**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

Convert Insights, Inc., a company incorporated under the laws of Delaware, having its registered office in at and principal place of business at 2093 Philadelphia Pike #9985 Claymont, DE 19703, USA as registered with the State of Delaware, Secretary of State, Division of Corporations under number 4717523 (hereinafter to be referred to as: the “**Data Processor**”).

THE PARTIES 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 “SaaS Subscription Agreement”)].2

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 Saas Subscription Agreement. Except as modified below, the terms of the Saas Subscription 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 Saas Subscription 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 Saas Subscription 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 Saas Subscription Agreement, to the extent that the Data Processor’s data processing activities are not adequately described in the Saas Subscription 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 Saas Subscription 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 organizational 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, 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.

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.

**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.

5.2. Where an amendment to the Saas Subscription 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 Saas Subscription 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.

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 Saas subscription 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:

1. 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.
2. the name and contact details of the Data Processor’s data protection officer or another contact point where more information can be obtained.
3. a description of the likely consequences of the incident.
4. 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 Subprocessors**

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 authorizes 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 the 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 Saas Subscription Agreement, without using the subprocessor 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 subprocessor, 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 subprocessor that fails to fulfill its data protection obligations.

8.4.The Data Processor shall ensure that the subprocessor 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 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 organizational measures, insofar as this is possible, for the fulfillment of the Data Controller’s obligation to respond to requests for exercising the data subject’s rights under the EU Data Protection Law.

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.

**12.Duration and Termination**

12.1.This Data Processing Agreement shall come into effect on the effective date of the Saas Subscription 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 Saas Subscription 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 Saas Subscription Agreement, the provisions of this Data Processing Agreement shall prevail.

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

| **For & on behalf of the Data Controller** | **For & on behalf of the Data Processor** |
| --- | --- |
| Signature:  | Signature:  |
| 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 Dionysia Kontotasiou of the Data Processor.

dionysia@convert.com

**Annex 2**

Types of Personal Data that will be processed in the scope of the Saas Subscription Agreement: (the categories may vary depending on the specific product and how you choose to configure it and may include):

* Unique Account ID;
* device screen resolution;
* device type,
* operating system,
* and browser type;
* console logs and errors;
* geographic location (country only);
* referring URL and domain;
* pages visited;
* date and time when your website was accessed and specific event on your website occured;
* attributes that you may choose to share with us via Convert API.

Categories of Data Subjects:

* End-users of the Controller’s websites which make use of the Platform provided by the Processor.
* authorized users (including but not limited to your employees, freelancers or contractors) from time to time to whom the Controller has granted the right to access the Platform in accordance with the terms of the Agreement;
* any other categories of Data Subjects as added by the Controller from time to time.

Nature and purpose of the Data Processing:

* Convert Experiences does not store any PII data but sets three cookies in order to run A/B experiences, track visitor actions and deliver consistent variations across page loads. These cookies are a small bit of text that accompanies requests and pages as they go between the Web server and browser. They keep track of the variation a user has viewed and help to serve the same variation to the user consistently; track goals completed by a user; and determine whether a user is a part of an experience.They are described here: <https://convert.zendesk.com/hc/en-us/articles/204495429-Convert-Experiences-Tracking-Cookies-Structure>. The sole purpose of collecting this data is that of improving the functionality of the website and enhancing the overall users and / or customer experience.

**Annex 3: Security Measures**

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 organizational 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**

**STANDARD CONTRACTUAL CLAUSES**

**SECTION I**

*Clause 1*

***Purpose and scope***

* 1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[[1]](#footnote-0) for the transfer of personal data to a third country.
	2. The Parties:
		+ 1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
			2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

* 1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
	2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*

***Third-party beneficiaries***

* 1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
		+ 1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
			2. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
			3. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
			4. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
			5. Clause 13;
			6. Clause 15.1(c), (d) and (e);
			7. Clause 16(e);
			8. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
	2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

* 1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
	2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
	3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*

***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Docking clause***

* 1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
	2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
	3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*

***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

**MODULE TWO: Transfer controller to processor**

**8.1 Instructions**

* 1. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
	2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

* 1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
	2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
	3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
	4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offenses (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[[2]](#footnote-1) (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

