DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements and forms part of the agreement between Poka and the Customer (the "**Agreement**"), effective as of the date set out in the Agreement or the applicable Order (the **"Effective Date"**). This DPA will remain in effect for the duration of the Agreement (the **"Term"**). Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

NOW, THEREFORE, the Parties agree as follows:

1.

1. DEFINITIONS

"**CCPA**" means the *California Consumer Privacy Act*, Cal. Civ. Code § 1798.100 et seq., as amended by the *California Privacy Rights Act*, and its implementing regulations.

"**Data Protection Laws**" means all applicable laws, rules and other legally binding instruments governing the Processing of Personal Data under this DPA, including, where applicable, (i) data protection and privacy laws of the United States, (ii) the GDPR; (iii) the *Personal Information Protection and Electronic Documents Act* (PIPEDA) of Canada and applicable provincial privacy laws, including the *Act respecting the protection of personal information in the private sector* (Québec), in each case as amended, replaced, or superseded from time to time.

"**GDPR**" means Regulation (EU) 2016/679 (General Data Protection Regulation) , including any amendments, replacements, or subsequent legislation.

"**Personal Data**" has the meaning found in Data Protection Laws where such data is Customer Data.

"**Poka Personnel**" means all Poka employees and consultants, including but not limited to personnel engaged through third-party service providers such as employers of record, staffing agencies, or similar intermediaries (such personnel shall be deemed to perform the Services on behalf of Poka).

"**Security Exhibit**" means the exhibit detailing the technical and organizational security measures applicable to the Software Services, available at: https://artifacts.poka.io/Security_Exhibit_EN.pdf.

"**Services**" means the Software Services as defined in the Agreement or, if not defined in the Agreement, Software Services shall mean the generally available software-as-a-service offering hosted on behalf of Poka and ordered by or for Customer to make available to authorized users, as set forth in an order form.

"Standard Contractual Clauses" means the standard contractual clauses for Processors as approved by the European Commission (implementing Decision (EU) 2021/914 of June 4th 2021) and attached hereto as **Schedule 4** to this DPA as may be amended, superseded or replaced.

"Sub-Processor" means any Processor engaged by Poka to process Personal Data on its behalf.

"**TOMS**" means the appropriate technical and organisational measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing.

The terms "**Controller**", "**Processor**", "**Data Subject**", "**Data Subject Rights**", "**Member State**", and "**Processing**" shall have the meaning given to them under the GDPR.

2. APPLICATION

2.1 Relationship of the Parties. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Poka is the Processor.

3. RESPONSIBILITIES OF THE PARTIES

3.1 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Poka as a Processor. Customer shall have sole responsibility for the means by which Customer acquired Personal Data. Customer acknowledges and agrees that its use of the Services will not violate the right of any Data Subject, including those that have opted-out from sales or other disclosures of

Personal Data, to the extent applicable under the CCPA.

3.2 Poka's Processing of Personal Data. Poka shall Process Personal Data on behalf of Customer solely (i) in accordance with Customer's lawful and documented instructions; (ii) for the purposes of providing, improving, enhancing and developing the Services as described in the Agreement; (iii) as otherwise required by Data Protection Laws. The duration of the Processing, the nature and purpose of the Processing, the categories of Personal Data and Data Subjects are described in **Schedule 1** of this DPA.

3.3 Poka Personnel. Poka shall grant access to Personal Data only to Poka Personnel engaged in the Processing of Personal Data who have a need to know such information. Poka Personnel shall perform their duties in a professional and workmanlike manner, and more specifically, in compliance with **Section 2.1** of the Security Exhibit. Poka has appointed a data protection officer who may be reached at privacy@poka.io.

4. DATA SUBJECT RIGHTS

4.1 Data Subject Request. Poka shall, to the extent legally permitted, notify Customer, without undue delay, of any complaint, dispute or request it has received from a Data Subject ("**Data Subject Requests**"). Poka shall not independently respond to a Data Subject Request, except that Customer authorizes Poka to forward or redirect such Data Subject Requests as necessary to enable Customer to respond directly, in accordance with Data Protection Laws.

