First AML - Data Processing Addendum ("DPA")

This Data Processing Addendum ("**DPA**"), forms part of, and is subject to the terms and conditions of the First AML Terms of Engagement or other written or electronic agreement ("**Agreement**") between Customer and the First AML entity as set out in the Agreement, ("**First AML**") (each a "**Party**" and collectively "**Parties**"). All capitalised terms not defined in this DPA shall have the meaning set forth in the Agreement.

The Parties agree as follows:

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity. **Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

"**Customer Personal Data**" means any Customer Data that is personal data that First AML's processes on behalf of Customer in the course of providing the Services.

"**Data Protection Laws**" means all data protection and privacy laws, regulations and secondary legislation applicable to the respective Party in its role in the processing of personal data under the Agreement, including, to the extent applicable, European Data Protection Laws, as may be amended, superseded or replaced.

"**European Data Protection Laws**" means (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**"); (ii) the UK Data Protection Act 2018 ("**UK GDPR**"); (iii) the Swiss Federal Data Protection Act ("**Swiss DPA**");

"**Europe**" means, for the purposes of this DPA, the European Economic Area and/or its member states, the United Kingdom and/or Switzerland.

"**First AML Data**" means any personal data relating to a data subject which is subject to Data Protection Laws and which First AML collects or receives in connection with the Services and processes for its own purposes, as a controller, as further described in Annex A of this DPA.

"**Purposes**" shall mean the data processing purposes described in Annex A of this DPA.

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"**Security Incident**" means any actual unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or

access to Customer Personal Data on systems managed by or otherwise controlled by First AML but does not include any Unsuccessful Security Incident.

"**Services**" means any product or service provided by First AML to Customer pursuant to the Agreement.

"Standard Contractual Clauses" means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); (ii) where the UK GDPR applies, the EU SCCs as supplemented and amended by the UK Addendum; and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (the "**Swiss SCCs**").

"**Sub-processor**" means any third party (including any First AML Affiliates) engaged by First AML to process any Customer Personal Data (but shall not include First AML employees or consultants).

"**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018.

"**Unsuccessful Security Incident**" means an unsuccessful attempt or activity that does not compromise the security of Customer Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents.

The terms "**data subject**", "**personal data**", "**controller**", "**processor**" and "**processing**" shall have the meaning given to them in applicable Data Protection Laws, or if not defined therein, the GDPR, and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that First AML processes Customer Personal Data that is protected by Data Protection Laws as a processor or sub-processor on behalf of the Customer in the course of providing Services pursuant to the Agreement.

2.2 Notwithstanding expiry or termination of the Agreement, this DPA and any Standard Contractual Clauses (if applicable) will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data by First AML as described in this DPA.

3. Roles and Scope of Processing

3.1 **Role of the Parties**. As between First AML and Customer, Customer is the controller or processor of Customer Personal Data and First AML shall process Customer Personal Data only as a processor acting on behalf of Customer (including as described in **Annex A** of this DPA). Each party shall comply with its obligations under applicable Data Protection Laws in respect of any personal data it processes under the Agreement. With respect to Customer Personal Data, First AML is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to First AML as a service provider.

3.2 **Customer Instructions**. First AML will process Customer Personal Data in accordance with the Customer's documented lawful instructions, except where otherwise required by applicable law. For these purposes, Customer instructs First AML to process Customer Personal Data for the Purposes. If Customer is itself processor acting on behalf of or jointly with a third-party controller, Customer represents and warrants to First AML that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of First AML as a processor or sub-processor, have been authorised by the relevant controller or joint controllers.

3.3 **Notification Obligations Regarding Customer Instructions**. First AML shall promptly notify Customer in writing, unless prohibited from doing so under Data Protection Law, if: (a) it becomes aware or believes that any data processing instruction from Customer violates Data Protection Law; or (b) it is unable to comply with Customer's data processing instructions.

4. First AML Data

4.1 **First AML Data.** First AML may collect First AML Data in connection with the provision of the Services. First AML shall process First AML Data in accordance with its obligations as a controller under applicable Data Protection Laws and only for the Purposes contemplated in the Agreement (including this DPA) as further described in Annex A.

