Data Processing Addendum
clockin GmbH

Table of Contents

Annex to the clockin General Terms and Conditions
Data Processing Addendum

Section 1
PARTIES AND BACKGROUND

1.1 Customer has entered into an agreement with clockin GmbH ("**clockin**") (each a "**Party**" and collectively the "**Parties**") under which clockin has agreed to provide certain services, including access to its software platform, support services and/or professional services (together the "**Services**") to the Customer (as amended from time to time) (the "**Agreement**").

1.2 In the course of providing the Services under the Agreement, clockin will process Customer Personal Data. This Data Processing Addendum ("**DPA**") regulates the data protection obligations of the Parties when processing Customer Personal Data.

1.3 Whether or not one of the following Exhibits of this DPA apply depends on where the Customer and Customer Affiliates reside. This DPA covers the following situations:

a) Where the Customer and Customer Affiliate (as defined below) reside in the European Economic Area, including the European Union ("**EU**", together the "**EEA**") the Data Processor Clauses (as defined below) laid down in **Exhibit A** of this DPA are intended to govern the processing.

b) Where the Customer and/or Customer Affiliate (as defined below) reside in the UK (as defined below) the UK Addendum (as defined below) included in **Exhibit B** of this DPA is intended to govern the processing.

c) Where the Customer and/or Customer Affiliate (as defined below) reside in a Restricted Country (as defined below) the Standard Contractual Clauses (as defined below) are laid down in **Exhibit C** of this DPA and are intended to govern the processing.

1.4 The mandatory annexes of the Data Processor Clauses and the Standard Contractual Clauses are laid down in **Exhibit D**.

Section 2
DEFINITIONS

2.1 Capitalized terms used but not defined within this DPA shall have the meaning set forth in the Agreement. The following capitalized terms used in this DPA shall be defined as follows.

a) "**Applicable Laws**" means all laws, rules and regulations applicable to either Party's performance under this DPA, including, but not limited to, those applicable to the processing of Personal Data. This means, in particular, the GDPR and all national laws validly amending the applicable rules for the processing of Personal Data.

b) "**Customer Affiliate**" means an affiliate of the Customer who is a beneficiary to the Agreement.

c) "**Customer Personal Data**" means Personal Data processed by clockin on behalf of Customer or Customer Affiliate in connection with the provision of the Services, which may also include Personal Data of Customer and Customer Affiliate's customers and other third parties whose Personal Data is being processed by Customer or a Customer Affiliate.

d) "**Data Processor Clauses**" means standard contractual clauses set out in the annex of the Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.

e) "**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as it forms part of the law for England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018.

f) "**Personal Data**" means any information relating to an identified or identifiable individual or device, or is otherwise "personal data," "personal information," "personally identifiable information" and similar terms, and such terms shall have the same meaning as defined by applicable data protection laws.

g) "**Restricted Country**" means a country, territory or a specified sector within a country, or an international organisation outside the EEA not deemed to ensure an adequate level of protection by the European Commission.

h) "**SCC**" means the Standard Contractual Clauses and the Data Processor Clauses.

i) "**Standard Contractual Clauses**" means module 4 of the standard contractual clauses set out in the annex of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

j) "**Sub-processor of clockin**" means a processor appointed by clockin to process Customer Personal Data; and

k) "**UK**" means the United Kingdom of Great Britain and Northern Ireland.

2.2 The terms "controller", "processor", "data subject", "process", "personal data breach" and "supervisory authority" shall have the same meaning as set out in the GDPR.

Section 3
INTERACTION WITH THE AGREEMENT

3.1 This DPA is incorporated into and forms an integral part of the Agreement and shall be effective and replace any previously applicable data processing and security terms as of the effective date of the

Agreement ("**Effective Date**"). This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any processing of Customer Personal Data.

3.2 Any processing operation as described in Section 6 and Annex II of **Exhibit D** to this DPA shall be subject to this DPA.

