AGREEMENT FOR ENTRUSTING THE PROCESSING OF PERSONAL DATA
(the Agreement or the DPA)

concluded between:

you, hereinafter referred to as the **Controller**,

and

Tidio Poland Sp. z o.o. with its registered office in [Wojska Polskiego 81, 70-481 Szczecin], hereinafter referred to as the **Processor**.

The **Controller** and the **Processor** are hereinafter collectively referred to as the '**Parties**,' and each of them individually as the '**Party**.'

PREAMBLE

Due to the **Parties**' cooperation involving the processing of personal data, whose Controller is the entrusting entity, as well as due to obligations ensuing from Article 28 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, and repealing Directive 95/46/WE (General Data Protection Regulation, hereinafter also referred to as 'the Regulation' or 'GDPR'), the **Parties** have decided to enter this Agreement on processing personal data as follows.

§ 1.
[ENTRUSTING THE PROCESSING OF PERSONAL DATA]

1. The **Controller** entrusts to the **Processor** personal data for processing, under Article 28 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, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter also referred to as 'the Regulation' or 'GDPR'), and under the terms and for the purpose set out in this Agreement.
2. The **Processor** undertakes to process the personal data entrusted to them in accordance with this Agreement, the Regulation and other provisions of generally applicable laws that protect the rights of data subjects.
3. The **Processor** declares that they apply security measures that meet the requirements of the Regulation.

§ 2.
[SCOPE AND PURPOSE OF DATA PROCESSING]

1. The **Processor** will process the personal data entrusted under the Agreement, in particular:
    1) Identification data e.g.:
        a. First name,
        b. Last name,
        c. Registration data (e.g. national court register number),
        d. Tax ID number,
    2) Contact data e.g.:
        a. Email address,
        b. Phone number,
    3) Device data e.g.:
        a. IP address,
        b. Location data,
    4) Transactional and sales data e.g.
        a. Payment receipts,
        b. Credit/debit card data,
        c. PayPal account data,
        d. Order information
    5) Data proceeded during interactions with end-users via the communication channels,
    6) Other data processed in regard to Services (applicable to the specific type and scope of Services).
2. Data processing will concern the following categories of people:
    1) End-users – individuals who interact with the **Controller** by way of the Tidio communication platform; end-users provide the personal data willingly.
3. Entrusting personal data takes place for the following purposes:
    1) Personal data will be transferred from the **Controller** to Tidio for Tidio to provide a communication platform to facilitate interaction and engagement between the **Controller** and the end-user.
    2) This service will consist of providing a communication platform for the **Controller** to use in order to onboard and retain end-users as well as analyse their use of the **Controller's** product and/or services.
4. The **Processor** may process personal data entrusted to them only to the extent and purpose specified in the Agreement and to the extent and purpose necessary to provide services specified in the Main Agreement.

§ 3.
[TERM OF CONTRACT]

1. The data entrusted to the **Processor** will be processed by them only for the period necessary in this regard. The **Parties** also agree that this Agreement shall be effective from the date of its conclusion to the moment of termination of the Main Agreement.
2. Either **Party** may terminate this Agreement with a one month's notice.

3. At the same time**,** the **Parties** agree that the Agreement shall be terminated upon the termination of the Main Agreement.
4. The **Controller** may terminate this Agreement with immediate effect when the **Processor**:
   1) despite the obligation to remove the infringements found during the inspection, they will not remove them within the prescribed period;
   2) processes personal data in a manner inconsistent with the Agreement;
   3) entrusts the processing of personal data to another entity without the consent of the **Controller**.

§ 4.
[OBLIGATIONS OF THE PROCESSOR]