4.2 **Mutual Assistance.** Each party shall provide reasonable assistance to the other as may be required in order to enable each party to perform its responsibilities under Data Protection Laws. In particular (and without limitation) (i) the parties shall notify each other promptly if either becomes aware of any breaches of this DPA or Data Protection Laws and will work together and assist each other as reasonably necessary to remediate any such breaches and (ii) in the event that either party receives any correspondence, enquiry or complaint from a data subject, regulator or other third party related to the disclosure of First AML Data to First AML or the processing of First AML Data by First AML, it shall promptly inform the other party giving full details of the same and the parties shall cooperate reasonably and in good faith in order to respond to the correspondence in accordance with Data Protection Laws.

5. Sub-processing

5.1 **Authorised Sub-processors**. Customer provides a general authorization for First AML to engage Sub-processors to process Customer Personal Data. The Sub-processors that are currently authorised to access and process Customer Personal Data are listed at www.firstaml.com/sub-processors. This URL may change if First AML updates its website or client-facing documentation, in which case Customer will be notified of the change.

5.2 **Sub-processor Obligations**. First AML shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause First AML to breach any of its obligations under this DPA.

5.3 **Changes to Sub-processors.** First AML shall notify Customer if it adds a new Sub-processors at least ten (10) days prior to any such changes if Customer opts-in to receive such notifications. Customer may object in writing to First AML's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the Parties will

discuss such concerns in good faith with a view to achieving resolution. If First AML cannot provide an alternative Sub-processor, or the Parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer as its sole and exclusive remedy, may terminate the relevant part of the Agreement (including this DPA) regarding those Services which cannot be provided by First AML without the use of the Sub-processor concerned without liability to either Party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

6. Security

6.1 **Security Measures**. First AML shall implement and maintain appropriate technical and organisational security measures to protect Customer Personal Data from Security Incidents and to preserve the security, integrity and confidentiality of the Customer Personal Data. These measures shall at a minimum comply with Data Protection Laws and include the measures described in Annex B (**"Security Measures"**). First AML shall ensure that any person who is authorised by First AML to process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

6.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by First AML relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that First AML may update or modify the Security Measures from time to time and without notice, provided that such updates and modifications do not result in a material degradation of the overall security of the Services subscribed to by Customer.

6.3 **Security Incident Response**. In the event of a Security Incident, First AML shall: (i) notify Customer without undue delay and in any event such notification shall, where feasible, occur no later than 48 hours from First AML becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) First AML shall promptly take all reasonable steps to contain, investigate, and mitigate any Security Incident. First AML's notification of or response to a Security Incident under this Section 6.3 (Security Incident Response) will not be construed as an acknowledgment by First AML of any fault or liability with respect to the Security Incident.

7. Security Reports and Audits

7.1 **Audit Rights**. First AML audits its compliance against data protection and information security standards on a regular basis. Upon Customer's written request, and subject to obligations of confidentiality, First AML will make available to Customer a summary of its most recent relevant audit report and/or other documentation reasonably required by Customer which First AML makes generally available to its customers, so that Customer can verify First AML's compliance with this DPA. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to First AML for any time expended for on-site audits.

8. Customer Responsibilities

8.1 **Security.** Customer agrees that, without prejudice to First AML's obligations under Section 6.1 (Security Measures) and Section 6.3 (Security Incident Response):

(a) Customer is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data, securing its account authentication credentials, managing its data back-up strategies, and protecting the security of Customer Personal Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Personal Data; and

(b) Customer shall be solely responsible for ensuring Customer Personal Data accessed, maintained or stored by First AML's personnel while on the Customer's facilities and/or otherwise accessed or processed by First AML's personnel on computer systems or other electronic equipment controlled by Customer during the provision of the Services is processed in compliance with Customer's data protection and security obligations under applicable Data Protection Laws and any associated policies, codes of practices and/or procedures relating to any User, worker, Client, Customer, or supplier of the Customer;

8.2 **Customer's Responsibilities**. Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Customer represents and warrants that: (i) it has provided, and will continue to provide, all notice and obtained, and will continue to obtain, all consents, permissions and rights necessary under Data Protection Laws for First AML to lawfully process Customer Personal Data on Customer's behalf and in accordance with its instructions; (ii) it has complied with all applicable Data Protection Laws in the collection and provision to First AML and its Sub-processors of such Customer Personal Data; and (iii) it shall ensure its processing instructions comply with applicable laws (including Data Protection Laws) and that the processing of Customer Personal Data by First AML in accordance with the Customer's instructions will not cause First AML to be in breach of applicable Data Protection Laws.