3.3 Customer Affiliates shall be beneficiaries under this DPA and – through Customer (see Clauses 3.4 and 3.5) – be entitled to enforce all rights in relation to the Customer Personal Data provided by the respective Affiliate. Customer will ensure that all obligations under this DPA will be passed on to the respective Customer Affiliate.

3.4 Customer warrants that it is duly mandated by any Customer Affiliates on whose behalf clockin processes Customer Personal Data in accordance with this DPA to (a) enforce the terms of this DPA on behalf of the Customer Affiliates, and to act on behalf of the Customer Affiliates in the administration and conduct of any claims arising in connection with this DPA; and (b) receive and respond to any notices or communications under this DPA on behalf of Customer Affiliates.

3.5 Customer shall be the only point of contact for all communication between the Customer Affiliates and clockin.

Section 4
SCOPE OF PROCESSING CLAUSES

4.1 The Data Processor Clauses included in Section 1 of **Exhibit A** of this DPA shall by default apply where Customer Personal Data is provided by either Customer or a Customer Affiliate located in the EU and/or EEA, or to which the GDPR otherwise applies.

4.2 In addition to the Clauses applicable under Clause 4.1, the UK Addendum included in **Exhibit B** shall apply where Customer Personal Data is provided by a Customer or a Customer Affiliate that is located in the UK.

4.3 The Standard Contractual Clauses included in Section 1 of **Exhibit C** of this DPA shall by default apply where Customer Personal Data is provided by a Customer or a Customer Affiliate located in a Restricted Country, or to which the GDPR otherwise does not apply.

Section 5
ROLES OF THE PARTIES

5.1 For the purposes of the GDPR, clockin acts as "processor" or "sub-processor." clockin' function as processor or sub-processor will be determined by the function of the Customer:

a) where Customer acts as a controller, clockin acts as a processor.

b) where Customer acts as a processor on behalf of a controller, clockin acts as a sub-processor.

5.2 Where clockin acts as a sub-processor, the terms provided in the Data Processor Clauses or the Standard Contractual Clauses shall apply *mutatis mutandis*. The Customer must inform clockin if it

acts as a processor under the instructions of a controller. clockin shall process the personal data only on documented instructions from the Customer's controller, as communicated to clockin by the Customer, and any additional documented instructions from the Customer. Such additional instructions shall not conflict with the instructions from the Customer's controller. The Customer's controller or the Customer may give further documented instructions regarding the data processing throughout the duration of the DPA.

Section 6
SUBJECT, DURATION, PURPOSE AND SPECIFICATION OF PROCESSING

6.1 The details of data processing (such as subject matter, nature and purpose of the processing, categories of personal data and data subjects) are described by the Parties in the Agreement and in **Exhibit D**.

6.2 The duration of the processing shall correspond to the duration of this DPA as set forth in Section 7.

6.3 For support services provided by clockin that are not included in the service description, that go beyond the statutory obligations of clockin, or that are not attributable to any fault on the part of clockin, a separate remuneration may be agreed upon. Unless otherwise agreed in writing, such remuneration shall be calculated at a standard hourly rate of EUR 130.00. The Parties undertake to ensure that any such remuneration is reasonable and consistent with market practice. Statutory cooperation obligations of clockin, particularly those under Article 28 GDPR, remain unaffected and are covered by the agreed principal remuneration.

Section 7
CONTRACT PERIOD

The duration of this DPA coincides with the duration of the Agreement. It commences and terminates with the provision of the Services under the Agreement, unless otherwise stipulated in the provisions of this DPA.

Section 8
MISCELLANEOUS

8.1 In the event of any conflict between the SCC, the DPA or the Agreement the order of prevalence between the terms included therein shall be as follows:

a) where applicable, SCC,

b) the terms in **Exhibit D** of the DPA which are meant to fill in the required information for the SCC (where applicable) and, in particular, its Appendix,

c) the remaining provisions of this DPA, and

d) the Agreement and other contractual documents.

8.2 In the event a clause under the Agreement has been found to violate the Applicable Laws, this shall not affect the validity of the remaining provisions, and the Parties will mutually agree on modifications to the Agreement to the extent necessary to ensure data privacy-law compliant processing.