1. The **Processor** hereby declares that they have the infrastructure, resources, experience, knowledge and qualified personnel, to the extent enabling the proper performance of the Agreement, in accordance with applicable law. In particular, the **Processor** declares that they are familiar with the principles of processing and securing personal data resulting from:
   1) GDPR;
   2) the applicable national regulations.
2. The **Processor** is obliged to:
   1) process entrusted personal data only on the basis of the Agreement and process the personal data only on documented instructions from the **Controller** unless required to do so by Union or Member State law to which the **Processor** is subject. In a situation where the **Processor**'s obligation to process personal data results from legal provisions, the **Processor** shall inform the **Controller** by electronic means - before processing - of that legal requirement, unless that law prohibits such information on important grounds of public interest;
   2) process entrusted personal data in accordance with the Regulation, regulations adopted to enable the Regulation to be applied, other applicable legal provisions, the Agreement and the instructions of the **Controller**;
   3) process personal data entrusted to them with the exception of the highest principles of security and protection of personal data required by applicable law, including in particular those required by the provisions of the GDPR;
   4) assign access to entrusted personal data only to persons who, due to the scope of their tasks, have been authorised by the **Processor** to process them, and committed themselves to confidentiality of data processed during and after termination of employment with the **Controller** and only for the purpose of performing duties resulting from the Agreement;
   5) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of violating the rights or freedoms of individuals whose personal data will be processed under the Agreement (Article 32 of the GDPR) and ensure the implementation of principles of data protection by design and data protection by default (specified in Article 25 of the GDPR);

6) maintain documentation describing the processing of data by the **Processor** , including, in particular, the record of processing activities (Article 30 of the GDPR);
7) immediately, and no later than within 24 hours, inform the **Controller** of any suspected violation of personal data protection;
8) support the **Controller** in the performance of the duties specified in art. 32-36 GDPR;
9) support the **Controller** (through the application of appropriate technical and organisational measures) in the fulfilment of the obligation to respond to requests of data subjects in the exercise of their rights set out in Chapter III of the Regulation;
10) make available to the **Controller**, at their request, no later than within 30 working days, all information necessary to demonstrate compliance of the **Processor** with the obligations laid down in the applicable law, in particular the Regulation, including information on the safeguards used, identified threats and incidents in the area of personal data protection;
11) immediately inform the **Controller** if, in their opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions;
12) immediately, but no later than within 10 business days, inform (if it does not lead to violation of the applicable law) the **Controller** of any proceedings, in particular administrative or judicial, concerning the processing of personal data by the **Processor**, any administrative decision or a judgment regarding the processing of data addressed to
the **Processor**, of any controls and inspections regarding the processing of personal data by the **Processor**, in particular those carried out by the supervisory authority, as well as any complaints from data subjects related to the processing of their personal data;
13) store personal data only as long as the **Controller** has designated it, and also, without unnecessary delay, update, correct, modify, anonymise, restrict the processing or deletion of personal data in accordance with the instructions of the **Controller** (if such action would cause inability to continue to implement processing activities, the **Processor** will inform the **Controller** before it is taken and then follow the instructions of the **Controller**);
14) return or delete in a permanent manner, upon the termination, expiration or termination of this Agreement, all personal data provided by the **Controller** and delete existing copies, unless Union or Member State law requires storage of the personal data (costs of return or destruction of personal data and copies thereof bears the **Processor**).

§ 5.
PERSONAL DATA SECURITY

1. In order to assure the personal data security, **Processor** certain defensive mechanisms which penetrate one another were introduced. Such mechanisms include physical securities, equipment related measures, organizational procedures and IT solutions.
2. The **Processor** assures that the physical securities include, in particular:

1) Access to personal data by the authorized persons only;
2) Storing physical data collections in the locked cabinets / premises, including the servers where the data are accumulated in the electronic form;
3) 24-hour protection of the premises where personal data are stored.

3. The **Processor** assures that the equipment related measures include, in particular:
   1) Equipment used within the IT system which is applied for personal data processing providing appropriate data access securities;
   2) Storing personal data on servers of external companies which provide proper standards of personal data protection supported by contractual provisions providing for the conditions of data storing by external entities;
   3) Managing the equipment used for personal data processing was entrusted to professionals acting within the Processor;
   4) Using a shredder to delete effectively all the documents containing personal data.
4. The **Processor** assures that the organizational procedures include, in particular:
   1) Training of the personnel having access to the data;
   2) Periodical audits regarding personal data protection;
   3) Application of mechanisms of privacy by design and privacy by default;
   4) Assessment of the influence on the data processing case by case;
   5) Obligation to provide due diligence aiming at assurance of conformity of the data protection and the actually binding requirements, including adjustment of the Policy and Directives to the changing legal environment.
5. The **Processor** assures that the protective measures within IT solutions consist in, in particular:
   1) Limitation of access to the devices and applications by ID and a password;
   2) Limitation of the user's access only to certain resources by providing him/her with a specified scope of authorizations from the administrator's level;
   3) Application of programs aiming at the actual monitoring of the malicious software presence;
   4) Updating the used software on current basis;
   5) Protection of the local network against the actions initiated from outside by using a firewall;
   6) Making back-ups
6. Selected aspects of the **Processor's** security measures applied under the Agreement are described at the website:
   https://www.tidio.com/knowledge/faq/how-are-the-security-matters-handled-at-tidio/

