SAMPLE DATA PROCESSING AGREEMENT

Key: Language to be inserted 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 B. Weiss and to be published by the IAPP in fall, 2018. It also reflects input provided by the global membership during an open comment period in Spring of 2018. This is not legal advice. Please feel free to use and modify for your own purposes, and at your own risk. The endnotes may provide insights or guidance in drafting or customising certain of the sections of this Agreement. They are not intended to be included in actual contracts. The forthcoming publication will discuss several provisions of the Agreement in greater detail.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA PROCESSING AGREEMENT[i]

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 to the processing of personal data subject to EU Data Protection Law [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**")].[ii]

   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).

1.3. Any capitalized terms not otherwise defined in this Data Processing Agreement shall have the meaning given to them in the Service Agreement. Except as modified below, the terms of the Service Agreement shall remain in full force and effect. Other terms used in this Data Processing Agreement that have meanings ascribed to them in the EU Data Protection law, including but not limited to "Processing", "Personal Data", "Data Controller" and "Processor," shall carry the meanings set forth under 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 Processing Agreement shall apply. In the event of a conflict between any provisions of the Service Agreement and the provisions of this Data Processing Agreement, the provisions of this Data Processing Agreement shall govern and control. An overview of the categories of Personal Data, the categories of Data Subjects, and the nature 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. Subject to the provisions of the Service Agreement, to the extent that the Data Processor's data processing activities are not adequately described in the Service Agreement, 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 and no Personal Data will be processed unless explicitly instructed by the Controller.

2.2. The Data Processor will only process the Personal Data on documented instructions of the Data Controller to the extent that this is required for the provision of the Services. Should the Data Processor reasonably believe that a specific processing activity beyond the scope of the Data Controller's instructions is required to comply with a legal obligation to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal obligation and seek explicit authorization from the Data Controller before undertaking such processing. 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 notify the Data Controller if, in its

opinion, any instruction infringes this Regulation or other Union or Member State data protection provisions. Such notification will not constitute a general obligation on the part of the Data Processor to monitor or interpret the laws applicable to the Data Controller, and such notification will not constitute legal advice to the Data Controller.

2.3. The Parties have entered into a Service Agreement in order to benefit from the capabilities 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, provided that all such discretion is compatible with the requirements of this Data Processing Agreement, in particular the Data Controller's written instructions.

2.4. The Data Controller warrants that it has all necessary rights to provide the Personal Data to the Data Processor for the Processing to be performed in relation to the Services, and that one or more lawful bases set forth in EU Data Protection Law support the lawfulness of the Processing. To the extent required by EU Data Protection Law, the Data Controller is responsible for ensuring that all necessary privacy notices are provided to data subjects, and unless another legal basis set forth in EU Data Protection Law supports the lawfulness of the processing, that any necessary data subject consents to the Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by a data subject, the Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and the Data Processor remains responsible for implementing Data Controller's instruction with respect to the 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 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

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, 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, at a minimum, the security measures agreed upon by the Parties in Annex 3.

4.2. Both the Data Controller and the Data Processor shall maintain written security policies that are fully implemented and applicable to the processing of Personal Data. At a minimum, such policies should include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on permanent staff who will have access to the Personal Data, conducting appropriate background checks,[iii] requiring employees, vendors and others with access to Personal Data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the Personal Data aware of information security risks presented by the Processing.

4.3. At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to this Article 4 and shall allow the Data Controller to audit and test such measures. Unless otherwise required by a Supervisory Authority of competent jurisdiction, the Data Controller shall be entitled on giving at least 30 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, and/or to ascertain the Data Processor's compliance with any approved code of conduct or approved certification mechanism referenced in Article 4.4.[iv]

4.4. The Data Processor's adherence to either an approved code of conduct or to an approved certification mechanism recognized under EU Data Protection Law may be used as an element by which the Data Processor may demonstrate compliance with the requirements set out in Article 4.1, provided that the requirements contained in Annex 3 are also addressed by such code of conduct or certification mechanism.[v]

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 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 EU Data Protection Law or by data protection authorities of competent jurisdiction.[vi]

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 EU 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 promptly notify the Data Controller of any planned permanent or temporary transfers of Personal Data to a third country, including a country outside of the European Economic Area without an adequate level of protection, and shall only perform such a 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 authorisation upon the conclusion of this Data Processing Agreement.[vii]

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 and that mechanism 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 suspend 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 has a material impact on 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 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 without undue delay after the Data Processor becomes 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, in order to assist the Data Controller in fulfilling its obligations under EU Data Protection Law, should 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.

8.2. The Data Controller authorises the Data Processor to engage the sub-processors listed in Annex 4 for the service-related Data Processing activities 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. If the Data Controller timely sends the Processor a written objection notice, setting forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve Data Controller's objection. In the absence of a resolution, the Data Processor will make commercially reasonable efforts to provide Data Controller with the same level of

service described in the Service Agreement, without using the sub-processor to process Data Controller's Personal Data. If the Data Processor's efforts are not successful within a reasonable time, each Party may terminate the portion of the service which cannot be provided without the sub-processor, and the Data Controller will be entitled to a pro-rated refund of the applicable service fees..