Exhibit A

Data Processor Clauses

1. The following outlines the Data Processor Clauses as implemented in the DPA, subject to the amendments in Section 2 of this **Exhibit A**:

Standard Contractual Clauses

based on Commission Implementing Decision (EU) 2021/915

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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)

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5 - Optional

Docking clause

Clause 5 of the Data Processor Clauses (Docking Clause) does not apply;

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process 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 this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 2 weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the

processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10
Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

***** END Data Processor Clauses *****

2. For the purposes of the Data Processor Clauses:

2.1 For the purposes of Clause 7.7 of the Data Processor Clauses the agreed list of Sub-processors of clockin for the purpose of Clause 7.7(a) of the Data Processor Clauses is set out in Annex IV of Exhibit D to this DPA.

2.2 Clause 7.7 lit. e) of the Data Processor Clauses shall not apply.

2.3 If Customer objects to clockin's use of a new Sub-processor of clockin (including when exercising its right to object under Option 2 of Clause 7.7(a) of the Data Processor Clauses) on reasonable grounds, it shall provide clockin with written notice of the objection within 2 weeks after clockin has provided notice to the Customer described in Clause 7.7(a) of the Data Processor Clauses in Section 1 of this Exhibit A to the DPA of such proposed change ("**Objection**"). If Customer does not object to the engagement within the objection period, consent regarding the engagement shall be assumed. In the event Customer objects to clockin's use of a new Sub-processor of clockin, Customer and clockin will work together in good faith to find a mutually acceptable resolution to address such Objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, either Party may, as its sole and exclusive remedy, terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to the other Party. During any such Objection period, clockin may suspend the affected portion of the Services. Customer may only request a pro-rata refund if Customer can prove that the Objection is based on justified reasons of non-compliance with Applicable Laws.

2.4 Annex I (List of Parties) of the Data Processor Clauses shall be deemed to incorporate the information in Annex I of **Exhibit D** to this DPA;

2.5 Annex II (Description of Transfer) of the Data Processor Clauses shall be deemed to incorporate the information in Annex II of **Exhibit D** to this DPA; and

2.6 Annex III (Technical and Organisational Measures) of the Data Processor Clauses shall be deemed to incorporate the information in Annex III of **Exhibit D** to this DPA.

2.7 Annex IV (Subprocessor) of the Data Processor Clauses shall be deemed to incorporate the information in Annex IV of **Exhibit D** to this DPA.

Exhibit B

UK Addendum

1. Definitions and Interpretation

1.1 Terms used in this UK Addendum but not defined in the DPA have the following meaning:

"**UK Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

1.2 This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation under the UK Data Protection Laws.

1.3 Where there is any inconsistency or conflict between the UK Addendum and Data Processor Clauses, the UK Addendum overrides the Data Processor Clauses, except where (and in so far as) the inconsistent or conflicting terms of the Data Processor Clauses provides greater protection for data subjects, in which case those terms will override the UK Addendum.

2. Incorporation of and changes to the Data Processor Clauses

2.1 This UK Addendum incorporates the Data Processor Clauses which are amended to the extent necessary so that they ensure compliance with the requirements under Art. 28 UK GDPR.

2.2 The Data Processor Clauses shall be read and interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to enter into an agreement that complies with Articles 28(3) and (4) of the UK GDPR.

2.3 The Data Processor Clauses are deemed amended to the extent necessary, so they operate:

2.3.1 for processing by clockin on behalf of the Customer, to the extent that UK Data Protection Laws apply to such processing; and

2.3.2 to ensure compliance with Article 28(3) and (4) of the UK GDPR.

2.4 The amendments referred to in Section 2.2 include (without limitation) the following:

2.4.1 references to 'Regulation (EU) 2016/679', '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)' and 'that Regulation' are all replaced by 'UK GDPR';

2.4.2 references to specific Article(s) of 'Regulation (EU) 2016/679' are replaced with the equivalent Article or Section of UK GDPR;

2.4.3 references to Regulation (EU) 2018/1725 are removed;

2.4.4 references to the "Union", "EU" and "EU Member State" are all replaced with the "UK"; and

2.4.5 references to the "competent supervisory authority" shall be replaced with the Information Commissioner.

