DATA PROCESSING AGREEMENT - EU/UK

PARTIES

1. **Customer** defined as the Customer in the Master Agreement, and
2. **Sumsub**, defined as the Service Provider in the Master Agreement.

BACKGROUND

a. The **Customer** and **Sumsub** entered into a Master Agreement that requires **Sumsub** to process Personal Data in relation to the subject matter of the Master Agreement.

b. This Data Processing Agreement (**DPA**) sets out the additional terms, requirements, and conditions on which **Sumsub** will process Personal Data when providing services under the Master Agreement. This DPA contains the mandatory clauses required by applicable Data Protection Legislation for contracts regarding data sharing and data processing activities.

AGREED TERMS

1. Definitions and interpretation

The definitions of the EU General Data Protection Regulation (GDPR), in particular Art. 4 EU GDPR, as well as those of the Master Agreement, apply to this DPA. In addition, the following definitions shall be applicable:

a. **Authorised Persons**: the persons or categories of persons that the Customer authorizes to give Sumsub Personal Data processing instructions pursuant to clause 2.1. (a).

b. **Applicant's information:** any information of Applicant, including Personal Data related to Applicant, tags of approval, rejection and resubmission, as well as log information.

c. **Business Purposes**: execution of the Master Agreement or any other purpose specifically defined by the Customer in Annex A.

d. **Data Subject**: an individual who is the subject of Personal Data, whose Personal Data is processed under this DPA (can be referred to as 'Applicant').

e. **Personal Data**: means any information relating to an identified or identifiable natural person which is processed as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable natural person is the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Data Subject).

f. **Processing, processes and process**: either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.

g. **Data Protection Legislation**: all applicable privacy and data protection laws, including but not limited to the **US Data Protection Legislation**, the EU General Data Protection Regulation (*(EU) 2016/679*)(‘**EU GDPR**’) and the UK General Data Protection Regulation (‘**UK GDPR’**) and the Data Protection Act 2018; any applicable national implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

h. **Personal Data Breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

i. **Sumsub Ecosystem**: an interaction model in which Sumsub customers are involved and integrated for data sharing activities required for provision of specific Services acquired pursuant to the Price List and/or any relevant supplemental agreement, provided that the Parties enter necessary legal arrangements and adhere to the allocation of respective rights and obligations.

j. **Travel Rule**: a requirement imposed by Financial Action Task Force (FATF) in Recommendation 16 and applicable national AML/CFT laws in relation to Virtual Assets Service Provider(s) (VASP) obligation to obtain, hold and exchange certain information regarding originator and beneficiary during virtual assets transfer.

k. **US Data Protection Legislation**: those laws, rules, and regulations of the United States of America relating to privacy, security, or data protection, including, as applicable, the California Consumer Privacy Act (‘**CCPA’**) and its replacement, the California Privacy Rights Act (‘**CPRA’**), the Virginia Consumer Data Protection Act (‘**VCDPA’**), the Colorado Privacy Act (‘**CPA’**), the Utah Consumer Privacy Act (‘**UCPA’**), the Illinois Biometric Information Privacy Act (‘**BIPA’**), the Washington’s Biometric Identifiers Law (‘**H.B. 1493’**), Texas Capture or Use of Biometric Identifier Act (‘**CUBI’**) and other laws that may apply to the processing of personal data under the Master Agreement and this DPA.

1.2 This DPA is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this DPA.

1.3. Any Annexes to this DPA form a part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes Annexes.

The DPA includes the following Annexes:

Annex A: Data Processing Instruction

Annex B: Consent and Privacy notice Wording

Annex C: Technical and organisational measures description

Annexes D - 1, D - 2, D - 3: Standard Contractual Clauses and Addendum

Annex E: List of Subprocessors

1.4. A reference to writing or written includes faxes, email and electronic messaging services, which the parties typically use to exchange information in order to execute the Master Agreement.

1.5. In the case of conflict or ambiguity between

a. any provision contained in the body of this DPA and any provision contained in any Annex hereto, the provision in the body of this DPA will prevail;

b. any of the provisions of this DPA and the provisions of the Master Agreement (excluding the Cover Sheet), the provisions of this DPA will prevail.

2. Personal Data processing

2.1. The Customer and Sumsub acknowledge and agree that for the purpose of the Data Protection Legislation:

a. Sumsub processes Personal Data provided by the Customer in relation to the Customer’s use of Services as a processor. The Customer is a controller which determines the purposes and scope of processing and instructs Sumsub on how to process Personal Data. Specifically, the Customer will provide or make available to Sumsub, the specific purposes, duration and nature of such collection being described in Annex A. The Customer retains control of the Personal Data and remains responsible for compliance with its obligations under the applicable Data Protection Legislation and for the processing instructions it gives to Sumsub, while Sumsub will process Personal Data as described in this DPA or in the respective instructions and implement appropriate technical and organisational measures as set out in clause 5 of this DPA. Where applicable, Sumsub is responsible for storing the applicant’s information, including any Personal Data, tagged with the corresponding risk level by the Customer. In case the fraud suspicion or commitment is reasonably high, the Customer, pursuant to its purposes related to fraud prevention and/or avoidance, authorises Sumsub to assign a relevant risk score to the applicant's information. Where Sumsub acts as a Processor on the Customer’s behalf, the parties will also comply with the obligations set out in this DPA.

b. In some circumstances, Sumsub may process and aggregate some of the Personal Data provided by Customer with data received from other sources (including Data Providers and other customers) as an independent controller for the purposes of development and improvement of the Services, including means of artificial intelligence (e.g. machine-learning techniques), flagging potentially fraudulent patterns which could lead to or signal of any illicit activity, provision customers with calculated risk score information and information about the increased risk of fraud to assist Customers in determining whether the user is a genuine user or there is a potential risk of impersonation fraud, concealing a real identity etc. and log audit reports as applicable, provided that Sumsub’s processing purposes are compatible with the Customer’s. Sumsub warrants that such processing relates to preventing and detecting fraud and other illicit activity as part of substantial public interest, and the Customer hereby authorises such use, including profiling of Personal Data. Even after the Customer's relationship with Sumsub is terminated, Sumsub may retain the Personal Data and related inferences where it has a lawful basis for doing so, including for purposes of Sumsub's own legitimate interests of continuing to provide services for all Sumsub customers, complying with its legal obligations, resolving disputes, and enforcing its agreements and serving the (substantial) public interest. Where Sumsub acts as an independent controller, each party shall be individually responsible for its own processing of the Personal Data and compliance with Applicable Data Protection Legislation unless otherwise provided herein.

2.2. To the extent the Customer provides Personal Data related to the execution of the Master Agreement via Sumsub's website, dashboard, or other communication means (including in connection with any requests), Sumsub will process such Personal Data in accordance with Sumsub's privacy notice available at https://sumsub.com/privacy-notice/

2.3. Party shall notify the other Party of any request for the disclosure of Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency in accordance with clause 18 of this DPA.

3. Parties' obligations

3.1. Sumsub's obligations as the Processor:

a. Sumsub will only process the Personal Data to the extent and in such a manner as is necessary for the Business Purposes and this DPA. Sumsub will also process Personal Data in accordance with the Customer's written instructions from Authorised Persons, if applicable. Sumsub will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or Data Protection Legislation.

b. Sumsub must promptly comply with any of the Customer's requests or instructions from Authorised Persons requiring Sumsub to rectify, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing. Sumsub must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with Data Protection Legislation.

c. Sumsub will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this DPA generally authorises the disclosure or as required by law. If a law, court, regulator or supervisory authority requires Sumsub to process or disclose Personal Data, Sumsub must first inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement unless the law prohibits such notice.

d. Sumsub will reasonably assist the Customer with meeting the Customer's compliance obligations under Data Protection Legislation, taking into account the nature of Sumsub's processing and the information available to Sumsub, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

e. Regardless of the type of integration (Web SDK or API) the Customer applies and unless the Customer instructs otherwise, Sumsub will (i) assist the Customer in notifying Data Subjects that Sumsub's Services may involve processing of their biometric data and (ii) where applicable under Data Protection Legislation, require Data Subjects to consent to such processing before its commencement.

3.2. Customer's obligations as the Controller:

a. The Customer represents and warrants that it has taken all the required measures to ensure that Sumsub and its subprocessors may lawfully process the Personal Data in accordance with the applicable Data Protection Legislation. The Customer is independently responsible for complying with applicable Data Protection Legislation, including BIPA, providing all necessary disclosures and obtaining all required consents.

b. The Customer ensures that all required privacy notices have been given to all Data Subjects and/or, as may be applicable under the Data Protection Legislation, all necessary consents have been obtained from Data Subjects before their Personal Data is processed by Sumsub or its subprocessors. Such notices and consents must be sufficient in scope to enable each Party to process the Personal Data as envisaged under this Agreement and the Master Agreement and in accordance with the applicable Data Protection Legislation, including the transfer of such Personal Data to and by Sumsub (including by having provided all necessary notices and obtained all necessary consents allowing both Parties to process biometric data pursuant to applicable Data Protection Legislation and any other applicable national rules, laws, regulations, directives and governmental requirements concerning biometric data).

In particular, the Customer will ensure the Data Subjects are familiarised with the notice wording contained in Annex B and/or, as may be applicable under the Data Protection Legislation, obtain each Data Subject's consent to that wording before any Personal Data is provided to Sumsub.

When processing of Personal Data of a child, the Customer shall make reasonable efforts to assure that the holder of parental responsibility over the child has given consent for the Processing or authorised the Processing in another manner required under applicable Data Protection Legislation.

c. Upon redirection by Sumsub of requests made by Data Subjects or the authorities empowered by the Applicable Data Protection Legislation, the Customer will respond to the requests concerning the processing of Personal Data conducted by Sumsub and controlled by the Customer or provide Sumsub with the relevant instruction on responding such a request. The communication details are provided in clause 18 of this DPA.

For requests made by the authorities empowered by the Applicable Data Protection Legislation the Parties shall use the notice contacts in accordance with clause 18 of this DPA. The Customer shall notify Sumsub of any inquiries by the supervisory authorities about Sumsub Service or Sumsub Processing of Personal Data.

4. Sumsub personnel

4.1. Sumsub will ensure that all of its personnel;

i. are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

ii. have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

iii. are aware both of Sumsub's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

4.2. Sumsub will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable law on all of Sumsub's personnel with access to the Personal Data.

5. Data Protection and Security

5.1. Sumsub must at all times implement appropriate technical and organisational measures (‘**TOMs**’) against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data.

The list of such measures is provided in Annex C.

5.2. Sumsub will keep detailed, accurate and up-to-date records on actions commited by the Customer and Sumsub personnel in order to ensure records of compliance with obligations under this DPA and Sumsub will provide the Customer with copies of the Records upon request.

6. Personal Data Breach

6.1. Sumsub will promptly and without undue delay notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. Sumsub will restore such Personal Data at its own expense.

6.2. Sumsub will immediately and without undue delay notify the Customer if it becomes aware of

a. any accidental, unauthorised or unlawful processing of the Personal Data; or
b. any Personal Data Breach.

6.3. Where Sumsub becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide the Customer with the following information:

i. description of the nature of (a) and/or (b), including the categories and an approximate number of both Data Subjects and Personal Data records concerned;

ii. the likely consequences; and

iii. description of the measures taken or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

6.4. Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will coordinate with each other to investigate the matter. Sumsub will reasonably cooperate with the Customer in the Customer's handling of the matter, including

i. assisting with any investigation;

ii. providing the Customer with physical access to any facilities and operations affected;

iii. facilitating interviews with Sumsub's employees, former employees and others involved in the matter;

iv. making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

v. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.5. Sumsub will not inform any third party of any Personal Data Breach without first obtaining the Customer's prior written consent, except when required to do so by law.

6.6. Sumsub agrees that the Customer has the sole right to determine:

i. whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

ii. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.7. Sumsub will cover all reasonable expenses associated with the performance of the obligations under clause 6.2 and clause 6.4 unless the matter arose from the Customer's specific instructions, negligence, wilful default or breach of this DPA, in which case the Customer will cover all reasonable expenses.

7. International transfers of personal data

7.1. Sumsub (or any subcontractor) shall not transfer or otherwise process Personal Data outside the European Economic Area (EEA) or the United Kingdom unless:

i. data recipients or third countries ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the Processing of Customer Personal Data as determined by the European Commission (EC) or the Information Commissioner’s Office (ICO);

ii. the transfer is based on the Binding Corporate Rules or Standard Contractual Clauses or another legally recognised transfer method.

Provided that an adequacy decision/regulation of the EC or the ICO is amended or withdrawn, resulting in the inability to rely on it as a data transfer mechanism by the Parties, such transfer shall be conducted as provided in clause 7.2.

7.2. If any Personal Data transfer between the Customer (as ‘data exporter’) and Sumsub (as ‘data importer’) requires the execution of the Standard Contractual Clauses (‘SCCs’) that are available here (https://eurlex.europa.eu) in order to comply with the Data Protection Legislation, the parties conclude SCCs as indicated in Annexes D-1, D-2 and D-3, accordingly, which shall be deemed incorporated into and form a part of this DPA, as follows:

In relation to transfers of Personal Data that is protected by the EU GDPR and processed per clause 2.1.(a) of this DPA, the SCCs shall apply, completed as follows:

i. Module Two or Module Three will apply (as applicable);

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in clause 8.1. of this DPA;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the SCCs will be governed by law of Ireland;

vi. in Clause 18(b), disputes shall be resolved before the courts of England and Wales;

vii. Annex I of the SCCs shall be deemed completed with the information set out in Annex D-1 to this DPA; and

viii. Subject to clause 6 of the SCCs, Annex II of the SCCs shall be deemed completed with the information set out in Annex C to this DPA;

In relation to transfers of Personal Data protected by the EU GDPR and processed per clause 2.1.(b) of this DPA, the SCCs shall apply, completed as follows:

i. Module One will apply;

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 11, the optional language will not apply;

iv. in Clause 17, Option 1 will apply, and the SCCs will be governed by law of Ireland;

v. in Clause 18(b), disputes shall be resolved before the courts of England and Wales;

vi. Annex I of the SCCs shall be deemed completed with the information set out in Annex D-2 to this DPA; and

vii. Subject to the language provided in clause6(i) of this DPA, Annex II of the SCCs shall be deemed completed with the information set out in Annex C to this DPA;

In relation to transfers of Personal Data protected by the UK GDPR, the SCCs, as implemented under sub-paragraphs (a) and (b) above, will apply with the following modifications:

i. the SCCs shall be deemed amended as specified by Part 2 of the UK Addendum;

ii. tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed respectively with the information set out in Annex D-3 of this DPA (as applicable); and

iii. table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

7.3. In cases where a third-party processor is involved in fulfilling the Master Agreement and processing Personal Data in accordance with this DPA, and such a third-party processor is located in a third country, the transfer of data from Sumsub to this third-party processor requires application of certain appropriate safeguards, such transfers will be subject to the appropriate safeguards specified in Article 46 EU GDPR and UK GDPR.

Where possible, such transfers should be made on the basis of Adequacy Decisions per Article 45 of the EU GDPR or Adequacy Regulations in accordance with Article 17A of the Data Protection Act 2018.

7.4. When the Customer transfers any Personal Data from the System or provides access to the System to any third party or recipient, including those located outside the EU/EEA/UK, the Customer is solely responsible for ensuring that such transfer is legal and is subject to the applicable protection regime and/or appropriate safeguards in accordance with applicable Data Protection Legislation.

8. Subprocessors

8.1. Sumsub may authorise a subprocessor to process the Personal Data, and it hereby represents and guarantees, subject to clauses 16 and 17, that:

a. Sumsub enters into a written contract with the subprocessor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures;

b. Sumsub maintains control over all Personal Data it entrusts to the subprocessor.

The Customer grants Sumsub general authorisation to engage any subprocessor by selecting a set of services for which this subprocessor needs to be involved when signing the Master Agreement. Sumsub will maintain the list of engaged subprocessors (Annex E), which will be updated in the Dashboard notifications and which the Customer shall read and review to receive the updated information. If the Customer objects to the engagement of the specified subprocessor and provides legitimate reasons for the objection, Sumsub, may (i) cease to use the new subprocessor with regard to Personal Data (if possible, to continue providing service without using a particular subprocessor, and it will not affect SLA and quality of service), (ii) taking into account the costs and state of the art, consider providing another subprocessor, or (iii) If it is impossible to provide another subprocessor or if the Customer objects to any subprocessor, Sumsub may cease to provide or the Customer may agree not to use (temporarily or permanently) the particular aspect of a Sumsub Service that would involve the use of the subprocessor to process Personal Data. Sumsub or the Customer may terminate this DPA in accordance with clause 11.4. hereto.

8.2. Where the subprocessor fails to fulfil its obligations under such a written agreement, Sumsub remains fully liable to the Customer for the subprocessor's performance of its agreement obligations.

8.3. The Parties consider Sumsub to control any Personal Data controlled by or in possession of its subprocessors.

9. Recipients

9.1. The parties agree that any transfer of Personal Data within the Sumsub Ecosystem from the Customer to a third party will be possible only if:

i. appropriate contractual obligations and other relevant obligations will be entered into between the Customer and the third party under applicable Data Protection Legislation; and

ii. the Customer will give written instructions to Sumsub for such a transfer by completing the relevant legal arrangement.

Without prejudice to the above, where the Customer receives the services under the Crypto Travel Rule Solution pursuant to the Price List or any supplement agreement conducted whereafter, the Customer ensures and guarantees the transferring of data within the Sumsub Ecosystem or to any third party chosen at Customer's own discretion be legal and adequate. The Customer solely settles the Sumsub Ecosystem and/or any transfers to a particular third party in accordance with the applicable Travel Rule. The Customer agrees that the personal data transferred following this paragraph will be defined and limited by the Customer at the time of transfer, and the Customer agrees to be fully responsible for any non-compliance and breach of applicable Data Protection Legislation related to and affects Sumsub data processing activity.

10. Complaints, data subject requests and third-party rights

10.1. Sumsub must, at no additional cost, take such technical and organisational measures as may be appropriate and promptly provide such information to the Customer as the Customer may reasonably require to enable the Customer to comply with:

i. the rights of Data Subjects under the Data Protection Legislation, including subject access and portability rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

ii. information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.

10.2. Sumsub must notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation. The communication details are indicated in clause 18 of this DPA.

10.3. Sumsub must notify the Customer within 10 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

10.4. Sumsub will give the Customer its full cooperation and assistance in responding to any complaint, notice, communication or Data Subject request.

10.5. Sumsub must not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this DPA or as required by law.

11. Term and termination

11.1. This DPA will remain in full force and effect so long as the Master Agreement remains in effect.

11.2. Any provision of this DPA that expressly should come into or continue in force on or after the termination of the Master Agreement in order to protect Personal Data will remain in full force and effect.

11.3. Sumsub's failure to comply with the terms of this DPA is a material breach of the Master Agreement. In such an event, the Customer may terminate any part of the Master Agreement authorising the processing of Personal Data effective immediately on written notice to Sumsub without further liability or obligation.

11.4. If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 2 (two) months, they may terminate the Master Agreement on written notice to the other party. By accepting this DPA, the Customer agrees that the termination is the sole remedy in such a situation.

12. Data return and destruction

12.1. At the Customer's request, Sumsub will give the Customer a copy of or access to all or part of the Customer's Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

12.2. Sumsub will cease any processing and delete and/or return if directed in writing by the Customer, all or any Personal Data related to this DPA upon (i) instruction from the Customer in connection with the Services or (ii) written request of the Customer in connection with the termination of the Master Agreement for any reason or expiry of its term.

This clause does not apply to the processing of Personal Data carried out in accordance with clause 2.1.(b).

12.3. If any law, regulation, or government or regulatory body requires Sumsub to retain any documents or materials that Sumsub would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

12.4. Where the Customer has instructed that any Personal Data be deleted, Sumsub will certify in writing that it has destroyed the Personal Data within 30 days after it completes the destruction.

13. Review

13.1. The Customer and Sumsub must review the information listed in Annex A to this DPA once a year or earlier subject to mutual consent to confirm its current accuracy and update it when required to reflect current practices.

14. Audit

14.1. Sumsub shall, in accordance with Data Protection Legislation, make available to the Customer any information as is reasonably necessary to demonstrate Sumsub's compliance with its obligations as a data processor under the Data Protection Legislation and allow for and contribute to audits, including inspections, by the Customer, subject to the Customer:

i. giving Sumsub 30-day prior notice of such information request, audit and/or inspection being required;

ii. ensuring that all information obtained or generated in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to a supervisory authority or as otherwise required by applicable law);

iii. ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to Sumsub's business, a subprocessors' business and the business of other customers of Sumsub; and

iv. paying Sumsub's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

14.2. Clause 14.1. shall be ensured as follows:

i. remote electronic access to, and copies of the Records and any other relevant information held at Sumsub's premises or on systems storing Personal Data;

ii. access to any of Sumsub's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

iii. remote inspection of all relevant documentation and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

14.3. At least once a year, Sumsub will conduct audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this DPA, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

14.4. Sumsub will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by Sumsub's management.

15. Breach Notification

15.1. If a Personal Data Breach occurs or is occurring, or Sumsub becomes aware of a breach of any of its obligations under this DPA or any Data Protection Legislation, Sumsub will:

i. promptly conduct its own audit to determine the cause;

ii. produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

iii. provide the Customer with a copy of the written audit report; and

iv. promptly remedy any deficiencies identified by the audit.

16. Warranties

16.1. Sumsub warrants and represents that:

a. its employees, subcontractors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation relating to the Personal Data;

b. it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

c. it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

d. considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

i. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

ii. the nature of the Personal Data protected; and

iii. comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

16.2. The Customer warrants and represents that Sumsub's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

17. Indemnification

17.1.The Customer shall defend, indemnify, and hold (i) Sumsub, its affiliates, successors, assigns, and (ii) the directors, officers, agents, and personnel of any person listed in subclause 17.1(i) harmless from and against any and all claims, causes of actions, suits and proceedings brought by any third party and any resulting judgments, settlements, liabilities, damages, losses, costs and expenses (including, without limitation, all attorneys' fees and legal costs) arising out of or incurred in connection with the Customer’s breach (including for the avoidance of doubt any alleged breach) or non-performance of any of its obligations under clause 3.2 hereof. For clarity, any limitations of liability as may be set out in the Master Agreement shall not apply to this clause 17.1.

18. Notice and the DPO

18.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to: privacy@sumsub.com.

18.2. Clause 18.1. does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

Annex A

Data Processing Instruction

The Customer's Purpose of Processing: CDD and AML/CFT rules compliance for KYC, if applicable

Business Purpose: Execution of the Master Agreement

Nature of Processing: Remote identity verification and other CDD procedures

Duration of Processing: Term of the Master Agreement or any other term indicated in line with clause 12 of this DPA

Data subjects categories: the Customer's customers

Categories of data for Processing: The Personal Data processing is based on the products or services selected in the Price List, which may include, but are not limited to the categories of Personal Data specified below.

For clarity, geolocation data (e.g. IP address) and technical data (e.g. (software and hardware attributes (camera and device name)) are strictly necessary to the extension of detection of fraud patterns as well as provision the correct risk score to the Customer.

KYC (A-Z)

- *For Address verification:* General Personal Data (full name, gender, personal identification code or number, date of birth, legal capacity, nationality and citizenship), ID document data (document type, issuing country, ID number, expiry date, MRZ, information embedded into document barcodes (may vary depending on the document), security features); PoA document data; Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from Data Subject’s device).

- *For AML Screening:* General Personal Data (full name, gender, personal identification code or number, date of birth, legal capacity, nationality and citizenship), ID document data (document type, issuing country, ID number, expiry date, MRZ, information embedded into document barcodes (may vary depending on the document), security features); Relevant publicly available data (information regarding a person being a Politically Exposed Person (PEP) or included in sanctions lists); Technical data (software and hardware attributes (camera and devise name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from the Data Subject’s device);

- *For Bank Card extraction and sensitive data masking*: General Personal Data (full name, gender, personal identification code or number, date of birth, legal capacity, nationality and citizenship); Banking details (card holder name, expiry date, first 6 and last 4 digits of the card number); Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from the Data Subject’s device.

- *For Biometric Checks (Liveness & Face Match):* Facial Image data (photos of face including selfie images and photo or scan of face on the ID document), Biometric data (numeric facial features); Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from the Data Subject's device.

- *For Biometric Checks (Selfie image & Face Match):* Facial Image data (selfie images and photo or scan of face on the ID document); Biometric data (numeric facial features); Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from Data Subject's device.

- *For Biometric Checks (Video selfie & Face Match):* Facial Image data (video-selfie (recording of short video with person saying 3 numbers transmitted to the screen of device used) and photo or scan of face on the ID document); Biometric data (numeric facial features); Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from the Data Subject's device.

- *For Crypto Travel Rule Solution:* Full name of the sender and the recipient, the physical (geographical) address of the sender, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth, recipient account number (e.g., wallet address); the legal name of counterparty VASP.

- *For Email verification:* Email address; Unique Identifier (Applicant ID).

- *For ID document verification*: General Personal Data (full name, gender, personal identification code or number, date of birth, legal capacity, nationality and citizenship); ID document data (document type, issuing country, ID number, expiry date, MRZ, information embedded into document barcodes (may vary depending on the document), security features); Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from the Data Subject's device).

- *For Phone verification:* Phone number; Unique Identifier (Applicant ID).

- *For Questionnaire:* Depends on the Customer's requirements

- *For Video Identification*: General Personal Data (full name, gender, personal identification code or number, date of birth, legal capacity, nationality and citizenship); ID document data (document type, issuing country, ID number, expiry date); Facial image data (video, sound recordings and screenshots of face); other Personal Data for AML/CFT purpose (activity profile, area of activity, purpose and nature of establishment of a business relationship, etc.); Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from the Data Subject's device).

KYB (A-Z)

- *For Intermediate Shareholder Check*: Corporate company documents, containing information about name, position, share owning of a particular person considered as shareholder.

- *For Ownership and Management Check*: Corporate company documents, containing information about name, position, share owning of particular person considered as a shareholder or a top manager.

<u>Extras (A-Z)</u>

- *For custom fields:* Additional information in the ID (depending on the country – personal identification number, tax ID, etc.);

- *For Face authentication:* Facial Image data (photos of face including selfie images and photo or scan of face on the ID); Biometric data (numeric facial features); Technical data (software and hardware attributes (camera and device name); Unique Identifier (Applicant ID); Geolocation data (IP address and domain name; general geographic location (e.g., city, country) from the Data Subject's device).

- *For Known Face Search (Additional to Biometrics Checks):* comparison of already provided facial image data.

- *For Phone Risk Scoring:* Phone number; Geolocation data (IP address); publicly available personal data (photo from the accounts in social media, etc.), Unique Identifier (Applicant ID).

- *For Email Risk Scoring:* Email address; Geolocation data (IP address); publicly available personal data (photo from the accounts in social media, etc.), Unique Identifier (Applicant ID).

- *For NIN verification for Nigeria:* NIN number data.

- *For Ongoing AML Screening:* AML Screening data set.

- *For Ongoing ID document verification:* ID document verification data set.

- *For SMS notification:* Phone number.

- *For Support:* Full name (name and surname); contact details (email address and/or phone number); Other information to mitigate the issue.

<u>KYT</u>

- *For Transaction monitoring*: Full name of the sender and the recipient, the address of the sender and the recipient, and the Unique identifier of the counterparties provided by Sumsub and the particular Customer.

Frequency of transfers in case of international transfers: on a continuous basis, in accordance with the Customer's purpose(s) and Business purpose.

Subject matter, nature and duration of the processing by (sub-) processor: The subject matter, nature and duration of the processing is indicated and specified in the relevant agreement with the subprocessor that Sumsub engages for Business purpose. More details is provided in Annex E.

Annex B

Consent and Privacy Notice Wording

The Customer shall ensure that, where applicable, it collects each Data Subject's consent allowing both Parties to process their biometric data as set out in this Agreement and the Master Agreement in accordance with the applicable Data Protection Legislation, in particular the US Data Protection Legislation, by complying with the below:

a. The following notice and consent language must be incorporated into the Customer's interface with respect to any individual using the Customer's services where Sumsub is integrated before redirecting any Data Subject to proceed with the onboarding:

"I hereby agree and express my voluntary, unequivocal and informed consent that personally identifiable information (PII) including biometric information will be processed for the purposes specified in this consent of the organisation for which I pass the identity verification process (hereinafter - the "Company") that uses Sumsub Group of Companies, (hereinafter - the "Service Provider" or "Sumsub") through which the Company collects and processes my PII and the biometric information. Please refer to the Privacy Notice (https://sumsub.com/privacy-notice-service) for details about the identity and contact details of Sumsub.

Categories of biometric data

My biometric information, to the processing of which by the Company and by the Service Provider I hereby agree and express my voluntary, unequivocal and informed consent, includes facial features or facial scans.

I hereby acknowledge and agree that facial images of myself are processed to confirm the liveliness of my face and/or to confirm that a given identity document is presented by me, its legitimate owner.

Purposes of processing of biometric data

I hereby acknowledge and agree that processing shall be done for the purposes of the Company and may include matters of compliance with applicable AML/CFT, anti-fraud laws and regulations, age restrictions acts and/or other laws and regulations and/or the Company customer due diligence procedures in accordance with the laws governing the intended business relationship.

The processing of biometric data will also be carried out for other compatible purposes of the Service Provider acting as a separate business including service development, fraud and criminal activity prevention, as well as 'litigation hold' and statutory obligations of the Service Provider (for details please see the Privacy Notice available here: https://sumsub.com/privacy-notice-service).

How will the biometric data be processed

I hereby acknowledge and agree that Company and Service Provider shall process my biometric information by means of automated reading, verification of the authenticity and other automated processing as stated in the Privacy Notice available at https://sumsub.com/privacy-notice-service/, which includes the processing of facial scan while passing liveness, video-selfie or video identification process, biometric authorisation, face comparison from the photo of an identity document and the facial image, searching of multiple identity creation, work and development of fraud control network to detect and prevent fraud and criminal activity.

The PII including biometric data may be disclosed to entities associated with Service Provider to achieve the purpose of the processing under this Consent. The Service Provider stores biometric information in AWS Amazon or Google Cloud (depending on the requirements of the Company on the place of data storage).

Retention of biometric data

I hereby represent that I have been informed that my PII will be retained and stored by Company and Service Provider and will be permanently destroyed based on the Company’s instructions when the Company’s initial purpose and/or retention period prescribed by applicable law expires. Where Service Provider independently defines the compatible purposes or under the legal obligation, the personal data, including biometric information, will be destroyed after Service Provider’s purposes for collecting the biometric information have been satisfied (and one (1) year of the date the purpose for collecting the data expires for residents of Texas) or after five (5) years from the provision of data to the Service Provider system, whichever occurs first. For the residents of Illinois, the retention period of personal data, including biometric information, will be three (3) years from the date of data provision to the Service Provider system. Please check how your PII will be deleted and destroyed in Service Provider’s Data Disposal and Destruction Policy at https://sumsub.com/privacy-notice-service/?id=#8.

I hereby represent that I have carefully read all of the above provisions and do voluntarily and unequivocally agree with them.”

b. The consent and privacy notice must include hyperlinks to Sumsub’s privacy notice available here: https://sumsub.com/privacy-notice-service/

c. Notwithstanding the above, the Customer will incorporate other necessary terms, notices, documents or consents (if applicable) into its own policies and legal agreements with Data Subjects which meet the requirements applicable to the Customer under Data Protection Legislation describing in particular:

- the processing of Personal Data, including biometric data while capturing face,

- the purposes for which Personal Data, including biometric data, are processed,

- the use of third-party service providers to perform this service aimed to perform identity verification on the Customer’s behalf, other matters required by the applicable Data Protection legislation, including as to storage, retention periods, third-countries transfers, etc.

d. Adoption of API consent parameter (privacy_notices_read_consent_given): where API integration is used under the Master Agreement, the Customer must additionally implement the following API consent parameter in respect of use of the Services: Sumsub privacy_notices_read_consent_given and/or other parameters, provided that they should enable Sumsub to log and verify whether the measures listed in this Annex B were implemented by the Customer in respect of that Data Subject.

Annex C

Minimum technical and organisational measures description

These measures refer to Sumsub group of companies (further - “Sumsub”) and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) and the United Kingdom (the UK) or processing the Personal Data of data subjects within EEA and the UK.

1. Definitions

1.1. (Personal) Data Protection Framework (also - Data Protection Framework) – a formal structure for managing personal data protection;

1.2. EU GDPR – EU General Data Protection Regulation;

1.3. UK GDPR – UK General Data Protection Regulation;

1.4. Applicable laws – the EU GDPR or the UK GDPR, or any other data protection legislation that directly applies to the Sumsub processing activities;

1.5. Sumsub group of companies – affiliates and the companies included in the group, for rendering remote identity verification services, compliance with applicable laws and improving the quality of such services.

2. Applicable standards and controls

Sumsub adheres to the principles of integrity, availability and confidentiality of the information (and Personal Data as its integral part) it processes in line with international industry standards and applicable law requirements.

2.1. Standards and normative requirements

Sumsub management is maintained in accordance with the lead industry standards (e.g., the ISO 27001 and/or SOC 2 Type 2) for the establishment, implementation, and control of the Information Security Management System (ISMS). Sumsub has established the organisational structure to ensure the effectiveness of the Data protection framework. Since Sumsub's business activities are worldwide oriented, Sumsub documents the regulatory obligations in the Data protection framework.

To maintain the ISMS and the Data protection framework, Sumsub implements policies, processes, enforcement measures and controls governing all storage/processing/transmitting of Personal Data, designed to

a. secure Personal Data against accidental or unlawful loss, access or disclosure;

b. identify reasonably foreseeable risks to security and authorized access to personal data; and

c. minimise security risks, including through risk assessment and regular testing.

Sumsub actively follows information security trends and developments as well as legal developments with regards to the services provided and especially with regards to Personal Data and uses such insights to maintain its ISMS and Data protection framework, taking into account privacy by design and by default.

To the extent of processing of cardholder or payment data (such as payment or credit cards), Sumsub will maintain its ISMS in accordance with the PCI DSS standard, augmented to cover Personal Data or other alternative standards that are substantially equivalent to PCI DSS for the establishment, implementation, and control of its ISMS. Additionally, Sumsub will be assessed against PCI DSS annually by an on-site inspection carried out by an independent party.

Sumsub implements the principles of documentation and formalization with subsequent unification of data processing procedures in terms of access control, segregation of duties (SoD) and mindful attitude to the personal data.

2.2. Management involvement

The Data protection framework is provided by the company management, defining the data protection goals and this Description implementation and control.

2.3. Register of assets and data flow

Assets containing any information are documented and evaluated in the ISMS Register of Assets. Personal data is an integral part of such information.

Sumsub documents its data flows by maintaining and updating the Register of Processing Activities and Mapping (RoPA) and reviews it at least annually or in case of an internal policy change. The information in RoPA demonstrates how data is processed and transferred, who it is disclosed to and whether it is secured.

2.4. Risk-based approach

Based on assets, the risks regarding information handling are assessed and registered. The risk assessment and treatment process is based on ISO 27005.

The risk assessment and risks mitigations procedures, including those related to a data protection impact assessment (DPIA) and a transfer impact assessment (TIA) is conducted at least annually.

2.5. International data transfer

The international data transfers are registered and subject to analysis. The international data transfer process complies with the applicable laws. As such, Sumsub relies on the EU adequacy decision (or UK adequacy regulations), the Standard Contractual Clauses (SCCs) and derogations under Article 49 of the EU GDPR and the UK GDPR; and Binding Corporate Rules or other safeguards defined in Article 46 of the EU GDPR or the UK GDPR as applied by Sumsub suppliers.

Sumsub prevents and does not conduct any restricted international data transfers.

3. Organisational and technical measures description

3.1. Maintain Policies and Procedures

Sumsub's ISMS is based on its policies that are regularly reviewed and maintained, and disseminated to all relevant parties, including all personnel. The policies and derived procedures clearly define information security responsibilities, including responsibilities for

- Maintaining policies and procedures,
- Secure development, operation and maintenance of software and systems,
- Security alert handling,
- Security incident response and escalation procedures,
- User account administration,
- Monitoring and control of all systems as well as access to personal data;
- Ensuring data subject rights' execution;
- Risk management and mitigation planning.

3.2. Data retention and encryption

The Personal Data is stored to a minimum and for a specific period in line with the Controller's instructions. The default infrastructure for data storage is AWS Amazon (Frankfurt am Main, Germany).

Sumsub uses strong encryption for personal data. As such, Sumsub has documented and implemented all necessary procedures to protect (cryptographic) keys used to secure stored Personal Data against disclosure and misuse. The Encryption Key is stored separately from other data and is by default located in Germany (Frankfurt am Main). All transmission of Personal Data across open, public networks is encrypted using strong cryptography and security protocols.

Personal information is encrypted using AES--256 at rest and HTTPS, TLS 1.2/1.3 in transit.

The Company implements data retention and disposal policies to limit data storage to that which is necessary, in accordance with the needs of the Controller.

3.3. Secure Networks and Systems

Sumsub has installed and maintains a firewall configuration to protect Personal Data that controls all traffic allowed between Sumsub's (internal) network and untrusted (external) networks, as well as traffic into and out of more sensitive elements of its internal network. This includes current documentation, change control and regular reviews.

Sumsub uses vendor-supplied defaults for system passwords and other security parameters on any systems if these are consistent with industry-accepted system hardening standards.

The firewalls are used to protect Sumsub's internet connection. This is the first line of defence against an intrusion from the Internet. The firewalls security rules on all layers are as follows:

- VPC,
- load balancing,
- instances,
- operating system (firewall rules via iptables),
- application.

3.4. Anti-malware protection

Anti-virus products that Sumsub employs regularly scan the network to prevent or detect threats include both internal and external vulnerability scanning and application scanning. Quarterly external scans and annual penetration tests are conducted by external qualified, credentialed, and industry recognised organisations. Sumsub will remedy vulnerabilities identified during scans and penetration tests in a commercially reasonable manner and time frame based on severity. Information systems and file transfer operations have effective and operational anti-virus software. All anti-virus software is configured for deployment and automatic updates. Anti-virus software is integrated with processes and will automatically generate alerts if potentially harmful code is dedicated for their investigation and analysis.

3.5. Implementation of Access Control Measures

3.5.1. Sumsub personnel access

Sumsub Systems means Sumsub's data centre facilities, servers, networking equipment, and host software systems (e.g. virtual firewalls) as employed by Sumsub to process Personal Data.

Sumsub Systems will be accessible to personnel as necessary to provide the services Sumsub offers. The access controls and policies are maintained to manage Sumsub Systems access ports in relation to any network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls.

Sumsub restricts access to Personal Data to businesses' need to know to ensure that critical data can only be accessed by authorised personnel. This is achieved by:

- Limiting access to system components and Personal Data to only those individuals whose job requires such access and
- Establishing and maintaining an access control system for system components that restricts access based on a user's need to know, with a default least privilege principle.

Sumsub implements 2FA or MFA for access to Sumsub Systems. Authentication policies and procedures are communicated to all users and groups.

3.5.2. Customer's access

Access control to Personal Data and services is implemented, and provision of access to the Customer's system to users and sources the Customer trusts in correspondence with the access restriction principle the Customer adheres to. Supplementary details of how access to your system is controlled:

- Service Auditing,
- File Auditing,
- Integrated security information management solution (on Linux): 389 Directory Server, MIT Kerberos, Dogtag certificate system, SSSD.

3.6. Restriction of Access to Personal Data

3.6.1. Virtual access

Access restriction is provided when there is no necessity to Processing Personal Data. Revocation of access is carried out automatically on personal dismissal through the electronic system. The Customer users' access will be restricted by the Customer via technical tools Sumsub provides in the Dashboard.

Access provision and restriction are also limited by the use of Sumsub's personal VPN connection. Some systems containing confidential (and highly confidential, if applicable) data are protected from unauthorised access due to VPN connection restrictions.

3.6.2. Physical access

Any physical access to Personal Data or Sumsub Systems that host Personal Data are appropriately restricted using entry controls and procedures to distinguish between onsite personnel and visitors. Access to sensitive areas is controlled and includes processes for authorisation based on job function and access revocation for personnel and visitors.

Media and backups are secured, and (internal and external) distribution is strictly controlled. Media containing Personal Data no longer needed for business or legal reasons is rendered unrecoverable or physically destroyed.

3.7. Log Management

All events happening in the Sumsub Systems are tracked and monitored using centralised logging mechanisms that allow thorough tracking of the following information:

- the system configuration changes;
- integration to the system activities;
- adding and deleting a user;
- approval of the applications and other automated requests within the system.

The audit trails are secured and protected, including file-integrity monitoring to prevent a change of existing log data and/or generate alerts. When alerting or in case of any problem, an analysis is conducted. Audit trails for critical systems are kept termless.

All Sumsub Systems are synchronised by implementing Network Time Protocol (NTP) or a similar capability.

3.8. Physical Security

3.8.1. Physical Access Controls

Physical components of Sumsub infrastructure are kept in office facilities ("Facilities"). Physical controls are used to prevent unauthorised entrance to Facilities both at the perimeter and at building access points. Depending on the office, passage through physical barriers at the Facilities requires either electronic access control validation (card access systems, etc.) or validation by human security personnel (a responsible staff member). Personnel are assigned full name badges that must be worn while the personnel is at any of the Facilities. Visitors are required to sign in with designated personnel, must show appropriate identification, are assigned a visitor badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by a responsible staff member while visiting the Facilities.

3.8.2. Limited Personnel Access

Sumsub provides access to the Facilities to those employees and contractors who have a legitimate job need for such access privileges. When an employee or contractor no longer has a job need for the access privileges assigned to them, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of the Sumsub.

3.8.3. Physical Security Protections

All access points are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Depending on the office, Sumsub also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities. All physical access to the Facilities by personnel is logged and routinely audited.

3.8.4. Continued Evaluation

Sumsub will conduct periodic reviews of the security of employed measures and their adequacy as measured against industry security standards and its policies and procedures. Sumsub will continuously evaluate the security of its Systems to determine whether additional or different security measures are required to respond to new security risks or findings generated during the periodic reviews.

3.9. Incident Management and Data Breach

Sumsub has implemented and maintains an incident response plan and prepared to respond immediately to an information security incident and data breach. Incident management includes

- Definition of roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of Customers;
- Specific incident response procedures;
- Analysis of legal requirements for reporting compromises;
- Coverage of all critical system components;
- Regular review and testing of the plan;
- Incident management personnel that is available 24/7;
- Training of staff;
- Inclusion of alerts from all security monitoring systems;
- Modification and evolution of the plan according to lessons learned and to incorporate industry developments.

Sumsub implements a business continuity process (BCP) and a disaster recovery process (DRP) that are maintained and regularly tested. An IT Service Continuity Plan is also prepared.

The process of responding to potential Personal Data breach situations is documented and the relevant notification templates for supervisory authority and concerned data subjects are prepared as well.

3.10. Backup and recovery

Personal Data is regularly backed up via snapshots (backup encrypted filesystem images). Regular backups of the most important Sumsub and Customer data will ensure it can be quickly restored in the event of disaster or ransomware infection.

Sumsub implements a number of recovery solutions designed to facilitate the quickest possible resumption of its critical functions. Examples of these include but are not limited to the use of alternative sites (relocation), remote access for staff members, evacuation, data backup, and Company Service provider mechanisms and procedures.

3.11. Supplier Management

The involvement of suppliers and subcontractors (also known as subprocessors) is carried out based on written legal arrangement with the specified rights and obligations, including the confidentiality and security of Personal Data and the use of a unified standard and implementation of the Customer Due Diligence and Data Protection Compliance assessment.

Sumsub documents the list of used suppliers depending on their function or role. The supplier management system is documented and monitored as well. An annual evaluation of each supplier is conducted, including the review of attestation reports (i.e. SOC 2, PCI, ISO) if available.

3.12. State of the art principle

Sumsub's software and devices are kept up-to-date via Operating System-Unattended Updates (Linux unattended-upgrades packages). Hardware and software need regular updates to fix bugs and security vulnerabilities.

3.13. Personnel and Privacy awareness

3.13.1. Newcomer awareness

Personnel undergo background checks prior to hiring. The newcomer is required to read the Introduction to Information Security Rules that includes privacy matters rules. Sumsub organises mandatory training/webinars regarding data protection and security for newcomers within the first 30 days where they are instructed on the rules of information security, whereof the protection of Personal Data is an integral part.

3.13.2. Further education process

In the further work process, personnel are also involved in different parts of training organised by Sumsub. For some specific topics or to optimize the way information is presented, Sumsub may supply ready-made solutions for training on privacy matters. It is highly welcomed for professional certification preparations for some personnel.

Sumsub uses Vanta to register internal data protection and information security training and keep track of those who miss mandatory training to encourage them to pass it.

The training schedule is drawn up in advance for a year, but there may be unplanned training if the need arises.

3.13.3. Privacy reminder

Sumsub implies 'privacy reminders' mechanisms by placing banners/signs on walls and other areas that employees can easily view. Banners/signs contain reminders of data privacy rules when performing everyday tasks of employees: email exchange, paper works, etc.

3.13.4. Administrative measures

Malicious behaviour must be prevented and shown unattractive. Sumsub informs its personnel of the negative consequences of non-compliance with internal policies and procedures. These consequences include personal responsibility (e.g. paying significant fines in line with Non-Disclosure Agreements).

Background checks are conducted to newcomers as permitted by local laws.

3.14. Assessment and Monitoring

Sumsub has implemented internal performance evaluation mechanisms of measures undertaken to protect Personal Data and will continue to implement them. The internal audits on EU GDPR and UK GDPR, ISO 27001, SOC 2 and other incoming standard certificates compliance are conducted.

Sumsub considers it necessary to conduct annual or, if applicable, one-time external evaluations of the effectiveness of measures to maintain a Personal Data protection framework. Internal staff perform internal penetration testing and vulnerability scanning on every significant production update using Burp Suite and other tools. Manual penetration testing also covers internet-facing infrastructure analysis, which includes: port scanning for unintended services and software composition analysis.

3.15. External Evaluation

Data protection framework external audits include compliance with the EU GDPR and the UK GDPR principles and requirements. Information security management system external audits (i.e. SOC 2 Type 2, PCI DSS, ISO standards). The other evaluations may include:

- Web application assessment of Sumsub's identity verification platform is provided annually;
- external ASV scanning is performed quarterly (in the framework of PCI DSS compliance measures).

Annex D-1

Description of Processing / Transfer

Modules 2 and 3 (controller/processor to processor transfers)

A. List of Parties

Data exporter(s)

Name: Party identified as ‘Customer’ in the DPA.

Address: as defined in the DPA.

Contact person’s name, position and contact details: As provided in clause 18 of the DPA.

Activities relevant to the data transferred under these Clauses: Provisioning data for the Business purpose.

Role: Controller/Processor

Data importer(s)

Name: Party identified as ‘Sumsub’ in the DPA.

Address: as defined in the DPA.

Contact person’s name, position and contact details: Sumsub’s DPO, email: privacy@sumsub.com

Activities relevant to the data transferred under these Clauses:

non-face-to-face customer identification, documents verification,

anti-money laundering customer screening (applies if it is indicated as a Service under the Master Agreement), and

other services related to customer identity verification according to the Master Agreement.

Role: Processor

B. Description of Transfer

As specified in Annex A of the DPA.

C. Competent Supervisory Authority

the competent supervisory authority will be determined in accordance with the criteria set forth in Clause 13 of the SCCs, provided that if the data exporter is not established in an EU Member State and has not appointed a representative, the Cyprus Supervisory Authority shall act as the competent supervisory authority.

ANNEX II

As specified in Annex C of the DPA.

ANNEX III

As specified in Annex E of the DPA.

Annex D-2

Description of Processing / Transfer

Module 1 (controller-to-controller transfers)

A. List of Parties

Data exporter(s)

Name: Party identified as ‘Customer’ in the DPA.

Address: as defined in the DPA.

Contact person’s name, position and contact details: As provided in clause 18 of the DPA.

Activities relevant to the data transferred under these Clauses: Provisioning data for the Business purpose.

Role: Controller

Data importer(s)

Name: Party identified as ‘Sumsub’ in the DPA.

Address: as defined in the DPA.

Contact person’s name, position and contact details: Sumsub’s DPO, email: privacy@sumsub.com

Activities relevant to the data transferred under these Clauses: Improvement of Services

Role: Controller

B. Description of Transfer

As specified in Annex A of the DPA.

C. Competent Supervisory Authority

the competent supervisory authority will be determined in accordance with the criteria set forth in Clause 13 of the SCCs, provided that if the data exporter is not established in an EU Member State and has not appointed a representative, the Cyprus Supervisory Authority shall act as the competent supervisory authority.

ANNEX II

As specified in Annex C of the DPA.

ANNEX III

As specified in Annex E of the DPA.

Annex D-3

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses - UK

PART 1. TABLE

Table 1. Parties

Commencement date: when the restricted transfer is to be conducted

The Parties' details:

Exporter: Customer

Importer: Sumsub

Key Contact: as specified in DPA

Table 2. Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs: The version of the Approved EU SCCs (stated in Annexes D-1 and D-2) to which this Addendum is appended, detailed below, including the Appendix Information.

Table 3. Appendix Information

ANNEX IA: List of Parties: As specified in the preamble of the SCCs (stated in Annex D-1 and/or Annex D-2).

ANNEX IB: Description of Transfer: As specified in Annex A to the DPA.

ANNEX II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As specified in Annex C to the DPA.

ANNEX III: List of Subprocessors: As specified in Annex E to the DPA.

Annex E

LIST OF SUBPROCESSORS

Please refer to Annex 1 of the Master Agreement.