DATA PROCESSING ADDENDUM

AMLBot KYC service – public offer · Version 1.0 · Last updated: 11 November 2026

This Data Processing Addendum (the “DPA”) is a public offer made by the AMLBot group company that is party to the agreement for the AMLBot KYC service with the Customer (the “Processor”, “we”). The Processor is either (a) Safe3 UAB, legal entity code 306141950, registered office J. Jasinskio g. 16B, LT-03163 Vilnius, Lithuania, or (b) Safelement Limited, Hong Kong Business Registration No. 73996474, registered office Office 1111, Suite 1102, Lee Garden One, 33 Hysan Avenue, Causeway Bay, Hong Kong, as stated in the Agreement. The DPA supplements the agreement under which the Processor provides the AMLBot KYC service (the “Services”) to the person that accepts the Services (the “Customer”) (the “Agreement”).

The DPA is accepted, and becomes binding between the Processor and the Customer, when the Customer accepts the terms of the Agreement that refer to it, or ticks the acceptance box for this DPA presented when the Agreement is concluded or when the Customer registers for the Services. The Processor records the acceptance (date, time and Customer account). If the Customer and the Processor have signed a separate data processing agreement for the Services, that agreement prevails.

This DPA consists of this text, Annex 1 (Details of the processing), Annex 2 (Security measures), Annex 3 (Processing instructions) and Annex 4 (Standard contractual clauses: completion), and of the document “AMLBot KYC – Sub-processors” (provided by the Processor to the Customer), which forms part of this DPA. No signature is required. Each document states the date of its latest update; the version in force on the date of acceptance applies, as recorded under the previous paragraph.

1. Definitions

1.1. “GDPR” means Regulation (EU) 2016/679. “UK GDPR” means the GDPR as it forms part of the law of the United Kingdom. “Data Protection Law” means the GDPR, the UK GDPR, the national laws implementing or supplementing them, and any other law on the protection of personal data that applies to the processing under this DPA, including US state privacy laws such as the California Consumer Privacy Act as amended (“CCPA”).

1.2. “Personal Data”, “controller”, “processor”, “processing”, “data subject”, “personal data breach”, “supervisory authority” and “special categories of personal data” have the meanings given in the GDPR. “Business”, “service provider”, “sell” and “share” have the meanings given in the CCPA.

1.3. “Customer Personal Data” means personal data of the Customer’s end users that the Processor processes on behalf of the Customer in providing the Services, as described in Annex 1.

1.4. “Sub-processor” means a third party engaged by the Processor, or by another Sub-processor, that processes Customer Personal Data.

1.5. “SCCs” means the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914.

2. Scope and roles

2.1. This DPA applies to the processing of Customer Personal Data in the course of the Services. The Customer is the controller (or a processor acting for its own controller) and the Processor is the processor (or sub-processor). Where the Agreement is concluded with Safe3 UAB, Safelement Limited acts as the Processor’s Sub-processor under the Sub-processor List. Where the Agreement is concluded with Safelement Limited, Safelement Limited is the Processor.

2.2. This DPA does not apply where the Processor acts as controller, including where it verifies its own users or processes data for its own legal obligations, security, accounting or enforcement of claims. In those cases the Processor's privacy notice applies.

2.3. The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.

3. Instructions

3.1. The Processor processes Customer Personal Data only on the Customer's documented instructions. The Agreement, this DPA (including the processing instructions in Annex 3), and the Customer's use and configuration of the Services are the Customer's complete instructions at the date of acceptance. Further instructions must be given in writing and are subject to agreement on any additional cost.

3.2. The Processor may process Customer Personal Data other than on instructions only where European Union or Member State law (or, for UK data, UK law) requires it. In that case the Processor informs the Customer before the processing, unless the law prohibits this.

3.3. The Processor informs the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Law. The Processor may suspend the instruction until the Customer confirms or amends it.

3.4. The Processor does not use Customer Personal Data, including images, documents and biometric data, to develop, train or improve its own or any third party's products, models or algorithms, and does not combine it with personal data from other sources except as needed to provide the Services.