2.5 References to the 'Clauses' means this UK Addendum, incorporating the Data Processor Clauses.

Exhibit C

Standard Contractual Clauses

1. The Standard Contractual Clauses are included herein by reference, and for the purposes of the Standard Contractual Clauses they shall apply as follows:

1.1 Module Four shall apply in the case of the processing under clause 5.1 a)of the DPA and in the case of processing under clause 5.1 b)of the DPA.

1.2 With regard to Clause 11 of the Standard Contractual Clauses (Redress), the Parties agree that the **OPTION** does not apply.

1.3 With regard to Clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that the governing law shall be the law of Germany.

1.4 In Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of **GERMANY**.

***** END Standard Contractual Clauses *****

2. For the purposes of the Standard Contractual Clauses:

2.1 Annex I.A (List of Parties) of the Standard Contractual Clauses shall be deemed to incorporate the information in Annex I of Exhibit D to this DPA; and

2.2 Annex I.B (Description of Transfer) of the Standard Contractual Clauses shall be deemed to incorporate the information in Annex II of Exhibit D to this DPA.

Exhibit D

Annex I of Exhibit D:

Customer referred to as the controller(s) in the Data Processing Clauses and data importer with respect to the Standard Contractual Clauses:

Name: The Customer is the party who has concluded the Agreement with clockin

Address: is provided by the Customer in the Agreement or the respective order.

Contact person's name, position, and contact details: are provided by the Customer in the Agreement or the respective order.

Contact details of the data processing officer: if applicable, are provided by the Customer in the Agreement or the respective order.

Activities relevant to the data transferred under the Standard Contractual Clauses: as described in the Agreement or the respective order.

Role under Applicable Law: controller or processor on behalf of a third party

clockin referred to as the processor with respect to the Data Processing Clauses and data exporter with respect to the Standard Contractual Clauses:

Name: clockin GmbH

Address: Rektoratsweg 36, 48159 Münster, Germany
Email: datenschutz@clockin.de

Contact details of the data processing officer: as provided in our privacy notice under the URL https://www.clockin.de/rechtliches/datenschutz; email: datenschutz@clockin.de.

Activities relevant to the data transferred under the Standard Contractual Clauses: as described in the Agreement and any applicable Order.

Role under Applicable Law: processor on behalf of Customer as a controller or sub-processor on behalf of Customer as a processor

[As an integral part of the Agreement, the DPA is effective without signature starting from the Effective Date of the Agreement]

Annex II of Exhibit D:

Categories of data subjects whose personal data is processed:

- Employees, customers, members, suppliers, prospective customers, and other persons whom the Customer enters into the clockin system

Categories of personal data transferred (for purposes of Standard Contractual Clauses) and personal data processed (for purposes of Data Processing Clauses)

- Names
- Address information
- Contact details
- Occupation/position in the company
- Details of the inquiry
- Products purchased
- Bank details
- Employment data
- Photos
- Location data (if selected)
- IT usage data
- Working hours and break times
- Absences and related data/information (vacation, illness, special leave, training/school, special leave, working time account, etc.)
- Documented work results in the form of photos, text, video, audio
- Documents and information stored in employee data or digital personnel files (if used)
- Signed order confirmations/checklists from the customer as PDF files

- Additional information entered into the system by the client or their employees (text, audio, video, images, PDFs, graphics, and more)

For purposes of the Standard Contractual Clauses, the frequency of the transfer (*e.g.*, whether the data is transferred on a one-off or continuous basis).

