# Flockler Data Processing Agreement (DPA) version 1.1. October 2026

**PREAMBLE AND INTRODUCTORY REMARKS**

This Flockler Data Processing Agreement ("**DPA**" or "**Data Processing Agreement**") and its Appendices reflects the parties' agreement with respect to the processing of personal data by **Flockler Commerce, Inc.**, 1870 The Exchange SE Ste 220, PMB 36051, Atlanta, GA 30339-2171, United States of America as the Supplier (i.e. the Processor of personal data) on behalf of the Customer(i.e. the Controller of personal data) or one of its Affiliates in connection with the Customers' use of the Flockler Services as per the Services Agreement.

This Data Processing Agreement consists of:
i) the General processing conditions set out in Appendix 1;
ii) the Data processing instructions regarding the processing of controller personal data in connection with the service & the List of Subprocessors ("**Processing Instructions**"), that are set out in Appendix 2;
iii) where applicable, the Standard Contractual Clauses for Processors ("**SCCs**") as set out in Appendix 3 ;
iv) where applicable, the United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**Addendum**") as set out in Appendix 4 ;
v) where applicable, the ("**US Processing Clauses**") as set out in Appendix 5 ;
vi) the List of technical and organisational measures offered by the Supplier for the protection of controller personal data ("**Security Requirements**") as set out in Appendix 6 and
vii) where applicable, the Processing clauses applicable to the processing of personal data in AI Systems as set out in Appendix 7 ("**Use of Personal Data in AI Systems**").

This DPA is supplemental to, and forms an integral and indispensable part of each Services Agreement (as specified in the Processing Instructions in the Purpose of processing / Legal grounds for processing - Services Agreement column next to each relevant service), which applies to all Flockler Services. In case of any conflict or inconsistency between the terms and clauses of this DPA and the terms and clauses of the relevant Services Agreement, this DPA will take precedence over the terms and clauses of the Services Agreement to the extent of such conflict or inconsistency.

In relation to this DPA and any data processing or other privacy issues, the Supplier has named a Data Protection Officer, who can be reached at privacy@flockler.com.

The Parties may make changes to this DPA at any time by either Party proposing the conclusion of an amendment to this DPA if the other Party accepts the proposed amendment. Unless stated otherwise, any change shall take effect once it is signed by both parties involved.

**APPLICATION AND BINDING EFFECT**

This DPA shall be deemed as validly concluded between the:

**Supplier**, namely **Flockler Commerce, Inc.,** 1870 The Exchange SE Ste 220, PMB 36051, Atlanta, GA 30339-2171, United States of America

Whereby **PARAGON d.o.o.**, Ograje 69, 1370 Logatec, Slovenia, Europe with company reg. no.: 9422676000 is acting as the EEA representative as per Article 27 of the GDPR for the Supplier (hereinafter jointly referred to as the "**Supplier**", "**data importer**", "**us**", or "**Processor**").

And the;

**Controller** ("**Customer**", "**data exporter**", "**you**" or "**User**") the legal entity that shall be identified as the registered user of the Flockler Services (as individually listed in Processing instructions) when you, the duly authorised individual representing said entity register a free or paid account in the name of the company you represent and are thereby bound to this DPA in accordance with the terms herein and the Services Agreement. The aforementioned also relates to any and all permitted users, personnel and affiliates.

Before the application of DPA you are asked to dully review, understand and get acquainted with the content of both the Services Agreement and this DPA.

By setting up an account and assenting to the Services Agreement or using any of the Flockler Services, you warrant that you have read, understand, agree to and accepted terms contained herein and that you have therefore entered into a legally binding agreement with the Supplier in the context of the terms and clauses herein, and that you have the power and authorisation to enter into this DPA personally or on behalf of the company you have named as the user and to bind that company to this DPA.

The Parties may make changes to this DPA at any time by either Party proposing the conclusion of an amendment to this DPA if the other Party accepts the proposed amendment. Unless stated otherwise, any change shall take effect once it is signed by both parties involved or by way of the Supplier notifying the Controller of any proposed changes and setting a deadline after which the changes shall take effect should the Controller elect to continue using the Flockler Services.

## VERSION HISTORY

| Version no. | Date of publication and changes from last version |
|---|---|
| 1.0. | First published version - June 2026 |
| 1.1 | Appendix 6 (Security Requirements) updated to reflect the SOC 2 Type II report and current controls - October 2026 |

# APPENDIX 1: GENERAL PROCESSING CONDITIONS

## 1. DEFINITIONS

For the purposes of this DPA and unless otherwise indicated in this Agreement, the terminology and definitions as used by the Regulation (EU) 2016/679 ("**GDPR**") and/or when applicable by the UK General Data Protection Regulation ("**UK GDPR**"), Data Protection Act 2018 ("UK Data Protection Laws") and the applicable data protection and privacy laws of the USA when Appendix 5 of this DPA applies.

In addition, the following terms shall have the following meaning:

1.1 **Addendum** shall mean the United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner and effective from 21 March 2022.

1.2 **Agreement** shall mean the Services Agreement that regulates the use of the Flockler Service (as specified in the Processing Instructions in the Purpose of processing / Legal grounds for processing - Services Agreement column next to each relevant service) and any successive agreement concluded by and between the Controller and the Supplier.

1.3 **Affiliate** shall mean a person/legal entity that directly, or indirectly through one or more intermediaries, owns or controls, is owned or is controlled by, or is under common ownership or control with, another person/legal entity.

1.4 **Controller Personal Data** shall mean any personal data processed by the Supplier or any Affiliate / Subprocessor of the Supplier on behalf of the Controller or any of its Affiliates, as set out in the Processing Instructions and elsewhere in this DPA.

1.5 **Security Requirements** shall mean the technical and organisational security measures included in Appendix 6 to this DPA.

1.6 **Controller** or **Data Controller** or **data exporter** shall mean the Controller and/or any its Affiliates for which the Data Processor processes Controller Personal Data as set out in the Processing Instructions and elsewhere in this DPA. "Data Controller" shall be understood to include "Business" and analogous terms under applicable Data Protection Law.

1.7 **Data Processor** or **Supplier** or **data importer** shall mean the individual who, or entity that, processes Personal Data on behalf of the Controller. "Data Processor" includes "Service Provider" and analogous terms as defined under applicable Data Protection Law.