4. Customer responsibilities

4.1. The Customer determines the purposes and means of the processing and is responsible for: (a) having a lawful basis for the processing and for its instructions; (b) giving data subjects the information required by Articles 13 and 14 GDPR, including about the use of the Processor and its Sub-processors; (c) the accuracy and lawfulness of the data it submits; and (d) responding to data subjects' requests, with the Processor's assistance under clause 9.

4.2. The Services may involve biometric data (facial recognition and liveness detection) that is processed to uniquely identify a natural person and is therefore a special category of personal data under Article 9 GDPR. The Customer is responsible for determining the condition under Article 9(2) GDPR that applies, for obtaining any consent required, and for giving data subjects the notice about biometric processing required by the Services, in the form and by the means made available in the Services. The Processor shall make available to the Customer reasonably necessary information about the biometric processing performed through the Services to enable the Customer to fulfil its applicable transparency and data protection impact assessment obligations.

4.3. The Customer confirms that it uses the Services only for lawful identity verification and in accordance with the Agreement.

5. Confidentiality and personnel

5.1. The Processor ensures that persons authorised to process Customer Personal Data are bound by an obligation of confidentiality, receive appropriate data protection instructions, and have access only to the extent needed to provide the Services.

6. Security

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, and the risks to data subjects, the Processor implements appropriate technical and organisational measures in accordance with Article 32 GDPR. The measures are set out in Annex 2 (the "Security Measures").

6.2. The Processor may update the measures provided the update does not reduce the overall level of protection.

7. Sub-processors

7.1. The Customer gives the Processor a general authorisation to engage Sub-processors. The Sub-processors engaged at the date of this DPA are listed in the document “AMLBot KYC – Sub-processors” provided by the Processor to the Customer (the “Sub-processor List”).

7.2. The Processor informs the Customer of any intended addition or replacement of a Sub-processor at least 5 days before the change takes effect, by notice to the Customer’s contact address (the e-mail address for notices stated in the Agreement or, if none is stated, the e-mail address of the Customer’s account) together with the updated Sub-processor List. The Customer may object on reasonable data protection grounds within that period. The parties then discuss in good faith. If no solution is found, the Customer may terminate the affected part of the Services and receives a refund of prepaid fees for the period after termination.

7.3. The Processor imposes on each Sub-processor data protection obligations no less protective than those in this DPA, and remains liable to the Customer for the Sub-processor’s performance of those obligations.

7.4. The Processor shall impose on each Sub-processor the data protection obligations required by Article 28(4) GDPR, including the obligation to process Customer Personal Data only on documented instructions, subject to the exceptions permitted by applicable Data Protection Law.

8. International transfers

8.1. The Processor transfers Customer Personal Data outside the European Economic Area only where the destination is covered by an adequacy decision of the European Commission or where appropriate safeguards under Chapter V GDPR are in place.

8.2. Transfers by the Customer to the Processor. If the Processor is established in a country outside the EEA that is not covered by an adequacy decision (in particular where the Processor is Safelement Limited, Hong Kong) and the Customer is subject to the GDPR, the Customer’s transfer of Customer Personal Data to the Processor is a restricted transfer. In that case the SCCs (Module Two, controller to processor) apply between the Customer as data exporter and the Processor as data importer and are incorporated into this DPA, completed as set out in Annex 4. Where the Customer acts as processor for its own controller, Module Three applies. Where the Processor is Safe3 UAB, established in Lithuania, no such transfer takes place between the Customer and the Processor.

8.3. Transfers by the Processor to Sub-processors. Where the Processor transfers Customer Personal Data to a Sub-processor outside the EEA that is not covered by an adequacy decision, the Processor concludes the SCCs (Module Three, processor to processor) with that Sub-processor, or relies on another valid transfer mechanism. The Customer authorises these transfers.

8.4. UK and Swiss data. Where UK GDPR or the Swiss Federal Act on Data Protection applies to a transfer, the SCCs apply as supplemented by the UK International Data Transfer Addendum issued by the UK Information Commissioner, or as adapted to Swiss law, as applicable, and the references in Annex 4 are read accordingly.

8.5. If the SCCs conflict with this DPA, the SCCs prevail.

9. Data subject requests and assistance

9.1. Taking into account the nature of the processing, the Processor assists the Customer by appropriate technical and organisational measures in responding to requests from data subjects to exercise their rights under Chapter III GDPR.