- Not on a regular basis, only upon Customer's request

Nature of the processing

- clockin provides a cloud-based solution for digital time tracking, project time tracking, and project documentation, which is used via mobile apps, web browsers, and tablet terminals; the processing that takes place within the app/system is regularly carried out on behalf of the Customer as the controller.
    - The processing includes, in particular, the collection and storage of work, break, travel, and project-related times by employees via app, browser, or terminal, including optional location-based time recording (GPS/geo-tags) for verifiable time/location documentation.
    - Processing of absences, work schedules, employee self-service functions, and the maintenance of a digital personnel file (document upload, including contract/HR documents).
    - Project documentation, including the recording and storage of photos, sketches, notes, digital checklists/forms, and the collection of digital customer confirmations/signatures; provision in a digital project file and optional project export/transfer to customers.
    - Evaluation/analysis and correction of time and project data, logging functions, and real-time overviews/dashboards for control and verification purposes.
    - Transfer/export of data to the customer's connected systems via interfaces and an open API;
    - Sending of system/status notifications (*e.g.*, push notifications) to authorized users for the provision of functions.
    - Hosting/operation including storage and retrieval of data in the cloud, transport encryption (HTTPS/TLS), and use of CDN.
    - clockin also offers support. In course of providing the support services and depending on the individual case, Customer may grant access to clockin into their IT. clockin only process personal data in course of such services.

- Depending on the function commissioned, the processing steps include, in particular, the collection, recording, organization, storage, evaluation, display, transmission/export to defined recipient systems, restriction, and deletion of personal data within the scope of contractual service provision and the respective customer configuration. Storage and deletion concepts are based on the principle of necessity and the relevant purposes/deadlines.

Purpose(s) for which the personal data is processed, and for purposes of the Standard Contractual Clauses transferred, on behalf of the Customer

- The purpose of the processing and transfer is to ensure the delivery and performance of clockin' Services agreed in the Agreement, and as configured and instructed by the Customer.

For Purposes of the Data Processing Clauses, the duration of the processing and for Purposes of the Standard Contractual Clauses, the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- The personal data is processed for the duration of the contractual relationship. In the meantime, the personal data will be deleted upon request or if the purpose ceases to exist. After termination of the contractual relationship, the personal data is deleted in accordance with the internal deletion concept of clockin.

For processing by (sub-) processors for purposes of the Data Processing Clauses, and for transfer to Sub-processors of clockin, also specify subject matter, nature and duration of the processing

- Sub-processors of clockin are used solely for the purpose of hosting the software solution provided by clockin. Such transfer and/or processing serves the purpose of providing the Services and occurs for the duration of the contractual relationship. The nature of the processing includes activities such as storing, transmitting, deleting, structuring, organisation.

Annex III of Exhibit D:

List of existing technical and organizational measures of the data processor pursuant to Art. 32 GDPR

The processor implements the following technical and organizational measures to protect the personal data covered by the contract. The measures were determined in accordance with Art. 32 GDPR.

Subcontractors shall implement at least equivalent, and generally higher, security measures. In this respect, reference is made to the technical and organizational measures of the service providers we use.

1. Purpose limitation and separability

The following measures ensure that data collected for different purposes is processed separately:

- Logical client separation (software-based)
- Authorization concept
- Separation of production and test systems

2. Confidentiality and integrity

The following measures ensure the confidentiality and integrity of the data processor's systems:

a. Encryption

The data or data carriers processed on behalf of the client are encrypted in the following manner: Only encrypted connections (e.g., TLS, SSH) are used during transport.

b. The following measures have been taken to prevent unauthorized persons from accessing the data processing equipment of the processor with which personal data is processed or used (access control):

- Alarm system
- Entrances and exits to the building cannot be opened from the outside
- Security measures for windows, basement windows, and light wells
- Central reception area with personnel control
- Automatic access control system

- Chip card/transponder locking system
- Light barriers/motion detectors
- Key management (key issuance, etc.)
- Card and key documentation Secure storage of replacement cards/keys

c. The following measures have been taken to prevent unauthorized third parties from using the data systems (access control):