§ 6.
[OBLIGATIONS OF THE CONTROLLER]

The **Controller** is obliged:

1. to cooperate with the **Processor** in the implementation of the provisions of this Agreement, provide explanations in the event of doubts as to the legality of the instructions of the **Controller**, as well as perform their specific duties in a timely manner;

2. to entrust only the Personal Data that was obtained and is processed by **Controller** in accordance with applicable laws, including the GDPR. The **Controller** confirms in particular that (i) it has collected and holds the consents required by law to conduct direct marketing activities, including consents to send commercial information by electronically and for the use of telecommunications means and automatic systems for the purposes of direct marketing - in the event that it conducts such activities, (ii) has provided data subjects with information about the processing of their data to the extent and in the manner required by the GDPR, and (iii) is authorized to process the Personal Data and entrust it to **Processor** for processing within the scope and purpose set out in § 2 above. In addition, if **Controller** is not the controller of the Personal Data, it confirms that it has obtained the consent of the relevant **Controller** for entrusting **Processor** with further processing of the Personal Data within such purpose and scope.

§ 7.
[RIGHT OF CONTROL - AUDIT]

1. The **Controller** is authorised to audit the compliance of the processing of personal data by the **Processor** with the Agreement and applicable law. The audit may only cover the control of the relevant documentation and the right to obtain the necessary information / explanations. The **Processor** has the right to refuse to provide documentation or to provide information / explanations to the extent that the audit could threaten the disclosure of personal data other than those processed by the Processor under the Agreement or with the disclosure of business secrets.

Processor.

2.The audit referred to in point 1 above may be performed by the **Controller** or third parties to whom the **Controller** entrusts the performance of the audit at the place where personal data are processed.

3. The **Processor** is required to cooperate with the **Controller** and auditors authorised by it
4. The audit is subject to the following conditions:
   (i) it may only concern Personal Data entrusted to **Processor** for processing pursuant to the Agreement;
   (ii) it shall be conducted efficiently and as soon as possible, not longer than 2 working days;
   (iii) take place no more frequently than once a year, unless an audit is required in accordance with required by law or by the applicable supervisory authority, or immediately following discovery of a material breach of Personal Data processed under the Agreement,
   (iv) may be performed during **Processor's** normal business hours, in a manner that does not interfering with Processor's business activities and in accordance with Processor's security policies **Processor**;
   (v) the **Controller** will notify **Processor** of its intention to carry out the audit by electronically or by letter at least 14 working days before the planned date of the audit. In the event of **Processor** being unable to carry out the audit on the planned date or other the planned date or other unexpected obstacles, **Processor** shall notify the **Controller** about such circumstances and will propose a new date of audit, but not later than within 7 working days from the date indicated by the **Controller**;
   (vi) The costs related to the audit are borne by the **Controller** without the right to demand reimbursement of such costs or payment of additional remuneration;

(vii) The audit must not aim at or lead to the disclosure of legally protected secrets (including business secrets of **Processor**). The **Controller** is obliged to create an Audit report summarizing findings of this audit. The report will be provided to **Processor** and will constitute confidential information about **Processor**, which cannot be disclosed to third parties without the consent of **Processor**, unless required by applicable law.