5. SUB-PROCESSORS

5.1 Current List of Sub-Processors. As of the Effective Date, the current list of Sub-Processors engaged in Processing Personal Data for the purpose of providing the Services, including a description of their processing activities and country of location, is available at https://artifacts.poka.io/Poka_Subprocessors_EN.pdf. Customer hereby generally consents to the use of these Sub-Processors, including their locations and processing activities, insofar as they relate to the Processing of Personal Data.

5.2 Authorized Sub-Processors. Subject to **Section 5.3**, Customer grants Poka the general authorization to engage Sub-Processors to Process Personal Data for the purpose of providing the Services pursuant to the Agreement. Poka shall (i) perform adequate due diligence on each Sub-Processor to ensure that it can provide a level of protection for Personal Data that is consistent with the requirements of this DPA, and (ii) enter into a written agreement with each Sub-Processor which (a) contains data protection obligations no less protective of Personal Data than Poka's obligations under this DPA, and (b) requires that each Sub-Processor comply with Data Protection Laws and Process Personal Data in accordance with the terms of this DPA.

5.3 Notification and Objection Right for New Sub-Processors. Poka shall inform Customer of additions or replacements of Sub-Processors by notifying Customer's contacts who have subscribed to notifications through the subprocessor online webpage available at https://www.poka.io/en/subprocessors (or a successor URL designated by Poka), thereby giving Customer the opportunity to object to such changes on data protection grounds by notifying Poka in writing within ten (10) days of receipt of Poka's notification. In the event Customer objects to a new Sub-Processor, Poka shall use reasonable efforts to avoid Processing of Personal Data by the objected Sub-Processor and work with Customer in order to achieve resolution. If Customer can reasonably demonstrate that the new Sub-Processor is unable to Process Personal Data in compliance with the terms of this DPA and Poka cannot provide an alternative Sub-Processor, or if the Parties are otherwise not able to achieve resolution, Customer may, as its sole and exclusive remedy, terminate without penalty only the portion of the Services which cannot be provided by Poka without the use of the objected-to Sub-processor.

5.4 Liability. Poka shall be liable for the acts and omissions of its Sub-Processors to the same extent Poka would be liable if performing the Services of each Sub-Processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

6. DATA TRANSFERS

6.1 Data Locations. Customer acknowledges that Poka may transfer and process Personal Data to and in the United States and anywhere else in the world where Poka or its Sub-Processors maintain data processing operations. Poka will ensure at all times that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

6.2 Transfer Mechanism. Any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their Member States, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing countries, to the extent such transfers are subject to Data Protection Laws, shall be made under the Standard Contractual Clauses set forth in **Schedule 4** to this DPA.

7. SECURITY

7.1 Technical and Organizational Measures. Poka shall maintain appropriate TOMS for protection of the security (including protection against Security Incident), confidentiality and integrity of Personal Data, as set forth in **Schedule 2** to this DPA. Customer acknowledges that Poka may update TOMS from time to time, provided that any updates do not materially diminish the overall protection afforded to Personal Data during the Term of the Agreement.

7.2 Security Incident Notification. Poka shall notify Customer of any Security Incident affecting Personal Data without undue delay, and, in any event, no later than seventy-two (72) hours after Poka becomes aware of such Security Incident. Such notifications shall be provided to Customer via the email address designated by Customer in its account.

7.3 Assistance. To the extent applicable to Poka's Processing activities under the DPA, Poka shall assist Customer in complying with its obligations under Data Protection Laws, including notifying Data Subjects or any competent supervisory authority of a Security Incident. Such assistance shall be provided to the extent commercially reasonably practicable, taking into account the nature of the Processing and the information available to Poka. Poka shall take commercially reasonable steps to contain, investigate, and mitigate the effects of any Security Incident, and shall provide Customer with timely information regarding such Security Incident as it becomes available. Poka's notification of or response to a Security Incident under **Section 7.2** shall not be construed as an acknowledgment by Poka of any fault or liability with respect to such Security Incident.

8. AUDITS

8.1 Audit Reports. Customer may access and review up-to-date attestations, certifications, reports or extracts thereof from independent bodies or other suitable certifications ("**Audit Report**") provided by Poka to ensure compliance with the terms of this DPA.