- Assignment of user rights
- Creation of user profiles
- Authentication with username/password
- Password assignment
- Use and control of password rules
- Automatic control of the immediate assignment of individual passwords
- Alerting when defined limits for incorrect login attempts are exceeded
- Locking of end devices when leaving the workplace
- Assignment of user profiles to IT systems
- Use of VPN technology for data transmission
- Encryption of mobile IT systems
- Encryption of mobile data carriers
- Encryption of data backup systems
- Use of intrusion detection systems
- Use of anti-virus software
- Encryption of data carriers in laptops/notebooks
- Use of a hardware firewall

- Use of a software firewall
- Regular installation of updates for firewalls and antivirus software
- Regular installation of security patches and updates for browsers
- Separation of company network and guest Wi-Fi
- Use of central administration software for external deletion of data on mobile devices
- Encryption of data carriers in mobile devices
- Deactivation/monitoring of unused connection sockets

d. The following measures have been taken to ensure that those authorized to use a data processing system can only access the data for which they have access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after storage ( ) (access control):

- Administration of rights by system administrator
- Regular review and updating of access rights
  (especially when employees leave the company, etc.)
- Number of administrators reduced to the "bare minimum"
- Logging of access to applications, especially when entering,
  modification, and deletion of data
- Secure storage of data carriers
- Physical deletion of data carriers before reuse
- Proper destruction of data carriers (DIN 66399)
- Use of document shredders or service providers

e. The following measures can be used to subsequently check and determine whether and by whom personal data has been entered, changed, or removed from data processing systems (input control).

- Logging of data entry, modification, and deletion
- Logging the creation/modification of users and rights

- Logging of system changes
- Monitoring of routers and switches
- Logging of connection and call data
- Traceability of data entry, modification, and deletion by individual usernames (not user groups)
- Assignment of rights to enter, change, and delete data based on an authorization concept

f. The following measures ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions (order control).

- Selection of the processor based on due diligence considerations
  (in particular with regard to data security)
- Prior review of the security measures taken by the processor
- Written instructions to the processor (e.g., through a processing agreement)
- Obligation of the processor's employees to maintain confidentiality and telecommunications secrecy
- Obligation of external service providers to maintain data secrecy, unless they are processors
- Ensuring the destruction of data after completion of the order
- Agreement on effective control rights vis-à-vis the processor
- Ongoing monitoring of the processor and its activities

For remote maintenance:

- Only temporary access limited to the respective maintenance session
- Restriction of access to the rights necessary for maintenance
- Events triggered by the client
- Virtual private network (VPN)
- Monitoring of the session by the client (dual control principle)

g. The following measures ensure that personal data cannot be obtained or accessed by unauthorized persons during transmission (physical and/or digital) (transport and transmission control):

- Use of VPN tunnels
- Encryption of communication channels (e.g., encryption of email traffic)
- Encryption of physical data carriers during transport
- Sensitive data/documents are encrypted/anonymized/pseudonymized when transferred/transmitted
- Regular installation of security patches/updates for email programs
- Security settings for email programs are applied in a targeted manner and cannot be changed by users
- Use of email content filters
- Logging of email traffic and regular evaluation for deviant and suspicious email behavior

3. Availability, recoverability, and resilience of systems

The following measures ensure that the data processing systems used function properly at all times and that personal data is protected against accidental destruction or loss

- Air conditioning in server rooms
- Devices for monitoring temperature and humidity in server rooms
- Protective power strips in server rooms
- Fire and smoke alarm systems in server rooms
- Fire extinguishing system/fire extinguishers with suitable extinguishing agents available
- Fire doors
- Creation and implementation of a backup and recovery concept
- Testing data recovery
- Creation of an emergency plan
- Storage of data backups in a secure, off-site location

4. Reviewing, evaluating, and adjusting existing measures

The processor shall review, evaluate, and, if necessary, adapt the technical and organizational measures set out in this annex at appropriate intervals and as required. In addition, the following measures have been taken:

- Appointment of an external data protection officer and involvement of the data protection officer in security incidents and data breaches
- Documentation of security incidents and data breaches
- Obligation of employees to maintain confidentiality
- Obligation of employees to maintain telecommunications secrecy
- Regular awareness-raising among employees
- Data protection impact assessments are carried out as required
- Documented process for detecting and reporting security incidents/data breaches
- Prior review of the security measures taken by the contractor and their documentation
- Selection of contractors based on special due diligence criteria

