SAMPLE DATA PROCESSING AGREEMENT

Key: Language to be customised in yellow

Note: This sample Data Processing Agreement was created by a team of IAPP members volunteering on behalf of the IAPP Privacy Bar Section in the course of creating the book "Negotiating Data Processing Agreements," edited by Justin Weiss and to be published by the IAPP in fall, 2018. This is not legal advice. Please feel free to use and modify for your own purposes, and at your own risk. The footnotes at the end incorporate comments made by the volunteer attorneys that may provide insights or guidance in drafting certain of the sections of this Agreement. They are not intended to be included in actual contracts.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA PROCESSING AGREEMENT

BETWEEN:

[The data controller], a company incorporated under the laws of [country], having its registered office and principal place of business in [city] at [address], as registered with the [Chamber of Commerce] under number [number] (hereinafter to be referred to as: the "**Data Controller**"),

AND

[The data processor], a company incorporated under the laws of [country], having its registered office in [town] at [address] and principal place of business in [city] at [address], as registered with the [Chamber of Commerce] under number [number] (hereinafter to be referred to as: the "**Data Processor**").

HEREBY AGREE AS FOLLOWS:

1. **Subject matter of this Data Processing Agreement**

   1.1. This Data Processing Agreement applies exclusively to the processing of personal data that is subject to EU Data Protection Law[i] [in the scope of the agreement of [date] between the parties for the [provision of services]("Services") (hereinafter to be referred to as: the "**Service Agreement**").]

   1.2. The term EU Data Protection Law shall mean 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 (General Data Protection Regulation).

i Although an EU model is presumed here, other applicable laws could be substituted as-needed for a given contract.

1.3. Terms such as “Processing”, “Personal Data”, “Data Controller” and “Processor” shall have the meaning ascribed to them in the EU Data Protection Law.

1.4. Insofar as the Data Processor will be processing Personal Data subject to EU Data Protection Law on behalf of the Data Controller in the course of the performance of the Service Agreement with the Data Controller the terms of this Data Protection Agreement shall apply. An overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed is provided in Annex 2.

2. The Data Controller and the Data Processor

2.1. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Controller’s written instructions.

2.2. The Data Processor will only process the Personal Data on documented instructions of the Data Controller in such manner as - and to the extent that - this is appropriate for the provision of the Services, except as required to comply with a legal obligation to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Data Controller. The Data Processor shall never process the Personal Data in a manner inconsistent with the Data Controller’s documented instructions. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

2.3. The Parties have entered into a Service Agreement in order to benefit from the expertise of the Processor in securing and processing the Personal Data for the purposes set out in Annex 2. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Agreement.

2.4. Data Controller warrants that it has all necessary rights to provide the Personal Data to Data Processor for the Processing to be performed in relation to the Services. To the extent required by Applicable Data Protection Law, Data Controller is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the data subject, Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and Data Processor remains responsible for implementing any Data Controller instruction with respect to the further processing of that Personal Data.

3. Confidentiality

3.1. Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security[ii] [iii]

4.1. 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, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

---

ii GDPR Article 32(3): Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

iii Many data processors will want to rely upon certifications to demonstrate their compliance with security matters. They will want their independent auditors to test against the certificates. Controllers may want these broad rights to audit, but audits are time intensive and expensive and relying upon certifications may make more sense. If audits are to be performed, they should be narrowed to the what, where, when and how.

(a) measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Annex 2 of this Data Processing Agreement;

(b) In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;

(c) the pseudonymisation and encryption of personal data;

(d) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(e) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

(f) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data;

(g) measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller;

(h) the measures agreed upon by the Parties in Annex 3.

4.2. The Data Processor shall at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures set forth in Article 4.1.

4.3. At the request of the Data Controller, the Data Processor, shall demonstrate the measures it has taken pursuant to this Article 4 shall allow the Data Controller to audit and test such measures. The Data Controller shall be entitled on giving at least 14 days' notice to the Data Processor to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Data Processor, audits of the Data Processor´s premises and operations as these relate to the Personal Data. The Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller and shall grant the Data Controller´s auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Data Processor shall provide the Data Controller and/or the Data Controller´s auditors with access to any information relating to

the Processing of the Personal Data as may be reasonably required by the Data Controller to ascertain the Data Processor´s compliance with this Data Processing Agreement.

5. Improvements to Security

5.1. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction.

5.2. Where an amendment to the Service Agreement is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in applicable data protection law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

6. Data Transfers

6.1. The Data Processor shall immediately notify the Data Controller of any (planned) permanent or temporary transfers of Personal Data to a country outside of the European Economic Area without an adequate level of protection and shall only perform such a (planned) transfer after obtaining authorisation from the Data Controller, which may be refused at its own discretion. Annex 4 provides a list of transfers for which the Data Controller grants its consent upon the conclusion of this Data Processing Agreement.