1.8 **Data Protection Law** Shall mean any laws relating to the processing of personal data and the protection of privacy to which Parties are subject, including without limitation, the GDPR, the Privacy and Electronic Communications Data Protection Directive (2002/58/EC) and any laws and regulations implementing or created pursuant to the GDPR or the Privacy and Electronic Communications Directive, the UK GDPR, the UK Data Protection Act 2018 the California Consumer Privacy Act of 2018 or their successor regulations.

1.9 **Security Breach** shall mean a breach in the technical and/or organisational measures to protect the confidentiality, integrity or availability of Personal Data or an incident that leads to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, Personal Data.

1.10 **Data Subject** shall mean an identified or identifiable natural person. "Data Subject" shall be understood to include "End Users" or "Individuals" that may interact with the Flockler Services when they are used by or deployed by the Controller or when the Controller enters their data into the services. The terms "Individual" or "Consumer" and any analogous terms are to be interpreted as per applicable Data Protection Law.

1.11 **Data Subject Request** shall mean requests of Data Subjects to exercise their rights under Data Protection Law.

1.12 **Member State** shall mean a country that is a member of the European Economic Area ("**EEA**") and the United Kingdom.

1.13 **Parties/Party** shall mean Controller and Supplier, which will jointly be referred to as "**Parties**" and individually referred to as a "**Party**".

1.14 **Processing Services** or **Services** shall mean the services which the Supplier agreed to provide Controller and/or its Affiliates as per the concluded Services Agreement and as further specified in the Processing Instructions.

1.15 **SCCs** shall mean the standard contractual clauses annexed to the EU 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.

1.16 **Flockler Services** shall mean the online platform(s) and software program(s) with the core functionalities as described in the Services Agreement and any related services, that the Supplier offers to the Controller under the Services Agreement and the respective underlying infrastructure, whereby provision of the Flockler Services requires the processing of certain Controller Personal Data for its normal and intended functioning, as further specified in the Processing Instructions and this DPA.

1.17 **Subprocessor** shall mean another Data Processor, located within or outside the EEA and/or the United Kingdom, that is engaged by Supplier as a subcontractor for the performance of the Processing Services or parts of the Processing Services on behalf of Controller and/or its Affiliates. The list of engaged subprocessors is disclosed in the appended Processing Instructions (i.e. Appendix 2).

## 2. ROLES

Parties acknowledge and agree that with regard to the processing of the Personal Data, the Controller or its Affiliates are the Data Controllers and the Supplier and its Affiliate are the Data Processors.

The Controller shall be entitled to exercise the Data Controller's contractual rights and powers (i.e., the rights and powers ensuing from this DPA) and the Data Controller's statutory privacy law-related rights and powers (i.e. the rights and powers ensuing from the Data Controller's position) vis-à-vis the Supplier (for the avoidance of doubt, the Data Controller shall remain entitled to exercise these rights and powers in its own name at any time at its discretion).

2.1 The Parties agree that Affiliates may accede to or leave this DPA at any time as a Data Controller subject to a notice to the Supplier.

2.2 To the extent applicable and the Data Controller(s) are contracting parties to this DPA instead of third party beneficiaries, the Parties agree that the bundling of the Data Controllers within this single DPA is only undertaken for efficiency purposes (i.e., to avoid a multitude of different DPAs with different entities) and (i) shall result in legally separate DPAs between the respective Data Controllers and the Supplier and (ii) shall not create any legal or other relationship whatsoever between the "bundled" Data Controllers and the Supplier. For the avoidance of doubt: the obligations of each Data Controller under this DPA shall be several but not joint in respect of the obligations of any other Data Controller and no Data Controller shall be liable to the Supplier for the actions of any other Data Controller as permitted under applicable law.

## 3. OBLIGATIONS OF THE SUPPLIER AND THE CONTROLLER

3.1 The Supplier shall solely process Controller Personal Data as instructed in this DPA, unless the Data Controller issues additional written instructions as mutually agreed by the parties or as otherwise required by applicable Data Protection Law. The Supplier will process Customer Personal Data for the purpose and in accordance with the Services Agreement and this DPA (namely the Processing Instructions the Customer gives the Supplier in Appendix 2 and their user account (e.g. through the Service platform dashboard). The Customer agrees that the Services Agreement and the Processing Instructions given as explained in the preceding sentence of this paragraph may be deemed as the complete and final instructions given to the Supplier in relation to Customer Personal Data. Additional instructions outside the scope of this DPA require prior written agreement between you and us, including, as the case may be, agreement on any additional fees payable for carrying out such instructions. Any data collected pursuant to data analytics or monitoring carried out by the Supplier in connection with the provision of the Services or otherwise connected with Customer's use of the Services may include Personal Data, which Customer hereby authorizes the Supplier to use solely in accordance with carrying out its obligations under the Services Agreement or this DPA.

3.2 The Supplier shall upon the Data Controller's request promptly provide to the Data Controller all information and documentation reasonably requested to demonstrate compliance with the obligations of the Supplier under Data Protection Law and this DPA.

3.3 Supplier shall immediately notify the Data Controller if, in its opinion:

a. an instruction of the Data Controller infringes Data Protection Law or if applicable law requires it to process the Controller Personal Data other than in accordance with the Data Controller's instructions and this DPA; and/or

b. changes in any laws, regulations or government policies applicable to Supplier that are likely to have an adverse effect on the obligations of this DPA and/or the rights and interests of the Data Subject's whose personal data is processed in relation to this DPA.

Following such notification, the Data Controller may suspend the transfer to and processing of Controller Personal Data by Supplier and terminate the Agreement and this DPA at its discretion at any time without any liability towards the Supplier.

3.4 The Supplier shall implement appropriate technical and organisational security measures and, at a minimum, the measures included in the Security Requirements when processing Controller Personal Data. The Supplier shall monitor developments in law, technology and security and will continually adopt additional measures, if and where needed, to ensure that the measures implemented remain up to date and appropriate, taking into account the nature of the Controller Personal Data and the risks which might arise from its unauthorised or unlawful destruction, loss, alteration, access or disclosure.

3.5 The Supplier shall only permit persons to access Controller Personal Data as strictly necessary for the provision of the Processing Services and in particular only to employees of Supplier and employees of any Subprocessors that are bound by confidentiality obligations or are under an appropriate statutory obligation of confidentiality with regard to the Controller Personal Data.

3.6 The Supplier shall assist the Controller with its obligation, where applicable under Data Protection Law, to carry out a data protection impact assessment (or similar required data protection assessments) and prior consultation with supervisory authorities in relation to the processing of Controller Personal Data including by providing the necessary information to the Data Controller and fully cooperating with any request or investigation in relation to such data protection impact assessment by a supervisory authority.