Annex IV of Exhibit D:

The Customer has authorized the use of the following Sub-processor(s) of clockin:

1&1 Internet SE
Services: Server hosting and backups
Address: Elgendorfer Str. 57, 56410 Montabaur

STRATO AG
Services: Server hosting and backups
Address: Pascalstraße 10, 10587 Berlin

Mailjet
Services: Email delivery
Provider: Mailgun Technologies Inc., 112 E Pecan Sr. #1135, San Antonio, Texas 78205, USA
Website: https://www.mailjet.de/
Further information & data protection: https://www.mailjet.com/legal/terms/, https://www.mailjet.de/privacy-policy/ and https://sinch.com/legal/terms-and-conditions/other-sinch-terms-conditions/data-protection-agreement/Garantie: EU standard contractual clauses. You can request a copy of the EU standard contractual clauses from us. The provider has joined the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/), which ensures compliance with an adequate level of data protection based on a decision by the European Commission.

AWS Cloud
Services: Server, hosting
Provider: Amazon Web Services EMEA SARL, Luxembourg.
Website: https://aws.amazon.com/de/websites/
Further information & data protection: https://aws.amazon.com/de/legal/
We don't plan to transfer personal data to third countries. Since Amazon is headquartered in the US, we can't completely rule out the possibility of personal data being transferred to AWS servers in the US. In this case, the following safeguards apply:
EU standard contractual clauses. You can request a copy of the EU standard contractual clauses from us. The provider has joined the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/), which ensures compliance with an adequate level of data protection based on a decision by the European Commission.

Google Cloud
Services: Server, hosting

Provider: In the European Economic Area (EEA) and Switzerland, Google services are provided by Google Ireland Limited, Ireland. Google Ireland Limited is a subsidiary of Google LLC, United States of America.
Website: https://cloud.google.com/
Further information & data protection: https://policies.google.com/?hl=de
There are no plans to transfer personal data to third countries. The transfer of personal data to third countries takes place depending on the respective Google service and in accordance with the various EU standard contractual clauses, provided these are offered by Google. Further information on this and Google's responsibility can be found at the following link: https://business.safety.google/gdpr/. You can view a copy of the EU standard contractual clauses there. The provider has joined the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov), which ensures compliance with an adequate level of data protection based on a decision by the European Commission.

DNN GmbH
Services: Marketing, consulting & marketing
Address: Rektoratsweg 36, 48159 Münster

ChatGPT
Services: Assistance with operation and customer support
Provider: OpenAI Ireland Limited, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
Website: https://openai.com/de-DE/policies/privacy-policy/
International Data Transfer: EU standard contractual clauses. You can request a copy of the EU standard contractual clauses from us.

Chatbase
Services: Customer support assistance
Provider: Chatbase, 4700 Keele Street, 215 Bergeron Centre, Toronto, ON, Canada, M3J 1P3
Website: https://www.chatbase.co/legal/privacy
Further information & data protection: https://www.chatbase.co/legal/terms and https://www.chatbase.co/legal/privacy
Appropriate safeguards: European Commission adequacy decision

maesn GmbH
Services: Interfaces to other systems
Address: c/o TechHubK67, Kasernenstraße 67, 40213 Düsseldorf
Website: https://www.maesn.com/

Microsoft Azure
Services: Server, Hosting

Provider: Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
Website: https://azure.microsoft.com/
Further information & data protection: https://azure.microsoft.com/de-de/explore/trusted-cloud/privacy and https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Twilio
Services: Cloud-communication (SMS, Voice Mail)
Provider: Twilio Ireland Limited, 25-28 North Wall Quay, Dublin 1, Irland
Website: https://www.twilio.com/
Further information & data protection: https://www.twilio.com/legal/privacy and https://www.twilio.com/legal/data-protection-addendum