8.3. 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 sub-processor that fails to fulfill its data protection obligations.

8.4. The Data Processor shall ensure that the sub-processor is bound by data protection obligations compatible with those 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 Sub-processor 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 Sub-processor'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.[viii]

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 EU Data Protection Law. [ix]

10.2. Taking into account the nature of processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller in ensuring compliance with obligations pursuant to Section 4 (Security), as well as other Data Controller obligations under EU Data Protection Law that are relevant to the Data Processing described in Annex 2, including notifications to a supervisory authority or to Data Subjects, the process of undertaking a Data Protection Impact Assessment, and with prior consultations with supervisory authorities.

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.

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 arising out of a breach of this Data Processing Agreement and/or the EU Data Protection Law by the Data Processor. The Data Controller indemnifies the Data Processor and holds the Data Processor harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Processor arising out of a breach of this Data Processing Agreement and/or the EU Data Law by the Data Controller. [x]

12. Duration and Termination

12.1. This Data Processing Agreement shall come into effect on the effective date of the Service Agreement.

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 expiration or termination of the Service Agreement, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on instruction of the Data Controller.

13. Miscellaneous [xi]

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.

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 Processor
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:

Types of Personal Data that will be processed in the scope of the Service Agreement:

Categories of Data Subjects:

Nature and purpose of the Data Processing:

Annex 3: Security Measures [xii]

Data Processor shall:

1. 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;
2. take all reasonable measures to prevent unauthorized access to the Personal Data through the use of appropriate physical and logical (passwords) entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities;
3. build in system and audit trails;
4. use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and virus protection;
5. account for 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;
6. ensure pseudonymisation and/or encryption of Personal Data, where appropriate;
7. maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
8. maintain the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
9. implement 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;
10. monitor compliance on an ongoing basis;
11. implement measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller;
12. provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.

Annex 4:

Transfers to subprocessors in third countries, including countries outside the European Economic Area without an adequate level of protection for which the Data Controller has granted its authorisation:

Subprocessor Name	Country

Endnotes

i. Individual country laws may specify requirements to ensure an agreement is legally binding on all parties and this will vary from country to country. There may also be certain contractual provisions that are unenforceable as a matter of a specific country's approach to contract law. It is therefore important to review a final agreement from the perspective of both applicable data protection law and applicable contract law.

ii. Although an EU model is presumed here, other applicable laws from various global jurisdictions could be substituted as-needed for a given contract. Even in the EU context, certain parties choose to add provisions that reference related laws, such as national implementing laws or ePrivacy laws.

iii. It is recognized that verifications, checks and background investigations are regulated differently in various jurisdictions. The key concept here is that there should be control over which individuals are qualified and should be eligible at any given time to access the Personal Data.

iv. In general, audits typically have some agreed limitations as to advance notice, frequency, non-disruption, confidentiality of results, no access to confidential information of other customers, and costs. Where it is impracticable to have a cloud provider allow audits by all its customers on premises, it is common practice for such entities to seek reports, such as SOC 2 reports, which can be furnished to the Data Controller.

v. The focus should only be on referencing frameworks that have been formally approved by the appropriate EU Data Protection authorities. Approvals carry a special meaning under EU Data Protection law. As the parties are free to add additional obligations beyond the baseline requirements contained in EU Data Protection Law, the clause is designed to reflect this possibility.

vi. The Parties will need to agree how to allocate responsibility and costs should such changes be required. It may be useful to distinguish between aspects of the law that apply to Data Controllers vs. those aspects that apply to Data Processors. If the change in law relates to controller elements, then the controller might agree to be responsible for the costs of the implementation. If the change in law relates to processor elements, then the processor could be responsible.

vii. For ease of use, the attempt here is to reference authorisations for third country transfers and sub-processors in the same Annex 4. Should a conglomerate or multinational Data Processor wish to include a list of its affiliates as eligible recipients, it could do so in Annex 4.

viii. A Data Controller might consider requiring proof or a certificate of data destruction, particularly if return of data is impossible. In the latter case, it may be useful to specify an instruction about what to do with backups and archived copies of the Personal Data.

ix. Some Data Controllers may agree to take responsibility for the "reasonable costs incurred" by the Data Processor in providing such assistance.

x. The specific terms of an indemnity clause are unique to the context of each agreement. Many practitioners prefer to leave indemnity to the Service Agreement. If it must be included in a Data Processing Agreement, a practitioner may consider adding some standard support language (e.g. each Party providing the other a notice of the claim promptly after receiving it; giving the indemnifying party the right to control the defense; requiring the indemnified party to help and to avoid admission of liability").

xi. A practitioner might consider adding a separate (optional) paragraph here discussing Special Categories of Data (sensitive data) for which the Data Processor needs documented prior written instruction from Data Controller, as an alternative to addressing it in the Annex.

xii. The measures contained in this Annex are offered as suggestions by IAPP members as examples of common measures that may be considered

THIS PAGE INTENTIONALLY LEFT BLANK