9.2. If a data subject contacts the Processor directly about Customer Personal Data, the Processor forwards the request to the Customer without undue delay and does not respond except on the Customer's instructions or where the law requires.

9.3. The Processor assists the Customer in meeting its obligations under Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments and prior consultation with a supervisory authority), taking into account the nature of the processing and the information available to the Processor. The Processor provides the information on the Services reasonably needed for a data protection impact assessment of the biometric processing.

9.4. The Processor maintains records of processing activities carried out on behalf of the Customer, as required by Article 30(2) GDPR, and makes them available to a supervisory authority on request.

10. Personal data breach

10.1. The Processor shall notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data.

10.2. The notification describes, to the extent known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information that is not yet available is provided in stages without undue further delay.

10.3. The Processor takes reasonable steps to contain and remedy the breach and cooperates with the Customer. The Processor does not notify supervisory authorities or data subjects about the breach on the Customer's behalf unless the law requires or the Customer instructs it to.

11. Government and third-party requests

11.1. If a public authority requests disclosure of Customer Personal Data, the Processor, unless the law prohibits it, informs the Customer promptly, reviews the legality of the request, challenges it where there are reasonable grounds to do so, and discloses only the minimum permitted.

12. Deletion and return

12.1. During the Agreement the Processor keeps Customer Personal Data for the period set by the Customer's instructions and configuration of the Services or, where the Customer gives no instruction, for the default periods in Annex 3.

12.2. On termination or expiry of the Services, the Processor, at the Customer's choice made within 30 days, deletes or returns Customer Personal Data and deletes existing copies, unless European Union or Member State law requires storage. If the Customer makes no choice, the Processor deletes the data after that period. The Processor carries out the deletion within 30 days after the choice or after the end of that period and instructs its Sub-processors to delete the data. Backup copies are overwritten in the normal backup cycle. On request the Processor confirms the deletion in writing, including, once the Sub-processors have confirmed it to the Processor, the deletion by them.

13. Audit and information

13.1. The Processor makes available to the Customer the information necessary to demonstrate compliance with this DPA and Article 28 GDPR, including, on request and subject to confidentiality, the certificates and audit summaries it holds (for example its ISO/IEC 27001 certificate).

13.2. The Processor shall allow and contribute to audits, including inspections, as required by Article 28(3)(h) GDPR. The parties shall, where appropriate, first seek to demonstrate compliance through available certifications, independent audit reports and other relevant documentation. Customer-initiated audits shall ordinarily be conducted on at least 30 days' written notice, during business hours and no more than once in twelve months, unless a personal data breach, a supervisory authority request or applicable law reasonably

requires otherwise. Audits shall be subject to appropriate confidentiality and security safeguards and shall not compromise the data of other customers. The Customer shall bear its own audit costs and the Processor's reasonable costs for audits exceeding one working day.

14. US state privacy laws

14.1. To the extent the CCPA or another US state privacy law applies to Customer Personal Data, the Customer is the business and the Processor is the service provider. The Processor processes the personal information only for the business purposes of providing the Services as specified in the Agreement and this DPA.

14.2. The Processor does not sell or share the personal information, does not retain, use or disclose it outside the direct business relationship with the Customer or for any purpose other than the business purposes specified, and does not combine it with personal information it receives from other sources, except as the law permits.

14.3. The Processor notifies the Customer if it determines that it can no longer meet its obligations under the applicable law. The Customer may take reasonable steps to stop and remediate unauthorised use of personal information.

15. Liability, term and general provisions

15.1. The liability of each party under this DPA is subject to the limitations of liability in the Agreement. If the Agreement contains no limitation of liability, the aggregate liability of each party under this DPA in any twelve-month period will not exceed the fees paid and payable by the Customer to the Processor under the Agreement in that period. The limitations apply except to the extent the law does not allow them to be limited. This does not affect the rights of data subjects under the SCCs or under Article 82 GDPR.

15.2. This DPA applies for as long as the Processor processes Customer Personal Data, and ends when all Customer Personal Data has been deleted or returned. Clauses that by their nature continue survive.

15.3. In a conflict between this DPA and the Agreement on the processing of personal data, this DPA prevails. The SCCs prevail over both.