3.7 The Data Controller shall exclusively handle and respond to Data Subject Requests relating to Controller Personal Data. The Supplier shall notify the Data Controller if it receives a Data Subject Request, and in any event no later than 72 hours after receiving such request. The Supplier shall, insofar as this is reasonable and possible, assist the Data Controller with the fulfilment of the Controller's obligation to comply with the Data Subject Requests.

3.8 During the term of the Agreement, the Supplier is obliged to either dispose of Controller Personal Data in accordance with the retention schedule as set out in the Processing Instructions or to return Controller Personal Data back to the Data Controller, unless applicable Data Protection Law requires that the Supplier retain such data. In such cases, the Supplier shall ensure that Controller Personal Data are kept confidential and are not further processed.

3.9 After the end of the provision of the Processing Services, the Supplier shall, if explicitly requested by the Controller to do so, transfer free of charge the Controller Personal Data to the Controller within 30 days after the termination of the Services Agreement. Otherwise, the Supplier shall delete the Controller Personal Data (including any back-up copies). The Supplier shall at the first request of the Data Controller attest (or if possible certify) that all Controller Personal Data has been deleted. Where applicable Data Protection Law requires Supplier to retain Controller Personal Data, Supplier shall promptly inform the Data Controller and shall ensure that Controller Personal Data are kept confidential and are not further processed.

3.10 If the Controller requests at its own discretion a copy of the Controller Personal Data held by the Supplier and its Subprocessor(s), the Supplier shall provide this without undue delay, free of charge and in a structured and commonly used format.

## 4. INFORMATION AND NOTIFICATION OBLIGATIONS

4.1 The Supplier shall promptly and in writing notify the Controller of:

a. any legally binding request for access to Controller Personal Data by a public authority received by the

Supplier or its Subprocessor(s) to enable the Controller to intervene and seek relief from such disclosure, unless the Supplier is legally prohibited from providing such notice, despite having used its reasonable best efforts to waive the prohibition;

b. any direct access by public authorities to Controller Personal data in which case the Supplier shall provide the Controller with all information available to the Supplier in this respect; and

c. any order, request, complaint or other demand by a court, supervisory authority or other regulator in relation to the Controller Personal Data received by the Supplier or its Subprocessor(s), without responding to such order, request, complaint or demand unless the Supplier has been authorised to do so in writing by the Controller. The Supplier shall provide all such cooperation and assistance to the Controller as the Controller may reasonably require in relation to any such order, request, complaint or other demand.

4.2 In the event Clause 4.1 (a) or (c) applies and it concerns a request, order, complaint or other demand received by the Supplier, the Supplier shall:

a. request that the public authority directs its request at the Data Controller, instead of Supplier. The Supplier will document any such request;

b. act in compliance with its established policies regarding the disclosure of personal data to public authorities;

c. oppose any request for access or disclosure and contest its legal validity to the extent legally permitted under applicable law; and

d. provide the minimum amount of information permissible when legally required to respond to the request for access or disclosure in case of unsuccessful opposition to the request, based on a reasonable interpretation of the request, and request the public authority to reduce the scope of any such request determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society.

4.3 Upon request of the Data Controller, the Supplier shall provide the Data Controller with:

a. an overview of laws and regulations that permit access to the Controller Personal Data in the jurisdiction to which the Supplier is subject, to the extent the Supplier is reasonably aware of such laws and regulations;

b. general information on the requests received from and/or direct access by public authorities, including on the nature and number of such requests in the preceding 12 month period relating to personal data it processes as a Data Processor. Where possible, such information will include the following:

(i) information about the nature and number of such requests received by the Supplier;
(ii) the type of data requested;
(iii) the requesting public authority;
(iv) the legal basis to disclose personal data to the public authority;
(v) in case the Supplier reasonably believes that it is legally prohibited to provide the information in subsections (i) to (iv) above, the extent to which such prohibition applies; and

c. any measures taken to prevent access by public authorities to the Controller Personal Data.

4.4 The Supplier is obliged to notify the Data Controller in writing without undue delay, and in any event within 48 hours, of any Data Security Breach after the Supplier becomes aware thereof. The Supplier shall: a) assist the Data Controller in satisfying the Data Controller's obligations under Data Protection Law to inform the Data Subjects and the applicable supervisory authorities, as may be required, of the Data Security Breach by providing all necessary information available to the Supplier in relation to the Data Security Breach and its remediation; b) take all necessary steps to investigate, mitigate and remediate the cause and the risks posed by the Data Security Breach, without obstructing the data Controller's investigations as may be necessary to comply with its obligations under Data Protection Law to inform the Data Subjects and the supervisory authorities; and c) where a Data Security Breach is discovered that was caused by the Supplier or its Subprocessors, the Supplier shall review the implemented technical and organisational measures and, if needed, shall make appropriate changes to prevent such Data Security Breach from reoccurring.

## 5. AUDIT

5.1 The Supplier shall make available to the Controller on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections by the Controller or an auditor mandated by the Controller in relation to the Processing of the Controller Personal Data by the Supplier or the Subprocessors. The Supplier shall immediately inform the Controller if, in their opinion, an audit request/instruction infringes the GDPR or other applicable data protection provisions, this DPA, or the Services Agreement.

5.2 When undertaking an audit, the Controller shall give the Supplier a notice at least five (5) business day prior to any audit or inspection being conducted under this section and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, unavoidable, to minimise) any damage, injury or disruption to the Supplier's or any Subprocessors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The Controller may conduct an audit by providing a notice to Supplier less than five (5) business days ahead if 1) there is an extraordinary audit to clarify the circumstances of a Data Breach, or 2) when the Controller is required or requested to carry out such an audit by a supervisory authority or any similar regulatory authority responsible for the enforcement of Data Protection Law in any country or territory. The Supplier or a Subprocessor need not give access to its premises for the purposes of such an audit or inspection:

a. to any individual unless he or she produces reasonable evidence of identity and authority;
b. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Controller undertaking an audit has given notice to the Supplier that this is the case before attendance outside those hours begins.

5.3 The Supplier shall, upon request also provide the Controller or the mandated auditor with documentation of implemented technical and organisational measures to ensure an appropriate level of security, and other information necessary to demonstrate the Supplier's or the Subprocessor's compliance with its obligations under this DPA and relevant Applicable legislation, but shall provide access to information concerning the Supplier's or the Subprocessor's other information subject to confidentiality obligations.

