inCTRL | shared insights, new value

Data Processing Agreement (DPA)

Agreement for the processing of personal data on behalf of a controller pursuant to Article 28(3) and (4) of Regulation (EU) 2016/679 (“**General Data Protection Regulation**”, or “**GDPR**”).

This data processing agreement is effective as of the last signature date of a purchase order (“**Order**”) and is between inCTRL, Inc. (“**inCTRL**”) and the other signatory to the Order (“**Customer**”). inCTRL and Customer are parties to a Software as a Service Agreement (including the opsCTRL Terms & Conditions, Order or any other agreement referencing this DPA), hereinafter referred to as the “Main Agreement”.

1. SUBJECT MATTER OF THE AGREEMENT

For the provision of services under the Main Agreement, it is necessary for inCTRL to process personal data for which the Customer acts as the controller within the meaning of the data protection regulations (hereinafter referred to as "**Customer Data**"). This contract specifies the rights and obligations of the parties under data protection law in connection with inCTRL’s handling of Customer Data for the purpose of providing services under the Main Agreement.

2. SCOPE OF DATA PROCESSING

2.1 inCTRL shall process the Customer Data on behalf of and in accordance with the instructions of the Customer within the meaning of Art. 28 GDPR. The Customer shall remain the responsible controller in the sense of applicable data protection law.

2.2 The processing of Customer Data by inCTRL shall be carried out in the type, to the extent and for the purpose specified in Schedule 1 to this agreement; the processing concerns the types of personal data and categories of data subjects designated therein. The term of the processing shall correspond to the term of the Main Agreement.

2.3 inCTRL is permitted to process Customer Data outside the EU/EEA in compliance with the provisions of this Agreement and the requirements of Articles 44 - 48 of the GDPR are met or an exception pursuant to Article 49 of the GDPR applies. In case inCTRL processes Customer Data outside the EU/EEA, inCTRL and Customer shall enter into the Standard Contractual Clauses, as set out at Schedule 4 to this agreement, such clauses being incorporated into and forming part of this agreement. To the extent that this agreement conflicts with the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

3. INSTRUCTION OF THE CUSTOMER

3.1 InCTRL shall process the Customer Data in accordance with the Customer's instructions, unless inCTRL is required by law to process them otherwise. In the latter case, inCTRL shall notify the Customer of these legal requirements prior to processing, unless the relevant law prohibits such notification due to an important public interest.

3.2 In general, the instructions of the Customer regarding the inCTRL data processing on behalf of Customer are conclusively defined and laid down in the provisions of this agreement. Individual instructions which deviate from the provisions of this agreement, or which impose additional requirements shall require the prior consent of inCTRL. Any additional costs incurred by inCTRL because of such deviating instructions shall be borne by the Customer.

3.3 InCTRL warrants that it will process the Customer Data in accordance with the Customer's instructions. If inCTRL is of the opinion that an instruction of the Customer violates this agreement or the applicable data protection law, it shall be entitled, after notifying the Customer accordingly, to suspend the execution of the instruction until the Customer confirms the instruction. The parties agree that the sole responsibility for the processing of the Customer Data in accordance with the instructions lies with the Customer.

4. CUSTOMER AS THE DATA CONTROLLER

The Customer shall be solely responsible for the lawfulness of the processing of the Customer Data as well as for the protection of the rights of the data subjects in the relationship between the parties. Should third parties assert claims against inCTRL based on the processing of Customer Data in accordance with this Agreement, the Customer shall indemnify inCTRL against all such claims upon first request.

5. REQUIREMENTS FOR PERSONNEL

InCTRL shall require all person’s processing Customer Data to maintain confidentiality with respect to the processing of Customer Data.

6. SECURITY OF PROCESSING

6.1 InCTRL shall, in accordance with Article 32 of the GDPR, take the necessary, appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing of the Customer Data as well as the varying likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection for the Customer Data appropriate to the risk.

6.2 InCTRL is permitted to change or adapt technical and organizational measures during the term of the contract if they continue to meet the legal requirements.