15.4. This DPA is governed by the law that governs the Agreement, subject to mandatory provisions of Data Protection Law. The SCCs are governed as set out in Annex 4.

15.5. The Processor may update this DPA by publishing a new version and informing the Customer at least 3 days in advance. Changes that reduce the protection of Customer Personal Data take effect for a Customer only with its consent. If a provision is invalid, the remaining provisions continue in force. The Security Measures and the Sub-processor List may be updated as set out in clauses 6.2 and 7.2.

15.6. This DPA and the Sub-processor List are provided in English.

16. Contact

Data protection officer and requests under this DPA: legal@safelement.org.

Annex 1 – Details of the processing

Subject matter	Identity verification of the Customer's end users through the AMLBot KYC service.
Duration	For the term of the Agreement and until deletion under clause 12.
Nature of the processing	Receiving, verifying with the verification software deployed on the Services' infrastructure, storing, retrieving, displaying to the Customer, and deleting identity verification data and results, and sending service e-mails to end users.
Purpose	To enable the Customer to verify the identity of its end users and to record the result of the verification.
Categories of data subjects	End users of the Customer who undergo identity verification.
Types of personal data	Full name, date of birth, country, identity documents and the data on them, photographs and selfie images, video and liveness check data, facial images, verification status and results, technical identifiers of the verification, e-mail address, IP address and request metadata.
Special categories	Biometric data processed for the purpose of uniquely identifying a natural person (Article 9 GDPR). See clause 4.2.
Frequency	Continuous, for the duration of the Services.
Retention	As instructed by the Customer. Where the Customer gives no instruction, the default periods in section 4 of Annex 3 apply. Deletion under clause 12 applies in all cases.
Sub-processors	See the Sub-processor List.

Annex 2 – Security measures

The Processor applies measures appropriate to the risk, including the following:

- Information security management (Safelement Limited). Safelement Limited, which operates and secures the platform, holds an information security management system certified to ISO/IEC 27001.
- Access control (Processor and Safelement Limited). Access to Customer Personal Data is limited to the personnel of the Processor and of Safelement Limited who need it to provide the Services, on the basis of individual accounts. Multi-factor authentication is required for enterprise applications and production systems.
- Authentication of user accounts (platform operated by Safelement Limited). Passwords of user accounts are stored only as salted hashes (bcrypt). Passwords are not stored in plain text.
- Confidentiality (Processor and Safelement Limited). Personnel with access are bound by confidentiality obligations (clause 5).
- Data in transit (platform). Customer Personal Data is transmitted over encrypted connections.
- Hosting (Google Cloud EMEA Limited). The Services are hosted with Google Cloud in the European Union.
- Identity verification (Regula software). Document authentication, face matching and liveness detection are performed by software provided by Regula Forensics, Inc. and deployed on the infrastructure of the Services in the European Union. Personal data is not transferred to the software provider.
- Backups (platform). Backups are encrypted and retained for up to 90 days.
- Change management (development team of the Processor and Safelement Limited). Changes to the code of the Services are reviewed by another developer before release.
- Incident management (Processor and Safelement Limited). Security incidents are handled under an incident procedure; personal data breaches are notified to the Customer under clause 10.
- Sub-processors (Processor). Sub-processors are assessed before engagement and bound by data processing terms (clause 7).

- Retention and deletion (Processor). Customer Personal Data is deleted or returned at the end of the Services (clause 12).

Annex 3 – Processing instructions

These are the Customer's documented instructions to the Processor under Article 28(3)(a) GDPR. The Processor follows them in providing the Services.

1. Permitted processing

- Receive from the Customer, or from the Customer's end user through the Services, the data needed for identity verification (Annex 1).
- Verify that data with the verification software deployed on the Services' infrastructure, and store and display the result and the verification materials to the Customer's authorised users.
- Delete the data in accordance with section 4 of this Annex and clause 12.
- Carry out technical operations needed to provide, secure, support and maintain the Services (hosting, backup, monitoring, troubleshooting), without using the data for any other purpose.