5.4 The Controller shall bear any and all costs related to any audit, regardless of the outcome of the audit or the reason for the audit.

## 6. SUBPROCESSING

6.1 Subject to the Supplier complying with the obligations set forth in this Clause 6, the Data Controller grants the Supplier general authorisation to engage Subprocessors.

6.2 The Supplier shall choose any Subprocessor diligently and ensure that any Subprocessor provides sufficient guarantees that it will implement and maintain appropriate technical and organisational measures to ensure that its processing of Controller Personal Data meets the requirements set out in this DPA and applicable Data Protection Law.

6.3 The Supplier shall enter into a written contract with any Subprocessor ("**Subprocessing Agreement**") and such Subprocessing Agreement shall impose upon the Subprocessor equivalent obligations as imposed by this DPA upon the Supplier, in particular in relation to the implementation of appropriate technical and organisational measures to meet the requirements of Data Protection Law, to the extent relevant to the subcontracted Processing Services.

6.4 Prior to entering into this DPA, the Supplier has provided to the Data Controller a list of all Subprocessors engaged by Supplier in the Processing Instructions (see "**List of Subprocessors**" in Appendix 2) represented as an online list of subprocessors that are engaged in the provision of the Flockler Service, whereby this list forms an integral part of this DPA).

6.5 The Data Controller and the Supplier hereby agree, that all of the subprocessors on the List of Subprocessor, both at the moment of signing of this DPA and in all future instances, represents the List of Subprocessors which have been accepted by the Data Controller as being allowed to be engaged for the purposes of supplying the stated Processing services. The Controller is required to continuously monitor the List of Subprocessors and raise any objection with the Supplier via email at privacy@flockler.com.

6.6 If the Data Controller has a reason to object to a Subprocessor, the Data Controller shall notify the Supplier thereof in writing. If the Data Controller objects to the use of the Subprocessor, the Parties shall use reasonable efforts to address the objection through one of the following options: (a) the Controller will discontinue using the Flockler Services; (b) the Supplier will offer an alternative to provide the Processing Services without such Subprocessor; or (c) the Supplier will take the corrective steps requested by the Data Controller in its objection (which would therefore remove Controller's objection) and proceed to use Subprocessor. If none of the above options are reasonably available and the Controller has not objected to the engagement of a new Subprocessor within five (5) days after the receiving sufficient notification or after such subprocessor being added to the List of Subprocessors, such Subproecessor shall be deemed as duly accepted by the Controller. If an objection had been duly raised by the Controller and no remedy could be found by either party, either party may terminate the affected Services Agreement with reasonable prior written notice without any liability towards the other party.

6.7 The Supplier shall provide, at the data Controller's request, a copy of each sub-processor data protection agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secrets or other confidential information, including personal data, the Supplier may redact the text of the agreement prior to sharing a copy.

6.8 The Supplier shall remain responsible to the Controller for the performance of the sub-processor's obligations under this DPA in the context of applicable laws. The Supplier shall notify the Controller of any failure by the sub-processor to fulfil its obligations under the DPA or the individual data processing agreement.

6.9 The Supplier shall agree a third-party beneficiary clause with the sub-processors whereby – in the event the Supplier 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. DATA TRANSFERS

7.1 The Data Controller authorises the Supplier to transfer the Controller Personal Data to the Processing Locations listed in the Processing Instructions. Where Supplier intends to transfer Controller Personal Data to a Processing Location not yet authorised by the Data Controller, the Supplier shall provide the Data Controller with ten (10) days advance notice of this intent. The Data Controller has the right to object in writing within five (5) days following receipt of such notice, citing its reasons for objecting. The Parties shall resolve such an objection in accordance with Clause 6.6 (mutatis mutandis).

7.2 The parties recognise, that the Supplier is established in the USA, namely a country outside the EEA that is not recognized as providing an adequate level of data protection by the European Commission at the time of the conclusion of this DPA, whereby the Data Controller hereby designates, that the appended SCCs (or possibly the other appendices, should the Data Controller be an entity, that is established in the UK or if UK / USA citizen data forms part of the Controller Personal Data) provide for a sufficient international data transfer mechanism. If an existing adequacy finding is amended or invalidated, or a derogation can no longer be relied upon in the opinion of the Data Controller, the Parties hereby agree that the potential new version of the SSCs apply to the transfer and further processing of the Controller Personal Data under this DPA.

7.3 When Clause 7.2 triggers the application of the SCCs and, where relevant, the Addendum between parties, the following terms apply:

a. The parties hereby agree that the SCCs shall automatically be replaced by any successor or replacement standard contractual clauses as approved by the European Commission. Parties shall each in good faith take those actions required to ensure any successor or replacement standard contractual clauses come into effect between Parties;

b. The parties hereby agree that the Addendum shall be automatically replaced by any successor or replacement clauses approved under UK laws. Parties shall each in good faith take those actions required to ensure any successor or replacement of the Addendum comes into effect between Parties;

c. The information required in Annexes I and III of the SCCs shall be as set out in the Processing Instructions. The information required in Annex II of the SCCs shall be as set out in the Security Requirements;

d. The SCCs and, where relevant, the Addendum shall prevail and take precedence over conflicting terms in the General Data Processing Conditions.

7.4 In the event of a data transfer to a country outside the EEA and/or UK as set out in clause 7.2, the Supplier (and its Subprocessor(s), as applicable) will assess whether the laws applicable to it provide adequate protection under

Data Protection Law. To the extent that it determines that any such laws are not in line with the requirements of the SCC, Addendum and/or an adequacy decision issued under Data Protection Law, and applicable Data Protection Law, it shall comply with the safeguards set out in Clauses 7.5-7.6 and provide the Data Controller the information and documentation reasonably requested to demonstrate compliance with these safeguards.

7.5 The Supplier (and its Subprocessor(s), as applicable), shall adopt supplementary measures to protect Controller Personal Data in accordance with the requirements of Data Protection Law, including by implementing appropriate technical and organisational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect Controller Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.

7.6 The Supplier warrants for itself and its Subprocessor(s), as applicable, that they:

a. have not purposefully created, or are legally required by national law or government policy to create or maintain, any means by which a public authority or third party can bypass their security mechanisms, authentication procedures and/or software to gain access to and/or use their systems and/or the Controller Personal Data, such as a back door or similar programming, or the handover of the encryption key to access such data; and

b. have not purposefully created or changed their business processes, security mechanisms, software and/or authentication procedures in a manner that facilitates access to their systems and/or the Controller Personal Data by public authorities or third parties.

