Laws.
- h) “**Services**” means the services provided by Company to Customer under the Agreement;
- i) “**Share**,” “**Shared**,” and “**Sharing**” have the meaning defined in the CCPA;
- j) “**Subprocessor**” means a Processor engaged by Company to Process Customer Personal Data;
- k) “**SCCs**” means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as amended or replaced from time to time;
- l) “**Third-Party Controller**” means a Controller for which Customer is a Processor; and
- m) “**UK Addendum**” means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).
- n) “**U.S. Privacy Laws**” means, collectively, all United States federal and state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the processing of individuals’ Personal Data and that do not apply solely to specific industry sectors (e.g., financial institutions), specific demographics (e.g., children), or specific classes of information (e.g., health or biometric information). U.S. Privacy Laws include, but are not limited to, the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (“**CCPA**”).

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

- 1.3. In the event of a conflict in the meanings of defined terms in Data Protection Law, the meaning from the Data Protection Law applicable to the relevant jurisdiction of the Data Subject applies.

2. Scope

- 2.1. This DPA applies to the Processing of Customer Personal Data by Company subject to Data Protection Law to provide the Services.
- 2.2. The subject matter, nature and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects are set out in **Annex I**, which is an integral part of this DPA.
- 2.3. Customer is a Controller and appoints Company as a Processor on behalf of Customer. Customer is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.
- 2.4. If Customer is a Processor on behalf of a Third-Party Controller, then Customer: is the single point of contact for Company; must obtain all necessary authorizations from such Third-Party Controller; and undertakes to issue all instructions and exercise all rights on behalf of such other Third-Party Controller.
- 2.5. Customer acknowledges that Company may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, technical support, and compliance with law. Company is the Controller for such Processing and will Process such data in accordance with Data Protection Law.
- 2.6. Company shall comply with the obligations of, and provide the level of privacy protection required by, Data Protection Law.

3. Instructions

- 3.1. Company will Process Customer Personal Data to provide the Services and in accordance with Customer's documented instructions.
- 3.2. The Controller's instructions are documented in this DPA, the Agreement, and any applicable statement of work.
- 3.3. Customer may reasonably issue additional instructions as necessary to comply with Data Protection Law. Company may charge a reasonable fee to comply with any additional instructions.
- 3.4. Company is prohibited from (i) Selling or Sharing Customer Personal Data, (ii) retaining, using, or disclosing Customer Personal Data for any purpose other than for the specific purpose documented in the Customer instructions, (iii) retaining, using, or disclosing Customer Personal Data outside of the direct business relationship between Customer and Company, and (iv) combining Customer Personal Data with Personal Data obtained from, or on behalf of, sources other than Customer, except as expressly permitted under applicable Data Protection Law.
- 3.5. Company certifies that it understands the Processing restrictions set forth in this DPA and will comply with them.
- 3.6. Unless prohibited by applicable law, Company will inform Customer if Company is subject to a legal obligation that requires Company to Process Customer Personal Data in contravention of Customer's documented instructions.

4. Personnel

- 4.1. Company will ensure that all personnel authorized to Process Customer Personal Data are subject to an obligation of confidentiality.

5. Security and Personal Data Breaches

- 5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in **Annex II**.

- 5.2. Customer acknowledges that the security measures in **Annex II** are appropriate in relation to the risks associated with Customer's intended Processing and will notify Company prior to any intended Processing for which Company's security measures may not be appropriate.
- 5.3. Company will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data. If Company's notification is delayed, it will be accompanied by reasons for the delay.

6. Subprocessing

- 6.1. Customer hereby authorizes Company to engage Subprocessors. A list of Company's current Subprocessors is available here: <https://www.ivorycc.com/subprocessors>
- 6.2. Company will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law.
- 6.3. Company will notify Customer prior to any intended change to Subprocessors by no less than five (5) business days' written notice to Customer. Customer may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Company's notification of the intended change. Customer and Company will work together in good faith to address Customer's objection. If Company chooses to retain the Subprocessor, Company will inform Customer at least thirty (30) days before authorizing the Subprocessor to Process Customer Personal Data, and either party may immediately discontinue providing or using the relevant parts of the Services, as applicable, and may terminate the relevant parts of the Services within thirty (30) days.

7. Assistance

- 7.1. Taking into account the nature of the Processing, and the information available to Company, Company will assist Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfillment of Customer's own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.
- 7.2. Company may charge a reasonable fee for assistance under this **Section 7**. If Company is at fault, Company and Customer shall each bear their own costs related to assistance.
- 7.3. Upon receiving notice from Company that it is unable to comply with Data Protection Law or this DPA, Customer may direct Company to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Customer Personal Data.