§ 8.
[FURTHER ENTRUSTING DATA FOR PROCESSING]

1. The **Processor** may entrust the processing of personal data covered by the Agreement to a third party (including other entrepreneurs) – general consent of the **Controller**.
2. In the case of further entrusting of personal data covered by this Agreement, the **Processor** guarantees that the entities to which they have entrusted these data meet all the conditions for the processing of personal data referred to in the Regulation, and will fulfil all obligations set out in this Agreement.
3. The **Processor** is obliged to notify the **Controller** of further data entrustment (possible in electronic form, including as part of information on the website.), .
4. The **Processor** is obliged to perform the same activities referred to in point 3 above also in the case of a change of the previously accepted entity, to whom they have further entrusted the data covered by this Agreement. The **Processor** will process data primarily within the European Economic Area (EEA). In some cases, in particular when the **Processor** uses the services of third parties / partners who support the Processor in its business activities, the personal data we collect from the **Controller** may also be accessed or processed outside the EEA. Such destination may not have laws which protect information to the same extent as in the EEA. We have obligations to ensure that your personal data is only accessed or processed from territories outside the EEA where the European Commission has decided that the territory in question ensures an adequate level of protection (known as a 'whitelisted' territory) or, in the absence of a decision by the European Commission, there are appropriate safeguards in place to protect your personal data. For example, if your personal data is accessed or processed from a territory outside the EEA which is not whitelisted, the appropriate safeguards may be provided by standard data protection clauses adopted by the European Commission (known as 'model clauses')

Controller authorises **Processor** to conclude, in the name and on behalf of **Controller**, standard contractual clauses approved by the European Commission by way of the European Commission Decision of 5 February 2010 No. 2010/87/EU with the sub-processors of the processing by **Processor** in connection with the entrusting of data by **Controller** to **Processor**, which are not established in the territory of the European Economic Area.

§ 9.
[RESPONSIBILITY OF THE PROCESSING PARTY]

1. The **Processor** undertakes not to provide or use personal data in a way that could result in breach of the Agreement, such as, in particular, entrusting unauthorised persons with access to personal data

2. **Each Party** shall immediately inform the **other Party** of any proceedings, in particular, administrative or judicial, regarding processing by the **each Party** of personal data specified in the Agreement, any administrative decision or ruling regarding the processing of such data, addressed to the **Party**, and any planned, if known, or carried out inspections and inspections regarding processing of such personal data, in particular those carried out by the supervisory authority.
3. Contractual liability and tort liability of the **Processor** is limited to direct losses incurred by the **Controller**. **Processor** shall not be liable for lost profits, regardless of their source, except in the case of intentional fault or gross negligence
4. The total liability of **Processor**, regardless of the number and basis of the **Controller's** claims is limited to the equivalent of the fixed subscription fee for a period of 3 (three) months, paid by the **Controller** for the Services during the billing period immediately preceding the date on which the event giving rise to the damage occurred, excluding any amounts comprising installation charges or additional charges of any kind. The **Controller** shall indemnify **Processor** against any liabilities exceeding the above-mentioned limitation.
5. **Processor** shall not be liable for improper performance or non-performance of the Services as a result of Force Majeure.
6. The Parties agree that the **Controller** shall be responsible for indemnifying the claims of data subjects caused as a result of incorrect processing of Personal Data under the DPA, unless **Controller** proves that the damage resulted from the sole fault of **Processor** or its subcontractors. In the event failure to prove the above, the **Controller** shall unconditionally release **Processor** from any claims made by entities whose Personal Data is processed by **Processor** on the basis of the Terms and Conditions. In the event of initiating court proceedings against **Processor**, the Controller shall be obliged, on Processor's request, to intervene as a party to such proceedings and assume responsibility for the asserted claim.

§ 10.
[PRINCIPLES OF CONFIDENTIALITY]

1. **Each Party** undertakes to keep confidential all information, data, materials, documents and personal data received from the **other Party** and from the persons cooperating with them and data obtained in any other way, deliberate or accidental in verbal, written or electronic form ('data confidential').
2. **Each Party** declares that due to the obligation to keep confidential data secret, it will not be used, disclosed or made available without the written consent of the **other Party** for the purpose other than the performance of the Agreement, unless the need to disclose information is required by applicable law or Agreement.

§ 11.
[FINAL PROVISIONS]

1. The **Parties** declare that there are no other arrangements in this Agreement that would modify or supplement its provisions.
2. Any issues not regulated by the provisions of this Agreement shall be governed by appropriate Polish Law Regulations.

3. Matters arising from the implementation of the provisions of this Agreement will be settled by a common court competent for the **Processor**.
4. The contract was drawn up in two identical copies, one for each of the **Parties**.