7.7 The parties hereby agree, that where the Supplier engages a USA based Subprocessor in accordance with this DPA and the Processing Instructions (i.e. for carrying out specific processing activities on behalf of the Supplier for the provision of the Flockler Services to the Controller) and such engaged processing activities involve the transfer of Controller Personal Data within the meaning of Chapter V of the GDPR, the Processor may also engage such Subprocessor without the implementation of SCC (and additional safeguards), if such Subprocessor has duly undergone and achieved full self-certification in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (i.e. the new EU-USA data transfer framework as per the stated adequacy decision from the 10th of July 2023).

## 8. LIMITATION OF LIABILITY

8.1 Each Party is liable for its obligations set out in this DPA and in the applicable Data Protection Law. Any liability arising out of or in connection with a violation of the obligations of this DPA or under applicable Data Protection Law, shall follow, and be governed by, the liability provisions set forth in, or otherwise applicable to, the Services Agreement. If the liability provisions in the Service Agreement do not cover liability under this DPA or applicable Data Protection Law then neither party will exclude or limit its liability under this DPA.

## 9. INDEMNIFICATION

9.1 The Controller will defend, indemnify, and hold harmless the Supplier and the officers, directors, employees, successors, and agents of Controller from all claims, damages, liabilities, assessments, losses, costs, administrative fines and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses) arising out of or resulting from any claim, allegation, demand, suit, action, order or any other proceeding by a third party (including supervisory authorities) that arises out of or relates to the violation of the Controller's obligations under this DPA or applicable Data Protection Law.

## 10. MISCELLANEOUS

10.1 This DPA shall be governed by the laws of the Republic of Slovenia, where the EEA representative of the Supplier is located.

10.2 The place of jurisdiction for all disputes regarding this DPA shall be as determined by the Services Agreement, or, in the absence thereof: Ljubljana, Slovenia.

10.3 Nothing in this DPA shall be construed so as to create a partnership or joint controller or joint venture relationship between the Parties.

10.4 To the extent that any changes in applicable law, regulatory requirements or case law compel the parties to amend the terms of this DPA, the Parties shall without undue delay enter into negotiations to appropriately address such changes.

10.5 Parties mutually agree that this DPA is subject to amendments in light of regulatory changes or other changing circumstances and hereby agree to amend this DPA in good faith where necessary.

10.6 Should any provision of this DPA be held by a court of competent jurisdiction to be invalid, illegal, void or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omissions.

10.7 In the event of inconsistency between the provisions of this DPA and any other agreements between the parties, including the Agreement, the provisions of this DPA shall prevail with regard to the parties' obligations under the DPA or any matter relating to data protection.

# APPENDIX 2: DATA PROCESSING INSTRUCTIONS REGARDING THE PROCESSING OF CONTROLLER PERSONAL DATA IN CONNECTION WITH THE SERVICE & THE LIST OF SUBPROCESSORS ("PROCESSING INSTRUCTIONS")

**General method and purpose of data collection**

In order to provide the Flockler Services and the corresponding features as per the concluded Services Agreement:

a) the Controller may input Controller Personal Data directly into the Flockler Service himself;
b) Controller Personal Data may also be entered into the Flockler Service by partners, affiliates, contractors of the Controller or other persons and entities that are authorised or instructed to do so by the Controller, and;
c) by end users, consumers or other individuals which interact with the Flockler Service that had been integrated or put into use by the Controller (e.g. integrated with the websites/systems of the Controller, etc.).

In all of the cases outlined above, the Supplier is therefore instructed by the Controller under this DPA to collect, store and process the entered data, so that the Controller may use the Flockler Services for his own business interests.

**General categories of Data Subjects**

The categories of Data Subjects whose personal data may be processed under this DPA correspond to the features the Controller elects to use in connection with the Flockler Services and are thereby defined by the individual use-case of the Controller as follows:

- Controller's End Users (i.e. employees or other authorised users of the Customer, other end users, consumers or other individuals which interact with the Services that had been integrated or put into use by the Customer (e.g. integrated with the systems of the Customer or otherwise inserted or collected by/through the Services
- other Data Subjects (i.e. when the Controller or his Affiliates/partners enter and use data of any other Controller Personal Data into the Flockler Service);

whereby the Controller expressly warrants to the Supplier, that he has satisfied the requirements regarding lawfulness of processing based on Article 6 of the GDPR or any other Data Protection Law requirement that might be binding in relation to Controller Personal Data prior to collecting/transferring/and otherwise processing such data in any way in connection with the Flockler Services.

**Personal Data types and the subject-matter, nature and purpose of processing and List of Subprocessors**

Subject to the Controller's use of the Flockler Services, the following processing of Controller Personal Data is instructed by the Controller to be carried out by the Supplier or his Affiliates/Subprocessors in order to provide each feature of the Flockler Services:

| **Controller Personal Data or other personally identifiable information** | **Purpose of processing / Legal grounds for processing - Services Agreement** | **Categories of individuals** |
|---|---|---|
| **Flockler - base level Service** | | |
| IP Address<br>Name (freeform text field)<br>Public social media content<br>Public social media handle<br>Social media account data for connected accounts (including username, association to a person, access token)<br>Email | Purpose of processing: Essential for offering the Flockler service.<br><br>Legal ground: Contractual (offering the service on the basis of the Flockler Terms & Conditions) | Individuals that are tied to the social media content that is shared with the Controller and the visitors of the website of the Controller. |
| **AI Customer content moderation - Feature** | | |
| IP Address<br>Name (freeform text field)<br>Public social media content<br>Public social media handle<br>Social media account data for connected accounts (including username, association to a person, access token)<br>Email | Purpose of processing: Content screening by AI for moderation purposes.<br><br>Legal ground: Opt-in feature. | Individuals that are tied to the social media content that is shared with the Controller and the visitors of the website of the Controller. |

**Retention Schedule**

The Supplier will store the Controller Personal Data for as long as it is necessary to fulfil the above stated purposes for processing and shall delete and procure the deletion of all copies of stored Controller Personal Data within 30 (thirty) business days (or 90 (ninety) days where the data is shared with AWS or Sentry - please see the List of Subprocessors) of the date of termination of the Services Agreement (i.e. termination by either the Controller or the Provider under the applicable clauses of the Services Agreement such as product/widget uninstall, as the case may be) or the date of the user account deletion (whatever comes first, whereby termination of the Services Agreement also means that the user account of the Controller and all corresponding Controller Personal Data shall be deleted in 30 days or 90 days where the data is shared with AWS or Sentry - see above).