8. Audit

- 8.1. Upon reasonable request, Company must make available to Customer all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested no more than once per year by Customer, and performed by an independent auditor as agreed upon by Customer and Company. The foregoing shall only extend to those documents and facilities relevant and material to the Processing of Customer Personal Data and shall be conducted during normal business hours and in a manner that causes minimal disruption.
- 8.2. Company will inform Customer if Company believes that Customer's instruction under **Section 8.1** infringes Data Protection Law. Company may suspend the audit or inspection or withhold requested information until Customer has modified or confirmed the lawfulness of the instructions in writing.
- 8.3. Company and Customer each bear their own costs related to an audit.

9. International Data Transfers

- 9.1. Customer hereby authorizes Company to perform International Data Transfers to any country deemed to have an adequate level of data protection by the European Commission or the

competent authorities, as appropriate; on the basis of adequate safeguards in accordance with Data Protection Law; or pursuant to the SCCs and the UK Addendum referred to in **Sections 9.2 and 9.3**.

- 9.2. By signing this DPA, Company and Customer conclude Module 2 (controller-to-processor) of the SCCs and, to the extent Customer is a Processor on behalf of a Third-Party Controller, Module 3 (Processor-to-Subprocessor) of the SCCs, which are hereby incorporated and completed as follows: the “data exporter” is Customer; the “data importer” is Company; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented and the time period therein is specified in **Section 6.3** above; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of [Ireland]; the courts in Clause 18(b) are the Courts of [Dublin, Ireland]; Annex I and II to Module 2 and 3 of the SCCs are **Annex I and II** to this DPA respectively. For International Data Transfers from Switzerland, Data Subjects who have their habitual residence in Switzerland may bring claims under the SCCs before the courts of Switzerland.
- 9.3. By signing this DPA, Company and Customer conclude the UK Addendum, which is hereby incorporated and applies to International Data Transfers outside the UK. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the “Exporter” is Customer and the “Importer” is Company, their details are set forth in this DPA, and the Agreement; (ii) in Table 2, the first option is selected and the “Approved EU SCCs” are the SCCs referred to in **Section 9.2** of this DPA; (iii) in Table 3, Annexes 1 (A and B) and II to the “Approved EU SCCs” are **Annex I and II** respectively; and (iv) in Table 4, both the “Importer” and the “Exporter” can terminate the UK Addendum.
- 9.4. If Company’s compliance with Data Protection Law applicable to International Data Transfers is affected by circumstances outside of Company’s control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Customer and Company will work together in good faith to reasonably resolve such non-compliance. In the event that additional, replacement or alternative standard contractual clauses or UK standard contractual clauses are approved by Supervisory Authorities, Company reserves the right to amend the Agreement and this DPA by adding to or replacing, the standard contractual clauses or UK standard contractual clauses that form part of it at the date of signature in order to ensure continued compliance with Data Protection Law.

10. Liability

- 10.1. Where Company has paid compensation, damages or fines, Company is entitled to claim back from Customer that part of the compensation, damages or fines, corresponding to Customer’s part of responsibility for the compensation, damages or fines.

11. Termination and return or deletion

- 11.1. This DPA is terminated upon the termination of the Agreement.
- 11.2. Customer may request return of Customer Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Company will delete all remaining copies of Customer Personal Data within one hundred eighty (180) days after returning Customer Personal Data to Customer.

12. Applicable law and jurisdiction

- 12.1. This DPA is governed by the laws of the State of California, U.S.A. Any disputes relating to this DPA will be subject to the exclusive jurisdiction of the state courts located in and serving Contra Costa County, California, or the federal courts for the Northern District of California.

13. Modification of this DPA

- 13.1. This DPA may only be modified by a written amendment signed by both Company and Customer.

14. Invalidity and severability

- 14.1. If any provision of this DPA is found by any court or administrative body of a competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

ANNEX I

DESCRIPTION OF THE TRANSFER

A. LIST OF PARTIES

Data exporter:

- Name: Customer (as specified in the Agreement or the Services)
- Address: The address for Customer as specified in the Agreement or the Services
- Contact person's name, position and contact details: The contact details for Customer as specified in the Agreement or the Services
- Activities relevant to the data transferred under these Clauses: Customer receives Company's services as described in the Agreement and Customer provides Personal Data to Company in that context.
- Signature and date: By using the Company's Services to perform International Data Transfers, the Customer will be deemed to have signed this Annex I.
- Role (controller/processor): Controller, or Processor on behalf of Third-Party Controller

Data importer:

- Name: Company (as defined above)
- Address: The address for Company as specified in the Agreement or the Services
- Contact person's name, position and contact details: The contact details for Company as specified in the Agreement or the Services.
- Activities relevant to the data transferred under these Clauses: Company provides its services to Customer as described in the Agreement and Processes Personal Data on behalf of Customer in that context.
- Signature and date: By transferring Personal Data in the context of International Data Transfers on Customer's instructions, the Company will be deemed to have signed this Annex I.
- Role (controller/processor): Processor on behalf of Customer, or Subprocessor on behalf of Third-Party Controller

B. DESCRIPTION OF INTERNATIONAL DATA TRANSFER

- Categories of Data Subjects whose Personal Data is transferred:

#	Category of Data Subjects
1.	End users, website users and any other data subjects whose Personal Data the Customer may extract, transfer, and load onto the Services or who contact Ivory for support with respect to the Services.