8.2 Audit Rights. In cases where an Audit Report is not sufficient for Customer to demonstrate Poka's compliance with the terms of this DPA, Customer will have the right to remotely audit such compliance, but only to the extent required under Data Protection Laws. The Parties agree that all such audits will be conducted: (i) upon reasonable notice to Poka; (ii) only once per year unless there are specific indications that, in Customer's reasonable opinion, require a more frequent audit or, to the extent further audits are required by Data Protection Laws; (iii) only during Poka's normal business hours; and (iv) in a manner that does not disrupt Poka's day-to-day operations.

8.3 Audit Terms. Customer will enter into a confidentiality agreement with Poka prior to conducting an audit. Before the commencement of any such audit, Customer and Poka shall mutually agree upon the scope, timing, and duration of the audit. Customer shall bear the costs for any audit initiated by Customer and if the audit reveals material non-compliance with the requirements of this DPA, Poka will bear the costs of the remediation measures to be put in place to restore compliance.

8.4 Third-Party Auditor. To conduct such audits, Customer may engage a third-party auditor subject to such auditor complying with confidentiality requirements under **Section 8.3** and provided such auditor is suitably qualified, independent, and not a competitor of Poka.

8.5 Findings. Poka will notify Customer of any non-compliance discovered during an audit, and shall use commercially reasonable efforts to address any confirmed non-compliance.

8.6 Data Protection Impact Assessment. Upon Customer's request, Poka shall provide Customer with reasonable cooperation and assistance as needed to fulfill Customer's obligation under Data Protection Laws to carry out a data protection assessment ("DPIA") related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Poka. Customer shall pay Poka mutually agreed charges for providing such assistance, to the extent that such assistance cannot be reasonably accommodated within the normal provision of the Services.

9. DELETION AND RETURN OF PERSONAL DATA

9.1 Retention Period. Following termination of the Agreement for any reason or expiration of its Term, Poka will retain Personal Data for sixty (60) days from such date of termination or expiration (“**Retention Period**”). Upon the expiration of the Retention Period, Poka will securely delete all Personal Data in its possession or control in accordance with Data Protection Laws. Subject to any applicable laws or regulations, Poka may retain a copy of any document or material that Poka may otherwise be required to return or destroy for audit purposes only.

9.2 Customer Request. At the Customer’s request within the Retention Period, Poka may return a copy of all Personal Data to Customer or provide a self-service functionality allowing Customer to do the same, and delete all other copies of Personal Data Processed by Poka or any Sub-Processors, and provide Customer with written confirmation of such deletion within fifteen (15) days of deletion.

10. CCPA OBLIGATIONS

10.1 Definitions. In this Section, the following terms “**Business**”, “**Service Provider**”, “**Consumers**”, “**Sell**”, and “**Share**”, shall have the meaning given in the CCPA. For the avoidance of doubt, the definition of “**Personal Data**” in this Section has the meaning found in the CCPA where such personal information, namely information that identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a personal consumer or household, is Customer Data.

10.2 Application and CCPA Obligations. Notwithstanding anything to the contrary in the DPA, this Section shall apply to the Personal Data of the residents of the State of California, USA. To the extent Poka receives or has access to Personal Data about California residents in connection with the provision of Services to Customer under the Agreement, Customer is the Business and Poka is the Service Provider. When Poka Processes Personal Data on behalf of Customer, Poka shall not:

a) Sell or Share Personal Data that Poka processes on Customer’s behalf pursuant to the Agreement and the DPA, or otherwise make Personal Data available to any third party for monetary or other valuable consideration;

b) Retain, use or disclose Personal Data for any purpose other than for the specific purposes set forth in the Agreement, the DPA and as part of the direct relationship between Customer and Poka;

c) except as otherwise permitted by Data Protection Laws or Customer, combine Personal Data with Personal Data that Poka receives from or on behalf of another person or persons.

10.2.1 Customer acknowledges and agrees that Customer shall be responsible for providing the required notice to Consumers with respect to sharing their Personal Data with Poka.

10.2.2 Poka acknowledges that Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate the unauthorized use of the Personal Data.

10.2.3 During the Term of the Agreement, to the extent that Customer, in Customer's use of the Services, do not have the ability to address a request from Consumers, including a request to delete Personal Data, Poka shall provide reasonable cooperation to assist Customer to respond to such requests from Consumers relating to the Processing of Personal Data under the Agreement and/or the DPA when Customer is required to respond to such requests under CCPA, subject to the provisions under CCPA. In the event that any such request is made directly to Poka, Poka shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so, except to confirm that such request relates to Customer to which Customer hereby agrees.