2. Prohibited processing

- Using Customer Personal Data for the Processor's or any third party's own purposes, including marketing, profiling, analytics, product development, and training or improving models (clause 3.4).
- Creating or using biometric data for any purpose other than the verification requested by the Customer.
- Linking Customer Personal Data with personal data from other services or customers of the Processor, except as needed to provide the Services.
- Disclosing Customer Personal Data to anyone other than the Customer, the Sub-processors listed in the Sub-processor List, and recipients required by law (clause 11).
- Storing Customer Personal Data in the Processor's CRM, messaging tools, e-mail, task trackers or other internal tools, except the verification status and the technical identifiers needed to administer the account.

3. Access by the Processor's personnel

- Personnel access the content of verification materials (documents, images, video, biometric data) only where needed to resolve a technical fault or a request from the Customer, and only to the extent needed.
- Access is limited to authorised personnel, using individual accounts with multi-factor authentication, and is recorded where the Services allow.

4. Retention and deletion

- The Processor keeps Customer Personal Data for the period configured by the Customer. If the Customer has not configured a period, the following default periods apply: (a) successful verifications, including documents, photographs, selfie images and verification results: 5 years from the date of verification; (b) rejected verifications: 90 days from the date of rejection; (c) unfinished verifications: 30 days from the last activity; (d) video and liveness data: deleted after the verification result is issued, and in any case within 30 days; (e) biometric templates: not stored after the comparison and, where storage is technically necessary, deleted within 30 days of the verification result; (f) application logs: 12 months from creation; (g) backup copies: up to 90 days, overwritten in the normal backup cycle.
- Data of unfinished, failed or rejected verifications is kept only for the period set in the previous paragraph and is not used for any other purpose.

- On termination of the Agreement, clause 12 applies in place of the default periods.
- The Customer may instruct deletion of a specific end user's data at any time through the Services or by written request to legal@safelement.org. The Processor carries out the deletion within 30 days of the instruction, deletes the corresponding data held by the Services and by its Sub-processors, and, on request, confirms the deletion in writing, including the deletion by a Sub-processor once the Sub-processor has confirmed it to the Processor.

5. Data subject requests

- The Processor forwards a request received directly from an end user to the Customer without undue delay and does not answer it (clause 9.2).
- On the Customer's instruction the Processor provides access to, exports, corrects or deletes the data of an end user, and informs the Sub-processor where needed.

6. Transfers

- The Processor transfers Customer Personal Data only to the Sub-processors listed in the Sub-processor List and only to the locations stated there (clause 8).

7. Notifications to the Customer

- Personal data breach: without undue delay (clause 10).
- Intended change of a Sub-processor: at least 5 days in advance (clause 7.2).
- Instruction that the Processor considers unlawful, or a request from a public authority: without undue delay (clauses 3.3 and 11).

8. Further instructions

- Further or changed instructions are given in writing to legal@safelement.org. The Processor confirms in writing whether and from when it can follow them. Until confirmation, the Processor continues under the existing instructions.
- Instructions that require the Processor to act contrary to the law, to the Agreement or to the Security Measures may be refused.

Annex 4 – Standard contractual clauses: completion

Modules	Module Two (controller to processor) for clause 8.2, or Module Three where the Customer is a processor.
Clause 7 (docking clause)	Included.
Clause 9 (sub-processors)	Option 2, general written authorisation; notice period 5 days as set out in clause 7.2 of the DPA.
Clause 11 (redress)	Optional independent dispute resolution body: not included.
Clause 13 and Annex I.C (supervisory authority)	Determined under Clause 13 of the SCCs: the supervisory authority of the Member State in which the data exporter is established; or, where the data exporter is not established in the EU but is subject to the GDPR under Article 3(2), the authority of the Member State in which its representative is established or, if it has none, of a Member State in which the data subjects are located.
Clause 17 (governing law)	Option 1: the law of Lithuania.
Clause 18 (forum)	The courts of Lithuania.
Annex I.A (parties)	Data exporter: the Customer. Data importer: the Processor named in the Agreement (Safe3 UAB or Safelement Limited, details in the introduction of the DPA), contact legal@safelement.org. Roles: as in clause 2 of the DPA.
Annex I.B (description)	As in Annex 1 of the DPA.
Annex II (security)	As in the Security Measures.
Annex III (sub-processors)	As in the Sub-processor List.