7. SUBPROCESSORS

7.1 The Customer hereby grants inCTRL general permission to involve further processors regarding the processing of Customer Data. The subprocessors engaged at the time of conclusion of the agreement are listed in Schedule 3.

7.2 InCTRL shall inform the Customer of any intended changes regarding the involvement or replacement of further subprocessors. In individual cases, the Customer shall have the right to object to the engagement of additional subprocessors. An objection may only be raised by the Customer for good cause to be proven to inCTRL. If the Customer does not raise an objection within 14 days after receipt of the notification, its right to object to the corresponding sub-processor engagement shall expire. If the Customer raises an objection, inCTRL shall be entitled to terminate the Main Agreement and this agreement with a notice period of 3 months.

7.3 The agreement between inCTRL and the additional sub-processor shall impose the same obligations on the latter as are imposed on inCTRL by virtue of this agreement. The parties agree that this requirement is met if the contract has a level of protection corresponding to this agreement or if the obligations set out in Article 28 (3) of the GDPR are imposed on the sub-processor.

7.4 Subject to compliance with the requirements of Section 2.3 of this Agreement, the rules in this Section 7 shall also apply if a sub-processor in a third country is involved.

8. DATA SUBJECT RIGHTS

8.1 InCTRL shall support the Customer with technical and organizational measures within the scope of what is reasonable to comply with its obligation to respond to legitimate data subject requests.

8.2 Insofar as a data subject asserts a legitimate request directly against inCTRL, inCTRL shall forward this request to the Customer in a timely manner.

8.3 InCTRL shall enable the Customer to correct, delete or restrict the further processing of the Customer Data within the scope of what is reasonable and necessary.

9. NOTIFICATION AND SUPPORT OBLIGATIONS OF INCTRL

9.1 Insofar as the Customer is subject to a statutory obligation to report or notify a breach of the protection of Customer Data (in particular pursuant to Art. 33, 34 DSGVO), inCTRL shall inform the Customer in a timely manner of any reportable events in its area of responsibility. InCTRL shall support the Customer in fulfilling the reporting and notification obligations at the Customer's request within the scope of what is reasonable and required if the Customer bears the expenses and costs incurred by inCTRL as a result.

9.2 InCTRL shall assist the Customer within the scope of what is reasonable and required in any data protection impact assessments to be carried out by the Customer and any subsequent consultations with the supervisory authorities pursuant to Art. 35, 36 of the GDPR against reimbursement of the expenses and costs incurred by inCTRL for such assistance.

10. DELETION OF DATA

10.1 InCTRL shall delete the Customer Data after termination of this Agreement, unless inCTRL is legally obliged to continue storing the Customer Data.

10.2 Documentation which serves as proof of the proper processing of the Customer Data in accordance with the data processing may be retained by inCTRL even after the end of the contract.

11. DEMONSTRATION OF COMPLIANCE

11.1 InCTRL shall provide the Customer with all necessary information available to inCTRL to prove compliance with its obligations under this Agreement at the Customer's request.

11.2 The Customer shall be entitled to verify inCTRL's compliance with the provisions of this agreement, in particular the implementation of the technical and organizational measures, including by means of inspections.

11.3 In order to carry out inspections in accordance with Section 11.2, the Customer shall be entitled to enter inCTRL's business premises where Customer Data are processed during normal business hours (Monday to Friday from 10 a.m. to 6 p.m.) after timely advance notice in accordance with Section 11.5 at its own expense, without disrupting the course of business and subject to strict confidentiality of inCTRL's trade and business secrets.

11.4 InCTRL shall be entitled, at its own discretion and taking into account the Customer's statutory obligations, not to disclose information which is sensitive with regard to inCTRL's business or if inCTRL would violate statutory or other contractual provisions by disclosing it. The Customer shall not be entitled to have access to data or information on other customers of inCTRL, to information regarding costs, to quality review and contract management reports as well as to any other confidential data of inCTRL which are not directly relevant for the agreed review purposes.