Individual data deletion requests will be initiated immediately and the data shall be deleted within 30 days or 90 days when the data is shared with AWS or Sentry.

**List of Subprocessors**

The list of engaged and agreed upon Subprocessors is available to the Controller at https://flockler.com/subprocessors.

# APPENDIX 3: STANDARD CONTRACTUAL CLAUSES

## SECTION I

### Clause 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Processing Instructions.

(d) The Processing Instructions and Security Requirements form an integral part of these Clauses.

### Clause 2 - Effect and invariability of the Clauses

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

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

### Clause 3 - Third-party beneficiaries

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

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

(ii) Clause 8.1 (b), 8.9(a), (c)-(e);

(iii) Clause 9(a), (c)-(e);

(iv) Clause 12(a), (d), and (f)

(v) Clause 13

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

(vii) Clause 16(e);

(viii) Clause 18.

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

### Clause 4 - Interpretation

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### Clause 5 - Hierarchy

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

### Clause 6 - Description of the transfer(s)

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

### Clause 7 - Intentionally left blank

## SECTION II – OBLIGATIONS OF THE PARTIES

### Clause 8 - Data protection safeguards

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

**8.1 Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

**8.2 Purpose limitation**

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

**8.3 Transparency**

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

**8.4 Accuracy**

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

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

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

**8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the

implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

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

**8.8 Onward transfers**

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

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

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

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

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

**8.9 Documentation and compliance**

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

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

**Clause 9 - Use of sub-processors**

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[2] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

**Clause 10 - Data subject rights**

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

**Clause 11 - Redress**

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

competent supervisory authority pursuant to Clause 13;

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

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

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**Clause 12 - Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

**Clause 13 - Supervision**

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in the Processing Instructions shall act as competent supervisory authority.

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

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

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

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

**Clause 14 - Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[3]

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

**Clause 15 - Obligations of the data importer in case of access by public authorities**

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### Clause 16 - Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

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

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

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

(iii) the data importer fails to comply with a binding decision of a competent court or

supervisory authority regarding its obligations under these Clauses.

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

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17 - Governing law**

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

Where such laws do not allow for third party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third party beneficiary rights. The Parties agree that this shall be the Laws of the Netherlands.

**Clause 18 - Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of the jurisdiction of the applicable Controller entity.

# APPENDIX 4: UNITED KINGDOM INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

**VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the UK Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## Part 1: Tables

**Table 1: Parties**

| | | |
|---|---|---|
| **Start date** | will be the "Effective Date" as stated in this Agreement | |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' details** | As set out on page 1 of this DPA | As set out on page 1 of this DPA |
| **Key Contact** | (see the préambule of this DPA) | (see the préambule of this DPA) |
| **Signature (if required for the purposes of Section 2)** | The DPA, including this Addendum, is made legally binding to the Data Exporter by means of the conclusion of the Services Agreement | The DPA, including this Addendum, is made legally binding to the Data Exporter by means of the conclusion of the Services Agreement |

## Table 2: Selected SCCs, Modules and Selected Clauses

| | |
|---|---|
| **Addendum EU SCCs** | The version of the Approved EU SCCs which this Addendum is appended to, detailed above, including the Appendix Information. |

## Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

| |
|---|
| Annex 1A: List of Parties:<br><br>Set out in the "Processing Instructions" within the DPA |

| |
|---|
| Annex 1B: Description of Transfer:<br><br>Set out in the “Processing Instructions” within the DPA |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:<br><br>Set out in the “ Security Requirements” |
| Annex III: List of Subprocessors (Modules 2 and 3 only) (see the relevant column of the table from Appendix 2):<br><br>(Data Importer to supply list or link) |

## Table 4: Ending this Addendum when the Approved Addendum Changes

| | |
|---|---|
| **Ending this Addendum when the Approved Addendum changes** | The Data Exporter may end this Addendum as set out in Section 19. |

## Part 2: Mandatory Clauses

**Entering into this Addendum**

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

**Interpretation of this Addendum**

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

| | |
|---|---|
| Addendum | This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| Addendum EU SCCs | The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information. |
| Appendix Information | As set out in Table 3. |

| | |
|---|---|
| Appropriate Safeguards | The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved Addendum | The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18. |
| Approved EU SCCs | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| ICO | The Information Commissioner. |
| Restricted Transfer | A transfer which is covered by Chapter V of the UK GDPR. |
| UK | The United Kingdom of Great Britain and Northern Ireland. |
| UK Data Protection Laws | 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. |
| UK GDPR | As defined in section 3 of the Data Protection Act 2018. |

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

**Hierarchy**

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

**Incorporation of and changes to the EU SCCs**

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

F. 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 Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”; m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”; n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

**Amendments to this Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

# APPENDIX 5: UNITED STATES PROCESSING CLAUSES

This Appendix 5 of the DPA shall apply to the extent Supplier processes personal data that relates to an identified or identifiable household or individual in the United States, where such personal data is provided by or on behalf of the Data Controller to Supplier in connection with Supplier's performance of the Services pursuant to the Agreement ("US Personal Data").

To the extent Supplier processes US Personal Data as a Data Processor or "service provider" under applicable Data Protection Laws, Supplier agrees to process such US Personal Data subject to the General Processing Conditions set forth in Appendix 2 of this DPA and the following provisions:

1. Supplier acknowledges that the Controller is disclosing to Supplier, or authorising Supplier to collect on the Data Controller's behalf or otherwise making available, US Personal Data only for the limited and specified purposes set out in the Processing Instructions set forth in Appendix 2 of this DPA, or as otherwise specified under the Agreement and any applicable Statement of Work (collectively, the "**Instructions**").

2. Supplier shall: (1) process US Personal Data only as set forth in the Instructions; and (2) process US Personal Data at all times in compliance with Data Protection Laws, including by providing no less than the level of privacy protection as required by Data Protection Laws.