- Categories of Personal Data transferred:

#	Category of Personal Data
1.	Data collected through cookies and other tracking technologies
2.	User account data and contact information, e.g. first and last name, email address, company, title, and phone number submitted during the signup process or otherwise provided to Company

- 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

#	Category of Sensitive Data	Applied restrictions or safeguards
1.	None expected	

- The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): *On a continuous basis.*
- Nature of the processing: *The Personal Data will be processed and transferred as described in the Agreement. The processing is incidental, and primarily pertains to ordinary business communication. Company does not expect to receive Customer's customer data in any form. Data Subjects are expected to be Customer's employees, subcontractors, etc, who contact Ivory.*
- Purpose(s) of the data transfer and further processing: *The Personal Data will be transferred and further processed for the provision of the Services as described in the Agreement. Data is transferred to facilitate support using our products and to make our software available via Company's websites.*
- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: *Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Law.*
- For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: *For the subject matter and nature of the Processing, reference is made to the Agreement and this DPA. The Processing will take place for the duration of the Agreement.*

C. COMPETENT SUPERVISORY AUTHORITY

- The competent authority for the Processing of Personal Data relating to Data Subjects located in the EEA is the Supervisory Authority a) of Customer's country of establishment, or, where not applicable, b) of the country where Customer's EU data protection representative is located, or, where not applicable, c) of one of the EEA countries where the Data Subjects are located.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in the UK is the UK Information Commissioner.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in Switzerland is the Swiss Federal Data Protection and Information Commissioner.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Company will, at a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Customer Personal Data are Processed, include:

- ☒ Establishing security areas, restriction of access paths;
- ☒ Establishing access authorizations for employees and third parties;
- ☒ Key management, card-keys procedures;
- ☒ Door locking (electric door openers etc.);
- ☒ Video/CCTV monitor, alarm system; and

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- ☒ User identification and authentication procedures;
- ☒ Strong ID/password security procedures (special characters, minimum length and complexity requirements, change of password);
- ☒ Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Customer Personal Data in accordance with their access rights, and that Customer Personal Data cannot be read, copied, modified or deleted without authorization, include:

- ☒ Internal policies and procedures;
- ☒ Differentiated access rights (profiles, roles, transactions and objects);
- ☒ Monitoring and logging of accesses;
- ☒ Disciplinary action against employees who access Customer Personal Data without authorization;
- ☒ Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Customer Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Customer Personal Data are disclosed, include:

- ☒ Encryption/tunneling;
- ☒ Transport security.

5. Control of instructions

Technical and organizational measures to ensure that Customer Personal Data are Processed solely in accordance with the instructions of the Controller include:

Unambiguous wording of the contract;

6. Availability control

Technical and organizational measures to ensure that Customer Personal Data are protected against accidental destruction or loss (physical/logical) include:

- ☒ Backup procedures;
- ☒ Mirroring of hard disks (e.g. RAID technology);
- ☒ Uninterruptible power supply (UPS);
- ☒ Remote storage;
- ☒ Anti-virus/firewall systems; and
- ☒ Disaster recovery plan.

7. Separation control

Technical and organizational measures to ensure that Customer Personal Data collected for different purposes can be Processed separately include:

- ☒ Separation of databases;
- ☒ Procedures for storage, amendment, deletion, transmission of data for different purposes.

8. Testing controls

Technical and organizational measures to test, assess and evaluate the effectiveness of the technical and organizational measures implemented in order to ensure the security of the processing include:

- ☒ Periodical review and test of disaster recovery plan;
- ☒ Testing and evaluation of software updates before they are installed;
- ☒ Authenticated (with elevated rights) vulnerability scanning; and

9. IT governance

Technical and organizational measures to improve the overall management of IT and ensure that the activities associated with information and technology are aligned with the compliance efforts include:

- ☒ Certification/assurance of processes and products;
- ☒ Processes for data minimization;
- ☒ Processes for limited data retention;
- ☒ Data subject rights policies.

Company will contractually require its Subprocessors to implement the same or at least equivalent technical and organizational measures to be able to provide assistance to Customer.