9. Co-operation and Data Protection Impact Assessments

9.1 **Data Subject Requests**. To the extent Customer is unable to independently retrieve, access or delete the relevant Customer Personal Data within the Services, First AML shall (at Customer's request and expense and taking into account the nature of the processing) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Personal Data under the Agreement. In the event that any request from individuals or applicable data protection authorities is made directly to First AML where such request identifies Customer, First AML shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so, and instead, after being notified by First AML, Customer shall respond. If First AML is required to respond to such a request, First AML will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

9.2 **Record Keeping**. Customer acknowledges that First AML is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which First AML is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, Customer will, where requested, provide such information to First AML via means provided by First AML, and will ensure that all information provided is kept accurate and up-to-date.

9.3 **DPIAs.** To the extent First AML is required under applicable Data Protection Laws, First AML shall (at Customer's request and expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

10. Return or Deletion of Data

10.1 Upon Customer's request, or upon termination or expiry of the Agreement, First AML shall destroy or return to Customer Personal Data in its possession or control within a reasonable period. This requirement shall not apply to the extent that First AML is required by any applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data First AML shall securely isolate and protect from any further processing and eventually delete in accordance with First AML's deletion policies, except to the extent required by such law.

11. Data Transfers

11.1 **Location of Processing**. Personal data that First AML processes under the Agreement may be processed in any country in which First AML, its Affiliates and authorised Sub-processors maintain facilities to perform the Services. First AML shall not process or transfer Customer Personal Data (nor permit such data to be processed or transferred) outside of Europe, unless it first takes such measures as are necessary to ensure the transfer is in compliance with this DPA and European Data Protection Laws. Such measures may include (without limitation) transferring Personal Data to a recipient: (i) in a country that the European Commission or competent UK or Swiss authority (as applicable) has decided provides adequate protection for Personal Data (an "adequacy finding"); or (ii) that has executed Standard Contractual Clauses, as applicable.

11.2 **Transfer Mechanism**. The Parties agree that when the transfer of personal data from Customer (as "data exporter") to First AML (as "data importer") is a Restricted Transfer and European Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA as set out in Annex C. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict;

11.3 **Alternative Transfer Mechanism**. If First AML adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to European Data Protection Laws) for the transfer of personal data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which the relevant personal data is transferred).

12. Limitation of Liability

12.1 Each Party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including, where applicable, the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set forth in the main body of the Agreement.

12.2 Any claims against First AML or its Affiliates under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely against the Customer entity that is a Party to the Agreement.

12.3 Notwithstanding any other provision of the Agreement or this DPA, in no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA, the Standard Contractual Clauses or otherwise.

13. Relationship with the Agreement

13.1 The Parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Services.

13.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) Standard Contractual Clauses (where applicable); then (b) this DPA; and then (c) the main body of the Agreement.