3. Supplier shall not: (1) retain, use, disclose, or otherwise process US Personal Data except as necessary for the business purposes specified in the Instructions; (2) "Sell" or "Share" US Personal Data as those terms are defined under Data Protection Laws; (3) retain, use, disclose, or otherwise process US Personal Data in any manner outside of the direct business relationship between the Data Controller and Supplier; or (4) combine any US Personal Data with any personal data that Supplier receives from or on behalf of any other third party or collects from Supplier's own interactions with Data Subjects, provided that Supplier may so combine US Personal Data with other personal data for a purpose permitted under Data Protection Laws if directed to do so by the Data Controller or as otherwise expressly permitted by Data Protection Laws.

4. The Data Controller may, upon providing reasonable notice to Supplier, take all reasonable and appropriate steps to prevent, stop, or remediate any unauthorized processing of US Personal Data.

5. Supplier agrees to promptly notify the Data Controller if it can no longer comply with Data Protection Laws applicable to US Personal Data, no later than three business days after it makes a determination that it can no longer meet its obligations.

6. For purposes of this Appendix 5 of the DPA, "**Deidentified Data**" means data originally created from US Personal Data that has been deidentified or anonymized such that it cannot reasonably be used to infer information about, or otherwise be linked to, a Data Subject and where such data is processed only in accordance with this Clause 6 of Appendix 5 of the DPA. To the extent the Data Controller discloses or otherwise makes available Deidentified Data to Supplier, or to the extent Supplier creates Deidentified Data from US Personal Data, Supplier shall (1) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (2) publicly commit to maintain and use such Deidentified Data in a deidentified form and to not attempt to re-identify the Deidentified Data, except that Supplier may attempt to re-identify the data solely for the purpose of determining whether Supplier's deidentification processes are compliant with Data Protection Laws; and (3) before sharing Deidentified Data with any other party, including Subprocessors, contractors, or any other persons ("**Recipients**"), contractually obligate any such Recipients to comply with all requirements of this Clause 6 of Appendix 5 of the DPA (including imposing this requirement on any further Recipients).

# APPENDIX 6: SECURITY REQUIREMENTS

The controller accepts the following Security Requirements as adequate and sufficient at the time of the conclusion of this Agreement. The Supplier shall not offer a lower level of Security Requirements than that listed at the time of the conclusion of this Agreement.

The Security Requirements describe the baseline technical and organisational measures that the Supplier will maintain through its systems and the Flockler Services and that the Supplier will operate to ensure confidentiality, integrity and availability of any data (including but not limited to personal data) created, collected, transferred or otherwise processed and provide the Services to Controller, in a manner that the data and the Services are sufficiently protected at all times (such as where appropriate, encryption, pseudonymization and anonymization).

**Security Requirements that have been integrated for the Flockler service:**

The following Measures reflect the controls attested in the Processor's SOC 2 Type II report (examination period 15 April 2026 to 15 July 2026), covering the Security trust services criteria:

---

**1. Physical access control**

- All production infrastructure and customer personal data are hosted in AWS data centres. The Processor maintains no on-premises servers, network hardware, or physical stores of customer personal data.
- Physical and environmental security of the hosting facilities is the responsibility of AWS, whose controls include: physical access to data centres approved by an authorised individual and managed through electronic access-control devices; physical access revoked within 24 hours of an employee or vendor record being deactivated; access reviewed on a quarterly basis; and CCTV monitoring of server locations, with images retained for at least 90 days unless limited by legal or contractual obligation.
- The Processor reviews AWS's attestation reports and performs a risk analysis of AWS at least annually.
- The Processor operates a bring your own device (BYOD) model. A BYOD and workstation security policy requires all devices accessing company systems and production resources to have active anti-malware software enabled, and compliance with endpoint security requirements is verified periodically.

**2. Logical and system access control**

- Access to systems and infrastructure is governed by a documented Access Security Policy and enforced through role-based access control (RBAC) on a least-privilege basis. Access is split into admin, user, and no-access roles.
- Access is granted based on job responsibility and is requested, documented, and authorised by management prior to the user's start date.
- In-scope systems and applications authenticate users with a unique user account and enforce minimum password requirements.
- Access to the production environment is restricted to members of the Operations team; backup infrastructure is accessible only to key personnel.
- User access roles and privileges are reviewed and re-approved (or updated) by management at least annually.
- Upon termination, access to all in-scope systems is disabled by IT following notification from HR, within 24 business hours; all access changes, including terminations, are documented and tracked in the ticketing system.

**3. Encryption and pseudonymisation**

- Customer data is encrypted both at rest and in transit.
- TLS encryption is used to protect web communication sessions and data during transmission.
- Backups are encrypted.
- Non-production (development/testing) environments use de-identified or "dummy" data rather than production personal data

**4. Network and transmission security**

- Production infrastructure runs on a platform-as-a-service model that provides an effective firewall around all application containers; the only network ingress is via HTTPS connections to designated web front-end endpoints.
- A Virtual Private Cloud (VPC) protects the network perimeter and restricts inbound and outbound access.
- Perimeter protection systems are configured to deny unauthorised traffic from external sources.
- Web servers use TLS encryption for web communication sessions.

**5. Confidentiality — personnel and organisational measures**

- Employees and contractors are bound by confidentiality obligations. A confidentiality statement forms part of the employee handbook, and new hires sign confidentiality and handbook acknowledgements on their first day of employment.
- The Processor maintains a process for background and/or reference checks as a condition of employment, as permitted by local law.
- All employees are required to accept a documented Code of Conduct; a documented employee sanction procedure applies for non-compliance with the handbook, Code of Conduct, or security policy.
- Security awareness training is completed by employees at least annually.
- Information system security and management policies are formally documented, communicated, and reviewed at least annually.
- Appointment of a Data Protection Officer

**6. Integrity — change and development management**

- The Processor maintains documented Systems Development Life Cycle (SDLC) and change-management policies and procedures.
- Change requests are submitted via a Change Request form and tracked in a ticketing system; management approval is obtained and documented before migration to production.
- Development and testing are performed in environments logically separated from the production environment.
- Segregation of duties is enforced: authorisation, development, testing, and implementation are segmented functions.
- Version control software maintains a history of code changes, supports rollback, and tracks changes to individual developers.

**7. Availability and resilience**

- Customer data is backed up and monitored by the Engineering team for completion and exceptions; on exception, the root cause is identified and the backup re-run.
- The environment is continuously monitored for security events, latency, and network and server performance (via AWS); capacity monitoring is performed against defined utilisation thresholds.
- The platform-as-a-service provider automatically replaces any failed application container, whether the failure is in the application or the underlying hardware.
- The Processor maintains a documented business continuity plan and disaster recovery plan.
- The Processor maintains a documented incident response plan and data-breach procedures, including notification procedures. IT Operations personnel review identified security events to

determine impact and recommend remediation, and recovery plans are in place to restore systems following incidents or outages.

**8. Vulnerability management, monitoring and testing**

- An Intrusion Detection System (AWS GuardDuty or equivalent) alerts personnel to unauthorised modifications of critical system files, configuration files, and content files.
- Automated vulnerability scanning is performed on a continuous basis using AWS Inspector and GitHub Dependabot across software libraries and running environments, with output reviewed as part of each development cycle.
- Critical vulnerabilities are remediated in a timely manner.
- A BYOD and workstation security policy requires active anti-malware software on all devices accessing company systems and production resources, and compliance with endpoint security requirements is verified periodically.

**9. Data retention and secure disposal**

- Media handling and disposal procedures ensure that data and software are rendered unrecoverable before an asset controlled by the Processor is retired.
- Electronic media containing confidential information is purged or destroyed in accordance with best practice, with a certificate of destruction issued for each device destroyed. (Disposal of hosting media is performed by AWS as sub-processor.)

**10. Sub-processor and vendor management**

- A vendor management process is in place and requires a signed contract for each vendor, addressing (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels where applicable.
- Management reviews the annual SOC 2 (or SOC 1) report of its hosting provider to confirm that outsourced controls are appropriately designed and operating effectively.
- Sub-processor controls are monitored through reconciliation of output reports, periodic discussions, review of attestation reports, and monitoring of relevant external communications.

**11. Testing and evaluation of effectiveness**

- The Processor performs continuous control-activity monitoring through a GRC platform (Vanta) and/or manual control testing.
- An internal control review is conducted at least annually, and control owners perform an annual self-evaluation of control effectiveness.
- A risk assessment is maintained in a risk register, with risks rated by likelihood and impact and assigned mitigation strategies; the register is reviewed at least annually.
- The effectiveness of the Measures is independently evaluated through periodic SOC 2 examination against the Security trust services criteria.

# APPENDIX 7: USE OF PERSONAL DATA IN AI SYSTEMS

This Appendix 7 of the DPA applies whenever the Supplier processes personal data that is or may be utilized in AI Systems. It remains applicable whether the AI System operates independently or as part of a Service. This Appendix 7 applies regardless of whether the AI System constitutes the Service provided by the Supplier or serves as a functionality/feature within the Services offered by the Supplier to the Controller. Nothing in this Appendix 7 shall limit the Supplier's obligations under the DPA.

**DEFINITIONS**

For the purposes of this Appendix 7, and unless otherwise specified in the DPA, the following terms shall have the meanings set forth below:

a) **AI System** shall mean a machine-based system that can operate autonomously and adapt after deployment that is used for generating outputs like predictions or decisions, whereby this includes artificial intelligence models that are trained on broad data sets or systems that are powered by such machine-based systems or models.
b) **AI Laws** means Regulation (EU) 2024/1689 (the "AI Act") and any similar regulation, directive, or binding law that is applicable to the Services and AI Systems of the Supplier and governs the development, provision or offering of AI Systems.
c) **Input** means any data, information, or content provided to the AI System for processing, analysis, or learning.
d) **Output** means the results, predictions, recommendations, or decisions generated by the AI System in response to provided Inputs.
e) **Adverse Impact** means the adverse impact that an unfair and/or biased Output may have on a Data Subject, including but not limited to biases, discrimination, or inconsistencies.

GENERAL CONDITIONS

2.1 The Supplier shall only use Personal Data in connection with an AI System if and to the extent it is strictly necessary for the provision of the Service.

2.2. The parties hereby agree, that unless explicitly agreed otherwise, the use of Personal Data for AI System training in relation to systems that belong to the Supplier does not require the Controller's prior approval if such data training can be achieved through the use of sufficient data protection measures such as:

a) Data Anonymization & De-identification
b) Differential Privacy
c) Federated Learning
d) Secure Multi-Party Computation (SMPC)
e) Homomorphic Encryption
f) Data Minimization & Purpose Limitation
g) Access Controls & Role-Based Access
h) Encryption in Transit & at Rest
i) Synthetic Data Generation

2.3. When conducting AI System training in relation to systems that belong to the Supplier, the Supplier shall integrate and/or use 3rd party models and/or systems/services that offer sufficient data protection measures, such as those listed in point 2.2. of this Appendix 7.

2.4. Where the Supplier processes Personal Data in connection with AI Systems that belong to the Supplier, the supplier shall:

a) adhere to all applicable Data Protection Laws and AI Laws.
b) treat all Input and Output data as Personal Data, when such data meets the criteria for Personal Data under applicable Data Protection Laws and AI laws,
c) develop, deploy and provide its AI Systems in adherence to the data minimisation principle, whereby the Supplier shall process only the minimum Personal Data necessary for providing the Services;
d) inform the Controller of any foreseeable adverse impacts the AI System may have on Data Subjects in accordance with applicable Data Protection Law and AI Law requirements;
e) Implement necessary technical and organizational safeguards, including privacy by design and default, pseudonymization, encryption, and cybersecurity protections in accordance with applicable Data Protection Law and AI Law requirements;
f) follow industry wide monitoring practices to prevent biases, discrimination, or other Adverse impacts.
g) Regularly train, test, and audit its AI Systems and promptly notify the Controller of any Adverse impacts, as per applicable Data Protection Law and AI Law requirements

2.5. If it is required under applicable Data Protection Laws or AI Laws, the Supplier shall draft and make available upon request to the Controller appropriate documentation on the purposes of Personal Data processing in connection with AI System training and testing, implemented anonymisation or pseudonymisation measures, storage and segregation information as well as other information that shall allow the Controller to make informed decisions and meet its legal obligations.

2.6. If it is required under applicable Data Protection Laws or AI Laws, the Supplier identifies known and potential Adverse Impact risks and takes appropriate actions to address, prevent, or minimize them. The Supplier shall also keep the Controller informed of such uncovered risks in a timely manner and notify the Controller about its mitigation efforts and their expected timelines

2.7. In cases where the Supplier identifies serious widespread Adverse Impact risks or where required under applicable Data Protection Laws or AI Laws, the Supplier shall suspend the development/provision of its affected AI Systems or the affected features of its Services until the risks are resolved or sufficiently mitigated, unless otherwise agreed in writing with the Controller.

—----------END OF DOCUMENT—----------