11.5 The Customer shall inform inCTRL in due time (as a rule at least two weeks in advance) about all circumstances related to the performance of the review. The Customer may carry out one inspection per calendar year. Further inspections shall be carried out if the Customer bears the related costs and after coordination with inCTRL.

11.6 If the Customer commissions a third party to carry out the inspection, the Customer shall obligate the third party in writing in the same way as the Customer is obligated to inCTRL on the basis of this Section 11 of this Agreement. In addition, the Customer shall oblige the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional confidentiality obligation. Upon request of inCTRL, the Customer shall immediately submit to inCTRL the obligation agreements with the third party. The Customer may not commission a competitor of inCTRL with the inspection.

11.7 At inCTRL's option, proof of compliance with the obligations under this contract may also be provided by providing a suitable, up-to-date certificate or report by an independent body (e.g., auditor, audit, data protection agency, etc.) instead of the above-mentioned inspection.

12. TERM AND TERMINATION

The term and termination of this Agreement shall be governed by the provisions governing the term and termination of the Main Agreement. Termination of the main contract shall automatically result in termination of this agreement. An isolated termination of this contract is excluded.

13. LIABILITY

The liability of inCTRL under this agreement shall be subject to the exclusions and limitations of liability under the Main Agreement.

14. FINAL PROVISIONS

14.1 Should individual provisions of this agreement be or become invalid or contain a gap in regulation, the remaining provisions shall remain unaffected. The parties undertake to replace the invalid provision with a legally permissible provision that comes as close as possible to the purpose of the invalid provision and meets the requirements of Article 28 of the GDPR.

14.2 In the event of contradictions between this agreement and other agreements between the parties, in particular the Main Agreement, the provisions of this agreement shall prevail.

SCHEDULE 1

DATA PROCESSING PARTICULARS

The subject matter of the processing	The subject matter of the processing is the performance of the Services pursuant to the Software License Agreement between inCTRL and Customer. For the service to properly function, personal data such as first and last name and email addresses have to be processed by inCTRL. In specific cases, Customer Data might include personal data captured via a camera.
The nature of the processing	Customer employee uploads personal data such as Customer employee data to a database that is controlled by inCTRL (Software-as-a-Service).
The type of Customer Data being processed	• First and last name • Email address • Optional: Picture, job title, department, and name of manager • Other personal data potentially entered by end users of the services into the services
The categories of data subjects	• Customers’ employees • Contractors • Consultants • Other individuals Customer grants access to the inCTRL services

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

inCTRL together with its sub-processor Amazon Web Services maintains the following technical and organizational measures in order to ensure a level of protection appropriate to the risk:

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control
  - EMPLOYEE DATA CENTER ACCESS
    AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.
  - THIRD-PARTY DATA CENTER ACCESS
    Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.
- Surveillance and Detection
  - CCTV
    Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.
  - DATA CENTER ENTRY POINTS
    Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.
  - INTRUSION DETECTION
    Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and

egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

- Monitoring and Logging
  - DATA CENTER ACCESS REVIEW
    Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

  - DATA CENTER ACCESS LOGS
    Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

  - DATA CENTER ACCESS MONITORING
    We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analysing, and dispatching responses

- Electronic Access Control
  No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media.

- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events

- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Device Management
  - ASSET MANAGEMENT
    AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

  - MEDIA DESTRUCTION
    Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

- Operational Support Systems
  - POWER
    AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.
  - CLIMATE AND TEMPERATURE
    AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.
  - FIRE DETECTION AND SUPPRESSION
    AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.
  - LEAKAGE DETECTION
    In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

- Data Transfer Control
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature.

- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management.

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control
  Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site, virus protection, firewall, reporting procedures and contingency planning.

- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR).
- Infrastructure Maintenance
  - EQUIPMENT MAINTENANCE
    AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

  - ENVIRONMENT MANAGEMENT
    AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
  No third-party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

- Governance & Risk
  - ONGOING DATA CENTER RISK MANAGEMENT
    The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

  - THIRD-PARTY SECURITY ATTESTATION
    Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

SCHEDULE 3

SUB-PROCESSORS

Name	Address	Services	Location
inCTRL Solutions Inc.	7 Innovation Dr. | Suite 107, Dundas, Ontario | L9H 7H9	Support Services	Canada
Twilio	San Francisco, USA	Processing text message and voice alerts for system alarms and warnings.	USA
PIWIK PRO	Kurfürstendamm 21 10719 Berlin	Shows anonymized analytics of application usage. Tracks analytic cookies.	Germany
Stonly	36 rue Chaptal, 92300 Levallois, USA	Overlays instructional documentation within our applications. Uses cookies to track logins but anonymizes the data to us.	USA
Amazon Web Services	Seattle, USA	Storage and processing of all our data is in the AWS cloud infrastructure.	USA
Vimeo	New York, USA	Video storage of individuals uploading content.	USA

SCHEDULE 4

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) 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) for the transfer of personal data to a third country.

(a) The Parties:

(i) 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

(ii) 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").

(b) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(c) 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

(a) 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.

(b) 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

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) 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);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) 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.

Clause 7 - Optional

Docking clause

(a) 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.

(b) 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.

(c) 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 organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) 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.

(b) 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

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised 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 organisational 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.

(b) 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 authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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.

(d) 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 offences (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[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:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) 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;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

[1] 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.

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

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) 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.

(c) 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.

(d) 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.

(e) 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

(a) 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 one month 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.

(b) 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. 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.

(c) 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.

(d) 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.

(e) 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

(a) 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 authorised to do so by the data exporter.

(b) 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 organisational 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.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) 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.

(b) 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.

(c) 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:

(i) 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;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) 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

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) 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. 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

(a) 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.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) 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;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational 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.

(c) 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.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) 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).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. 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 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

15.1 Notification

(a) 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:

(i) 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

(ii) 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.

(b) 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.

(c) 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.).

(d) 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.

(e) 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

(a) 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).

(b) 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.

(c) 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

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) 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).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) 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;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) 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 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.

(d) 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. 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.

(e) 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

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 Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Munich, Germany.

(c) 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.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Customer

Address: The Adress is set out in the Order.

Contact person's name, position and contact details: The contact details are set out in the Order.

Activities relevant to the data transferred under these Clauses: Customer uploads Customer personal data to database operated by inCTRL (Software-as-a-Service).

Role (controller/processor): Controller

Data importer(s):

1. Name: inCTRL Corp.

Address: 2825 East Cottonwood Parkway, Suite 500, Cottonwood Heights, UT 84121, USA

Contact person's name, position and contact details: Dave Williams, williams@inctrl.com

Activities relevant to the data transferred under these Clauses: inCTRL uses Customer personal data in order to be able to provide the services to Customer (Software-as-a-Service).

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Customers' employees
- Contractors
- Consultants
- Other individuals Customer grants access to the inCTRL services

Categories of personal data transferred

- First and last name
- Email address
- Optional: Picture, job title, department, and name of manager
- Other personal data potentially entered by end users of the services into the services

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive datais being transferred.

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

Data is being transferred on a continuous basis, i.e. as long as the Customer uses the inCTRL services.

Nature of the processing

The Customer uploads personal data such as Customer employee data to a database that is controlled by inCTRL (Software-as-a-Service).

Purpose(s) of the data transfer and further processing

The purpose of the processing is to enable the Customer to use the inCTRL services.

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

In general, personal data will be retained for such periods as are necessary in relation to the purpose for which they were collected or otherwise processed. Something else might apply if retaining personal data is necessary for compliance with statutory obligations, such as statutory retention requirements resulting from tax or commercial requirements.

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

Please see Schedule 3 – Sub-Processors.

C. COMPETENT SUPERVISORY AUTHORITY

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Promenade 18

91522 Ansbach , Germany

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

Please refer to Schedule 2.

ANNEX III – LIST OF SUB-PROCESSORS

Please refer to Schedule 3.