6.2. To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

7. Information Obligations and Incident Management

7.1. When the Data Processor becomes aware of an incident that impacts the Processing of the Personal Data that is the subject of the Services Agreement, it shall promptly notify the Data Controller about the incident, shall at all times cooperate with the Data Controller, and shall follow the Data Controller's instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

7.2. The term "incident" used in Article 7.1 shall be understood to mean in any case:

(a) a complaint or a request with respect to the exercise of a data subject's rights under EU Data Protection Law;

(b) an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent;

(c) any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;

(d) any breach of the security and/or confidentiality as set out in Articles 3 and 4 of this Data Processing Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place;

(e) where, in the opinion of the Data Processor, implementing an instruction received from the Data Controller would violate applicable laws to which the Data Controller or the Data Processor are subject.

7.3. The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about an incident. Where the incident is reasonably likely to require a data breach notification by the Data Controller under applicable EU Data Protection Law, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller no later than 24 hours of having become aware of such an incident.

7.4. Any notifications made to the Data Controller pursuant to this Article 7 shall be addressed to the employee of the Data Controller whose contact details are provided in Annex 1 of this Data Processing Agreement, and shall contain:

(a) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;

(c) a description of the likely consequences of the incident; and

(d) a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

8. Contracting with Sub-Processors

8.1. [The Data Processor shall not subcontract any of its Service-related activities consisting (partly) of the processing of the Personal Data or requiring Personal Data to be processed by any third party without the prior written authorisation of the Data Controller].

[The Data Controller authorises the Data Processor to engage the sub-processors in the country locations for the Service-related activities specified as described in Annex 2. Data Processor shall inform the Data Controller of any addition or replacement of such sub-processors giving the Data Controller an opportunity to object to such changes.]

8.2. Notwithstanding any authorisation by the Data Controller within the meaning of the preceding paragraph, the Data Processor shall remain fully liable vis-à-vis the Data Controller for the performance of any such subprocessor that fails to fulfil its data protection obligations.

8.3. The consent of the Data Controller pursuant to Article 8.1 shall not alter the fact that consent is required under Article 6 for the engagement of sub-processors in a country outside the European Economic Area without a suitable level of protection.

8.4. The Data Processor shall ensure that the sub-processor is bound by the same data protection obligations of the Data Processor under this Data Processing Agreement, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of EU Data Protection Law.

8.5. The Data Controller may request that the Data Processor audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to ensure compliance with its obligations imposed by the Data Processor in conformity with this Agreement.

9. Returning or Destruction of Personal Data

9.1. Upon termination of this Data Processing Agreement, upon the Data Controller's written request, or upon fulfillment of all purposes agreed in the context of the Services whereby no further processing is required, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies.

9.2. The Data Processor shall notify all third parties supporting its own processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

10. Assistance to Data Controller

10.1. The Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under the GDPR.

10.2. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Section 4 (Security) and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.

10.3. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.[iv]

11. Liability and Indemnity

11.1. The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Controller and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Protection Law by the Data Processor. The Data Controller indemnifies the Data Processor and holds the Data Process harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Processor and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Law by the Data Controller.

12. Duration and Termination

12.1. This Data Processing Agreement shall come into effect on [date].

12.2. Termination or expiration of this Data Processing Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to Article 3.

12.3. The Data Processor shall process Personal Data until the date of termination of the agreement, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on instruction of the Data Controller.

13. Miscellaneous

13.1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Service Agreement, the provisions of this Data Processing Agreement shall prevail.

iv Processor and Controller may wish to add language regarding the parties' agreement as to the scope of the audit and the manner in which it may be performed - e.g., response written questionnaires, interviews, review of documents, onsite inspections?

13.2. This Data Processing Agreement is governed by the laws of [Country]. Any disputes arising from or in connection with this Data Processing Agreement shall be brought exclusively before the competent court of [Jurisdiction].

Signed for and on behalf of the Data Controller	Signed for and on behalf of the Data Controller
Name:	Name:
Title:	Title:
Date:	Date:

Annex 1:

Contact information of the [data protection officer/compliance officer] of the Data Controller.

[Contact information]

Contact information of the [data protection officer/compliance officer] of the Data Processor.

[Contact information]

Annex 2:

Personal data that will be processed in the scope of the Service Agreement and the purposes for which these data will be processed

---

Annex 3:

Security measures

Annex 4:

Transfers to countries outside the European Economic Area without a suitable level of protection for which the Data Controller has granted its authorisation: