Data Processing Agreement for Aproove Services
(“Data Processing Agreement ”)

1. SCOPE AND APPLICABILITY

1.1. This Data Processing Agreement applies to Aproove’s processing of Personal Data on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

1.2. The scope and duration, as well as the extent and nature of the collection, processing and use of Client Personal Data under this Data Processing Agreement shall be as defined in the Services Agreement. The term of this Data Processing Agreement corresponds to the duration of the Services Agreement.

1.3. The parties acknowledge that GDPR will apply to the processing of Client Personal Data if, for example, the processing is carried out in the context of the activities of an establishment of Clients in the territory of the EU. The parties further agree that U.S. Data Protection Laws, including the CCPA, may also apply to the processing of Client Personal Data. Unless expressly stated in this Data Processing Agreement, this Data Processing Agreement will apply irrespective of whether GDPR or U.S. Data Protection Law applies to the processing of Client Personal Data.

2. DEFINITIONS

The terms below shall have the following meanings:

“Aproove” means the Aproove Affiliate that has executed the Services Agreement.

“Aproove Affiliate(s)” means the affiliated company(ies) of the Aproove group as listed in Annex 3.

“CCPA” means the California Consumer Privacy Act, as may be amended from time to time, and any rules or regulations implementing the foregoing.

“Client”, “you”, “your” means the individual or entity that has executed the Services Agreement.

"Client Personal Data" means the personal data processed by Aproove on your behalf in the course of providing the Services to you.

“**Controller**” means the entity which determines the purposes and means of the processing of Personal Data as defined in the Data Protection Law, including as applicable any "business' as defined under the CCPA.

"**data processor**", "**data subject**", "**personal data**", "**processing**" "**subprocessor**" and "**appropriate technical and organisational measures”** as used in this Data Processing Agreement shall have the meanings given in the GDPR irrespective of whether GDPR or U.S. Data Protection Law applies.

"**Data Protection Law**" means the GDPR, the applicable U.S. Data Protection Law, the Swiss Federal Act of 19 June 1992 on Data Protection, as amended and the UK Data Protection Act 2018, that are applicable to the processing of Client Personal Data under this Data Processing Agreement.

“End Users” means an individual you permit or invite to use the Services. For the avoidance of doubt: (a) individuals invited by your End Users, (b) individuals under managed accounts, and (c) individuals interacting

with a Service as your customers, suppliers or other third parties are also considered End Users.

"Europe" means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Lichtenstein and Norway; (ii) Switzerland and (iii) the UK after it withdraws from the EU.

"**GDPR**" means the 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),as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement;.

"Personal Data Breach" means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Aproove systems or the Services environment that compromises the security, confidentiality or integrity of such Personal Data.

"**Processor**" means the entity which Processes Client Personal Data on behalf of the Controller means, collectively, both the Cloud Services and Professional Services, including as applicable any "service provider" as defined by the CCPA.

"Services" means our means, collectively, both the Cloud Services and Professional Services provided to you under the Services Agreement.

"**Services Agreement**" means (i) the applicable order for the Services you have purchased from Aproove; (ii) the applicable cloud services agreement referenced in the applicable Order Form, and (iii) the Service Specifications.

"U.S. Data Protection Law" means data protection or privacy laws applicable to Client Personal Data in force within the United States, including the CCPA.

Other capitalized terms have the definitions provided for them in the Services Agreement.

3. PROCESSING OF PERSONAL DATA

3.1. The provisions of this Section 3 shall apply where Data Protection Law applies to your processing of Client Personal Data and where we process that Client Personal Data as a data processor in the course of providing you the Services. If U.S. Data Protection Law applies to either party's processing of Client Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Client Personal Data.

3.2. The subject-matter of the data processing is providing the Services and the processing will be carried out until we cease to provide any Services to you. Annex 1 of this Data Processing Agreement sets out the nature and purpose of the processing, the types of Client Personal Data we process and the data subjects whose Client Personal Data is processed.

3.3. You are responsible for ensuring that the processing of personal data takes place in compliance with Data Protection Law and this Data Processing Agreement. You have the right and obligation to make decisions about the purposes and means of the processing of personal data. You shall be responsible, among other, for ensuring that the processing of personal data, which we are instructed to perform, has a legal basis.

Aproove provides a HIPAA-, SOC 2-, and ISO 27001:2022-compliant environment designed to support our clients in meeting their own regulatory compliance requirements. Aproove processes personal data solely in accordance with documented instructions from you. However, Aproove is not responsible for the content,

quality, or legality of the data you or your End Users input, upload, or process within our service. Responsibility for managing and safeguarding the data inputted by you remains solely with you.

While our compliance with HIPAA, SOC 2, and ISO 27001:2022 covers the technical and procedural measures within our platform to ensure a secure and compliant data processing environment, it does not extend to your data handling practices outside our platform. You are solely responsible for the accuracy, legality, and appropriateness of data shared or processed within our platform and must ensure their use of our services aligns with any regulatory obligations applicable to your business.

To maintain data security and compliance within Aproove's services, you should take appropriate steps to ensure that all data you input complies with applicable laws, regulations, and best practices. You must also manage access controls, restrict data sharing, and regularly review data practices to ensure compliance within your scope of responsibility. Aproove remains committed to supporting these efforts through ongoing updates to our security controls and compliance measures as per industry standards.

Aproove will process any Personally Identifiable Information (PII) or Data Disclosure requests related to our own Marketing, HR, Finance, and Aproove Software operations. However, any data uploaded, stored, or processed on the Aproove platform by you remains out of scope for Aproove's responsibility. Such data is fully owned and managed by the Client who uploaded it, and Aproove serves as the data processor only in a technical capacity.

Clients retain full responsibility and ownership over all data they upload and are accountable for managing and responding to any regulatory requirements related to this data. This includes meeting any legal or compliance obligations, implementing necessary access controls, and addressing data requests pertaining to the information they store within the Aproove platform.

3.4. When we process Client Personal Data in the course of providing Services to you, we will:

3.4.1. process the Client Personal Data only in accordance with documented instructions from you (as set forth in this Data Processing Agreement or the Services Agreement or as directed by you through the Services). If applicable law requires us to process the Client Personal Data for any other purpose, we will inform you of this requirement first, unless such law(s) prohibit this on important grounds of public interest;

3.4.2. notify you promptly if, in our opinion, an instruction for the processing of Client Personal Data given by you infringes applicable Data Protection Law;

3.4.3. assist you, taking into account the nature of the processing:

a) by appropriate technical and organizational measures and where possible, in fulfilling your obligations to respond to requests from data subjects exercising their rights;

b) in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the information available to us; and

c) by making available to you all information reasonably requested by you for the purpose of demonstrating that your obligations relating to the appointment of processors as set out in Article 28 of the GDPR have been met.

3.4.4. We will not provide access to or transfer any Client Personal Data to any third party for their independent use (e.g., purposes unrelated to the provision of the Services) without your prior written consent. By agreeing to this Data Processing Agreement, you consent to our use of Aproove affiliates and the third-party sub-processors listed in Annex 5 – "List of Approved Sub-processors" for the purposes described herein.

We reserve the right to update the list of approved sub-processors. In such cases, you will have 45 days to object by terminating the Services Agreement for convenience. To stay informed about updates, please refer to https://www.aproove.com/legals#tab3, where the most recent and active version of this Data Processing Agreement is maintained, including Annex 5.

When engaging sub-processors to process Client Personal Data, we remain responsible for their performance. Our agreements with these sub-processors will include terms that are at least as protective of your rights as those contained in this Agreement and as required by applicable Data Protection Law.

3.4.5. ensure that our personnel required to access the Client Personal Data are subject to a binding duty of confidentiality with regard to such Client Personal Data;

3.4.6. except as set forth in Section 3.3.5 above or in accordance with documented instructions from you (as set forth in this Data Processing Agreement or the Services Agreement or as directed by you through the Services), ensure that none of our personnel publish, disclose or divulge any Client Personal Data to any third party;

3.4.7. upon your written request following the expiration or earlier termination of the Services Agreement securely return to you such Client Personal Data, and unless prohibited under applicable law delete such Client Data in our possession in compliance with procedures and retention periods outlined in our Services Agreement;

3.4.8. on the condition that you have entered into an applicable non-disclosure agreement with us:

a) allow you and your authorized representatives to access and review up-to- date attestations, certifications, reports or extracts thereof from independent bodies (e.g., external auditors, internal audit, data protection auditors) or other suitable certifications to ensure compliance with the terms of this Data Processing Agreement; or

b) where required by Data Protection Law or the Standard Contractual Clauses (where the GDPR is applicable) contained in Annex 4 (and in accordance with this Section 3.4.8), allow you and authorized representatives to conduct audits (including inspections) during the term of the Services Agreement to ensure compliance with the terms of this Data Processing Agreement. Notwithstanding the foregoing, any audit must be conducted during our regular business hours, with reasonable advance notice to us and subject to reasonable confidentiality procedures. The scope of any audit shall not require us to disclose to you or your authorized representatives, or to allow you or your authorized representatives to access:

- any data or information of any other Aproove Client;
- any Aproove internal accounting or financial information;
- any Aproove trade secret;
- any information that, in our reasonable opinion could: 1) compromise the security of our systems or premises; or 2) cause us to breach our obligations under Data Protection Law or our security, confidentiality and or privacy obligations to any other Aproove Client or any third party; or
- any information that you or your authorized representatives seek to access for any

reason other than the good faith fulfilment of your obligations under the Data Protection Law and our compliance with the terms of this Data Processing Agreement.

c) In addition, audits shall be limited to once per year, unless 1) we have experienced a Personal Data Breach within the prior twelve (12) months which has impacted your Client Personal Data; or 2) an audit reveals a material noncompliance. If we decline or are unable to follow your instructions regarding audits permitted under this Section 3.4.8 (or the Standard Contractual Clauses, where applicable), you are entitled to terminate this Data Processing Agreement and the Services Agreement for convenience.

4. PROCESSING OF CLIENT PERSONAL DATA SUBJECT TO U.S. DATA PROTECTION LAW

The parties agree that this section 4 shall apply only to Client Personal Data that is protected by U.S. Data Protection Law. In addition to the processing requirements set out in Section 3 above, where we process Client Data Under U.S. Data Protection Law,we shall not retain, use, sell or otherwise disclose Client Personal Data other than as required by law or as needed to provide the Services to you. For purposes of this section 4, the term "sell" shall have the meanings given in the CCPA irrespective of whether CCPA or GDPR applies.

5. SECURITY AND NOTIFICATION OF PERSONAL DATA BREACH

5.1. We shall implement and maintain appropriate technical and organizational measures to protect the Client Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure in accordance with Annex 2. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of Client Personal Data and appropriate to the nature of the Client Personal Data which is to be protected. We may amend the technical and organizational measures, provided that the new measures do not fall short of the level of security provided by the specified measures

5.2. If we become aware of and confirm any Personal Data Breach we will notify you without undue delay. We shall assist You in notifying the personal data breach to the competent supervisory authority.

6. DATA TRANSFERS

The parties agree that this section 6 shall apply only to Client Personal Data that is protected by GDPR and such Client Personal Data is transferred outside the European Economic Area (EEA) to Aproove, either directly or via onward transfer.

6.1. EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

Aproove Affiliates comply with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks ("**Privacy Shield**"). Where the transfer of Client Personal Data is made to a Privacy Shield-certified entity, we agree to process Client Personal Data covered by Privacy Shield in accordance with the Privacy Shield Principles. We agree to comply with Privacy Shield throughout the term of the Services Agreement.

6.2. European Commission Standard Contractual Clauses (2010/87/EU)

The terms of the Standard Contractual Clauses outlined in Annex 4 will apply where the applicable transfer of Client Personal Data is (a) not subject to the laws of a jurisdiction recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR); or (b) not covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. In the event of any conflict or inconsistency between the provisions of this Data Processing Agreement and the Standard Contractual Clauses outlined in Annex 4, the provisions of the Standard Contractual Clauses shall prevail. In the event that any provision of the Standard Contractual Clauses is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of the Standard Contractual Clauses and the

terms of this Data Processing Agreement shall remain operative and binding on the parties.

7. MISCELLANEOUS.

7.1. Client acknowledges and agrees that as part of providing the Services and services, Aproove has the right to use data relating to or obtained in connection with the operation, support or use of the Services for its legitimate internal business purposes, such as to support billing processes, to administer the Services, to improve, benchmark, and develop our products and services, to comply with applicable laws (including law enforcement requests), to ensure the security of our Services and to prevent fraud or mitigate risk. To the extent any such data is personal data, Aproove warrants and agrees that: (i) it will process such personal data in compliance with Data Protection Law and only for the purposes that are compatible with those described in this Section 7.1; (ii) it will not use Client Personal Data for any other purpose or disclose it externally unless it has first aggregated and anonymised the data so that it does not identify the Client or any other person or entity. Aproove further agrees that it shall be a Controller and solely responsible and liable for any of its processing of personal data pursuant to this Section 7.1.

7.2. Through use of the Services, as further described in the Services Agreement, you or your End Users, as applicable, may elect to grant third parties visibility to your data or content (which may include Client Personal Data). You also understand that user profile information for the Services may be publicly visible. Nothing in this Data Processing Agreement prohibits (and, for the avoidance of doubt, Sections 3.3.5 and 3.3.7 above do not apply to) Aproove making visible your data or content (which may include Client Personal Data) to third parties consistent with this paragraph, as directed by you or your End Users through the Services.

7.3. In the event of any conflict or inconsistency between the provisions of the Services Agreement and this Data Processing Agreement, the provisions of this Data Processing Agreement shall prevail. This Data Processing Agreement is subject to the governing law and venue terms in the Services Agreement, except as otherwise provided in Annex 4 to the extent Annex 4 applies. For avoidance of doubt and to the extent allowed by applicable law, any and all liability under this Data Processing Agreement (including its Annexes) will be governed by the limitations of liability and other relevant provisions of the Services Agreement. Without limiting the foregoing, any liability arising under this Data Processing Agreement shall be subject to the limitations of liability under the Services Agreement as if such liability arose under the Services Agreement or the applicable order, and any liability of a party, its affiliates, their signatories or their suppliers arising under this Data Processing Agreement will be aggregated with any other applicable liability arising under the Services Agreement for purposes of applying any applicable liability caps. Save as specifically modified and amended in this Data Processing Agreement, all of the terms, provisions and requirements contained in the Services Agreement shall remain in full force and effect and govern this Data Processing Agreement. Except as otherwise expressly provided herein, no supplement, modification, or amendment of this Data Processing Agreement will be binding, unless executed in writing by a duly authorized representative of each party to this Data Processing Agreement. If any provision of the Data Processing Agreement is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of this Data Processing Agreement shall remain operative and binding on the parties.

***

Annex 1

Data

A.1. Data subjects

The personal data concern End Users of the Services, in addition to individuals whose personal data is supplied by End Users of the Services.

A.2. Categories of data

The personal data transferred concern the following categories of data:

- Direct identifying information (e.g., name, email address, telephone).
- Indirect identifying information (e.g., job title, gender, date of birth).
- Device identification data and traffic data (e.g., IP addresses, MAC addresses, web logs).
- Any personal data supplied by users of the Services.

A.3. Special categories of data

Aproove does not knowingly collect (and Client or End Users shall not submit or upload) any special categories of data (as defined under the Data Protection Legislation).

A.4. Purposes of processing

The personal data is processed for the purposes of providing the Services in accordance with the Services Agreement.

Annex 2
Security Measures

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

3. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized input, reading, copying, removal modification or disclosure of data. These measures shall include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems

- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

4. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.
- Creating an audit trail of all data transfers

5. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

Measures should include:

- Logging user activities on IT systems
- That it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- That it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data have been input;

6. Job control

Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

7. Availability control

Measures should be put in place designed to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Installed systems may, in the case of interruption, be restored
- Systems are functioning, and that faults are reported

- Stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.

These measures should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

Annex 3
Aproove Affiliates

- Aproove SA, a company incorporated under the laws of Belgium with registered office at 1, Boulevard Initalis, 7000 Mons, Belgium and registered with Crossroads bank for Enterprise under number 0867.065.974.

- Aproove Technologies, Inc., an Illinois corporation, with offices located at 132 N. York Street, Suite 1A, Elmhurst, IL 60120

Annex 4 – Standard Contractual Clauses

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

Data Transfer Services Agreement

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Aproove (hereinafter the "**data importer**") **and**

Client (hereinafter the "**data exporter**")

each a "**party**"; together "**the parties**",
HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their

implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional

qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

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

subprocessor shall be limited to its own processing operations under the Clauses.

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

Annex 5 – List of Approved Sub-processors

This Data Processing Annex outlines the approved sub-processors engaged by Aproove in connection with the processing of Client Personal Data under this Agreement.

1. Sub-processor Details

Name: Microsoft Azure
Role: Infrastructure Environment Provider
Scope of Processing: Microsoft Azure provides the cloud infrastructure services used by Aproove to deliver its platform and process Client Personal Data.
Jurisdiction: Global (Data residency and processing in compliance with applicable Data Protection Laws).

2. Terms and Obligations

As a sub-processor, Microsoft Azure operates under its **Microsoft Online Services Data Protection Addendum ("Microsoft DPA")**, which governs its processing of personal data. The Microsoft DPA can be reviewed at the following link: Microsoft Online Services Data Protection Addendum.

Aproove, as a processor, mirrors to the Client (the controller) the same rights and obligations received from Microsoft Azure under the Microsoft DPA. These include, but are not limited to:

- **Data Security:** Ensuring robust safeguards to protect personal data, including encryption, access controls, and security monitoring.
- **Data Transfers:** Complying with international transfer mechanisms as required by applicable Data Protection Law.
- **Data Subject Rights:** Facilitating the exercise of data subject rights as described in the Microsoft DPA.
- **Audit Rights:** Supporting audits and certifications, as outlined by Microsoft Azure.

3. Aproove as Processor

Aproove utilizes Microsoft Azure exclusively as its infrastructure provider.
Aproove is responsible for:

1. Ensuring compliance with obligations under applicable Data Protection Laws when using Microsoft Azure services.
2. Including terms in this Agreement that provide protections for the Client equivalent to those Microsoft Azure provides under the Microsoft DPA.
3. Providing transparency regarding Microsoft Azure's role as a sub-processor.

4. Updates to Sub-processors

If Aproove engages additional sub-processors or updates this list, we will notify the Client. The Client may object to such changes within forty-five (45) days of notice by terminating the Services Agreement for convenience.

For ongoing updates to this list, refer to: https://www.aproove.com/legals#tab3.

This annex is incorporated into and forms part of the Data Processing Agreement. All sub-processors engaged by Aproove, including Microsoft Azure, will adhere to terms no less protective than those stated herein.

Appendix 1 to the Standard Contractual Clauses

Data exporter

Client **Data**

importer

Aproove

Data subjects

The personal data concern End Users of the Services, in addition to individuals whose personal data is supplied by End Users of the Services.

Categories of data

The personal data transferred concern the following categories of data:

- Direct identifying information (e.g., name, email address, telephone).
- Indirect identifying information (e.g., job title, gender, date of birth).
- Device identification data and traffic data (e.g., IP addresses, MAC addresses, web logs).
- Any personal data supplied by users of the Cloud Product.

Special categories of data

Aproove does not knowingly collect (and Client or End Users shall not submit or upload) any special categories of data (as defined under the Data Protection Legislation).

Purposes of processing

The personal data is processed for the purposes of providing the Services in accordance with this Services Agreement.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The technical and organizational security measures implemented by the data importer are as described in Annex 2 of the Data Processing Data Processing Agreement.