10.2.4 Poka shall notify without undue delay Customer if Poka determines or reasonably suspects its inability to comply with the obligations set forth in **Section 10**. Upon any such notice to Customer, Poka shall immediately cease all use of Personal Data of California residents.

10.2.5 Poka certifies that Poka understands the restrictions set forth in **Section 10**, and will comply with such restrictions and all applicable obligations under the CCPA throughout the Term of the Agreement.

11. GENERAL

11.1 Governing Law. This DPA will be governed by and construed in accordance with the governing law of the Agreement and any dispute between Parties will be subject to the exclusive jurisdiction of the forum set forth in the Agreement, unless otherwise required by Data Protection Laws.

11.2 Term. This DPA will commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, Poka's deletion of all Personal Data as described in this DPA.

11.3 Amendments. Where amendments are required to ensure compliance of this DPA or a Schedule, the Parties shall agree on such amendments upon request of Customer. Notwithstanding the foregoing, Poka may update this DPA to comply with changes to applicable law, provided that no such update materially diminishes the privacy or security of Personal Data. Poka will provide written notice to Customer of any changes to comply with applicable law, with those changes being effective immediately.

11.4 Precedence. In case of any conflict or inconsistency between this DPA and any other part of the Agreement, the provisions of first the Standard Contractual Clauses and then this DPA shall take precedence over any provisions of the Agreement to the contrary.

11.5 Severability. Should any provision of this DPA become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this DPA, which shall remain in full force and effect to the fullest extent permitted by law.

[*Signatures on the following page*]

The Parties hereto have executed this DPA as of the Effective Date.

Customer	**Poka**
(Signature) Name: Title: Date:	(Signature) Name: Title: Date:

SCHEDULE 1

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Customer has authorized Poka to Process Personal Data which are further described below. The purpose of this Schedule is to define the details of the Processing of Personal Data. The provisions of the DPA between the Parties shall apply.

Nature and Purpose of Processing

Poka will process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to **Section 11.2** of the DPA, Poka will process Personal Data for the Term of the Agreement, unless otherwise agreed upon in writing.

Data Categories

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

Required Personal Information:

- **Full Name**: First and last name of an Authorized User;
- **Username**: Username created by the Customer for each Authorized User to access the Services;
- **Authorized User ID**: Pseudonym automatically created by Poka for each Authorized User (Customer name and unique identifier (e.g., acme_201))
- **Log Data**: Information related to access logs of the Services:
    - Internet Protocol (IP) address including Authorized User's geographic location;
    - Date and time of usage of the Services;
    - Device information assigned to IP address;
    - Web browser configurations;
    - Cookie data

Optional Personal Information:

- **Additional User Information**:
    - **Job title**: Job title of an Authorized User;
    - **Employee number**: Employee number of an Authorized User
    - **Email Address**: Email address of an Authorized User;
    - **Telephone number**: Telephone number of an Authorized User;
    - **Birthday**: Date of birth of an Authorized User;
    - **Hire Date**: Hiring date of an Authorized User;
    - **Profile Picture**: Profile picture of an Authorized User.

- **Content**: Content created or published on the Software Services by Authorized Users may contain additional personal information, including but not limited to:
    - **Communication**: Authorized Users can communicate through a factory feed by creating posts, commenting on posts and publishing photos and/or videos. Those posts, photos or videos may contain personal information (e.g. someone appears in a video).

- **Knowledge Management**: Authorized Users can publish work instructions to better share knowledge. Photos and/or videos can be added to a work instruction. Those posts, photos or videos may contain personal information (e.g. someone appears in a video).
- **Skills Management**: Skills can be created and managed directly inside Poka, and Authorized Users can be attributed a level of competence for each skill.
- **Forms:** Authorized Users can create and use forms, whereas some personal information may be entered and processed during those activities.
- Poka makes available within our platform an approval process that can be used to ensure adherence with your corporate privacy policy and practices by enabling you, our Customer, to validate and filter the content before it is published.

Special Categories of Personal Data

Poka does not process any special categories of Personal Data.

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL MEASURES

Poka has implemented and shall maintain appropriate TOMS for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as set forth in the Security Exhibit.