* + - 1. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
			2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
			3. the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
			4. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

* 1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
	2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
	3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
	4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
	5. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*

***Use of sub-processors***

**MODULE TWO: Transfer controller to processor**

* 1. OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter’s prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

* 1. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[[3]](#footnote-2) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
	2. The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
	3. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
	4. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*

***Data subject rights***

**MODULE TWO: Transfer controller to processor**

* 1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.
	2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
	3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*

***Redress***

* 1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**MODULE TWO: Transfer controller to processor**

* 1. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
	2. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
		+ 1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
			2. refer the dispute to the competent courts within the meaning of Clause 18.
	3. The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
	4. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
	5. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

***Liability***

**MODULE TWO: Transfer controller to processor**

* 1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
	2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
	3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
	4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.
	5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
	6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
	7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

***Supervision***

**MODULE TWO: Transfer controller to processor**

* 1. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

* 1. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

**MODULE TWO: Transfer controller to processor***(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

* 1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
	2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
		+ 1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
			2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[4]](#footnote-3);
			3. any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
	3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
	4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
	5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]
	6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

***Obligations of the data importer in case of access by public authorities***

**MODULE TWO: Transfer controller to processor***(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

**15.1 Notification**

* 1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
		+ 1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
			2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

* 1. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
	2. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]
	3. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
	4. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

* 1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
	2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]
	3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

*Clause 16*

***Non-compliance with the Clauses and termination***

* 1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
	2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
	3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
		+ 1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
			2. the data importer is in substantial or persistent breach of these Clauses; or
			3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

* 1. [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
	2. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*

***Governing law***

**MODULE TWO: Transfer controller to processor**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

*Clause 18*

***Choice of forum and jurisdiction***

**MODULE TWO: Transfer controller to processor**

* 1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
	2. The Parties agree that those shall be the courts of the Republic of Ireland.
	3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
	4. The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

**ANNEX I**

**A. LIST OF PARTIES**

**MODULE TWO: Transfer controller to processor**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

**B. DESCRIPTION OF TRANSFER**

**MODULE TWO: Transfer controller to processor**

Categories of data subjects whose personal data is transferred

* End-users of the Controller’s websites which make use of the Platform provided by the Processor.
* authorized users (including but not limited to your employees, freelancers or contractors) from time to time to whom the Controller has granted the right to access the Platform in accordance with the terms of the Agreement;
* any other categories of Data Subjects as added by the Controller from time to time

Categories of personal data transferred

* Unique Account ID;
* device screen resolution;
* device type,
* operating system,
* and browser type;
* console logs and errors;
* geographic location (country only);
* referring URL and domain;
* pages visited;
* date and time when your website was accessed and specific event on your website occured;
* attributes that you may choose to share with us via Convert API.

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.

N/A

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

Continuous Nature of the processing

Convert Experiences does not store any PII data but sets three cookies in order to run A/B experiences, track visitor actions and deliver consistent variations across page loads. These cookies are a small bit of text that accompanies requests and pages as they go between the Web server and browser. They keep track of the variation a user has viewed and help to serve the same variation to the user consistently; track goals completed by a user; and determine whether a user is a part of an experience.They are described here: <https://convert.zendesk.com/hc/en-us/articles/204495429-Convert-Experiences-Tracking-Cookies-Structure>.

Purpose(s) of the data transfer and further processing

The sole purpose of collecting this data is that of improving the functionality of the website and enhancing the overall users and / or customer experience.

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

As long as subscription is active

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

N/A

**C. COMPETENT SUPERVISORY AUTHORITY**

**MODULE TWO: Transfer controller to processor**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

*………………………….*

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

**MODULE TWO: Transfer controller to processor**

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

 *Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also* *describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

**ANNEX III – LIST OF SUB-PROCESSORS**

**MODULE TWO: Transfer controller to processor**

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorized the use of the following sub-processors as listed in the link below:

<https://www.convert.com/list-of-third-parties-with-whom-we-share-data/>

1. Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […]. [↑](#footnote-ref-0)
2. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses. [↑](#footnote-ref-1)
3. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-2)
4. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. [↑](#footnote-ref-3)