SCHEDULE 3

LIST OF SUB-PROCESSORS

The list of Sub-processors for Poka is available at https://artifacts.poka.io/Poka_Subprocessors_EN.pdf

SCHEDULE 4

STANDARD CONTRACTUAL CLAUSES

Clause 1 - Definitions

For the purposes of the Clauses:

a) '***personal data***', '**special categories of data**', 'p**rocess/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority'** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b) '***the data exporter'*** means the controller who transfers the personal data;

c) ***'the data importer'*** means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d) ***'the subprocessor'*** means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e) '***the applicable data protection law'*** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f) ***'technical and organisational security measures'*** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in **Appendix 1** which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiaries

2. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
3. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
4. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
5. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in **Appendix 2** to this contract;
d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
e) that it will ensure compliance with the security measures;
f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
h) to make available to the data subjects upon request a copy of the Clauses, with the exception of **Appendix 2**, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 - Obligations of the data importer

The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organisational security measures specified in **Appendix 2** before processing the personal data transferred;

d) that it will promptly notify the data exporter about:

i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

ii. (any accidental or unauthorised access, and

iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of **Appendix 2** which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7- Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

    a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

    b. to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 - Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Categories of data subjects to whom the processing relates

The data exporter may submit personal data to the data importer through the Services, the extent of which is determined and controlled by the data exporter in compliance with applicable data protection law and which may include, but is not limited to, personal data relating to the following categories of data subject:

- Employees, consultants, contractors of the Customer or its Customers;
- Authorized users.

Categories of data

The personal data transferred concern, at least, the following types of data:

Required Personal Information:

- **Full Name**: First and last name of an Authorized User;
- **Username**: Username created by the Customer for each Authorized User to access the Services;
- **Authorized User ID**: Pseudonym automatically created by Poka for each Authorized User (Customer name and unique identifier (e.g., acme_201))
- **Log Data**: Information related to access logs of the Services:
    - Internet Protocol (IP) address including Authorized User's geographic location;
    - Date and time of usage of the Services;
    - Device information assigned to IP address;
    - Web browser configurations;
    - Cookie data

The data exporter may submit other types of personal data to the data importer, to the extent of which is determined and controlled by the data exporter in compliance with applicable data protection law.

Optional Personal Information:

- **Additional User Information**:
    - **Job title**: Job title of an Authorized User;
    - **Employee number**: Employee number of an Authorized User
    - **Email Address**: Email address of an Authorized User;
    - **Telephone number**: Telephone number of an Authorized User;
    - **Birthday**: Date of birth of an Authorized User;
    - **Hire Date**: Hiring date of an Authorized User;
    - **Profile Picture**: Profile picture of an Authorized User.

- **Content**: Content created or published on the Software Services by Authorized Users may contain additional personal information, including but not limited to:
    - **Communication**: Authorized Users can communicate through a factory feed by creating posts, commenting on posts and publishing photos and/or videos. Those posts, photos or videos may contain personal information (e.g. someone appears in a video).
    - **Knowledge Management**: Authorized Users can publish work instructions to better share knowledge. Photos and/or videos can be added to a work instruction. Those posts, photos or videos may contain personal information (e.g. someone appears in a video).
    - **Skills Management**: Skills can be created and managed directly inside Poka, and Authorized Users can be attributed a level of competence for each skill.

- **Forms:** Authorized Users can create and use forms, whereas some personal information may be entered and processed during those activities.
- Poka makes available within our platform an approval process that can be used to ensure adherence with your corporate privacy policy and practices by enabling you, our Customer, to validate and filter the content before it is published.

Special categories of data

Poka does not process any special categories of Personal Data.

Processing operations

Data importer (“**Poka**”) shall make available to data exporter ("**Customer**”) during the Term, the Services in accordance with the Agreement.

The personal data transferred by the data exporter will be processed by the data importer only in order to perform its obligations under the Agreement and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain and improve the Services provided to the data exporter;
- to provide Customer and technical support to the data exporter; and
- disclosures in accordance with the Agreement in accordance with the applicable data protection law.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Technical and Organizational Measures

Processing of Personal Data must take place on data processing systems for which technical and organizational measures for protecting personal data have been implemented. In this context, Poka assures Customer that it will take all measures required for the Processing of Personal Data on the Poka Systems in accordance with the following measures described:

- For Poka’s Services as described at https://artifacts.poka.io/Security_Exhibit_EN.pdf