13.3 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

Annex A – Description of Data Processing / Transfer

Data exporter	**Name of the data exporter:** The Party identified as the Customer in the Agreement. **Contact person's name, position and contact details:** The details provided in the Agreement. **Activities relevant to the data transferred:** Personal data transferred will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities: (i) storage and other processing necessary to provide, maintain and improve the Service pursuant to and as contemplated the Agreement; and/or (ii) disclosures in accordance with the Agreement and/or as compelled by applicable laws. **Role (Controller/Processor):** Controller.	
Data importer	**Name of the data importer:** The First AML entity as set out in the Agreement. **Contact person's name, position and contact details:** The details provided in the Agreement. **Activities relevant to the data transferred:** Personal data transferred will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities: (i) storage and other processing necessary to provide, maintain and improve the Service pursuant to and as contemplated the Agreement; and/or (ii) disclosures in accordance with the Agreement and/or as compelled by applicable laws. **Role (Controller/Processor):** Controller (for Module 1) or Processor (for Module 2).	
Categories of Data Subjects whose Personal Data is transferred	Data subjects include individuals about whom data is provided to First AML via the Services by, or at the direction of, the Customer, Clients, or by Users.	
Categories of Personal Data transferred:	**Where Module 1 is applicable**	• First and Last Name • Email • IP Address • Device ID • Domain Server • Type of device/ Operating System, browser used • Photos / selfies • Videos • Gender • Residential address • Date of birth / age • Digital images • Recordings of environment or documents provided by clients of Customer • Identity documents • Country of residence and location data • Country of citizenship • IRD/Tax numbers

		• Forms, information and documents required for tax reporting purposes (e.g. financial statements, trust documents, FATCA/CRS status, info and/or returns) • Other documents provided by the clients of Customer
	Where Module 2 is applicable	As described above in Module 1 above.
Sensitive Data Transferred (if appropriate) and applied Restrictions or Safeguards:	Customer may submit (or First AML may collect on behalf of Customer) sensitive personal data about Clients, the extent of which is determined and controlled by the Customer in its sole discretion and which may include the following types of sensitive personal data: • Biometric data such as faceprints; • Racial or ethnic origin; and • Any other category of sensitive personal data uploaded by (or on behalf of) the Customer or agreed upon between the Parties in the Agreement.	
Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous.	
Subject Matter and Nature of the Processing (Module 2 only):	First AML performs Customer Due Diligence on behalf of the Customer including determination of AML requirements based on the information and instructions provided by Customer and liaising directly with Clients to collect and verify their information. First AML will process the data only for the following purposes, (i) processing to provide the Services in accordance with the Agreement, (ii) processing to perform any steps necessary for the performance of the Agreement, (iii) processing initiated by Users in their use of the Services, and (iv) processing to comply with other reasonable instructions that are consistent with the terms of the Agreement.	
Duration of the Processing (Module 2 only):	The term of the Agreement until deletion of the personal data by First AML upon termination of the Agreement and in accordance with the terms of the Agreement.	
Purpose of the Data Transfer/Processing Operations:	**Module 1**	Personal data shall be processed by First AML for the purposes contemplated by the Agreement and described in the First AML Privacy Policy.
	Module 2	Customer Personal Data may only be processed by First AML on behalf of Customer for the following purposes: (i) as necessary for the performance of the Services and First AML's obligations under and pursuant to the Agreement (including the DPA); (ii) processing initiated by Clients or Users in their use of the Services; and (iii) any other purposes of processing of Customer Personal Data agreed upon between the Parties in writing (the "Purposes").
Period for which the Personal Data will be retained, or if that is not possible the criteria used to	**Module 1:** First AML will retain First AML Data for no longer than the period during which First AML has a legitimate need to retain such data for purposes it was collected or transferred.	

determinate that period, if applicable:	**Module 2:** First AML will retain Customer Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which First AML processes Customer Personal Data.
Competent supervisory authority	The competent supervisory authority, in accordance with Clause 13 of the Standard Contractual Clauses, shall be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.

Annex B – Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures of pseudonymisation and encryption of personal data	First AML utilises a cloud-based infrastructure for all of its systems: the Service operates on the Amazon Web Services ("AWS") platform and is protected by their security and environmental controls. **Pseudonymisation** ● Sequentially allocated integer internal identifiers are assigned to records of individuals within the platform. After personally identifiable data is removed, logs of those identifiers may remain as part of audit records recording that information was removed. These identifiers cannot be correlated back to any personal data, and are used to ensure First AML maintains evidence of complying with deletion requests (in accordance with applicable legal requirements on retention periods). **Encryption** ● Wherever available, First AML utilises AWS features to encrypt data at rest and in transit. Primarily this takes the form of at-rest encryption of data in AWS RDS and AWS S3, and transmission of data via HTTPS using TLS 1.2+ through AWS Cloudfront and AWS ALBs (Application Load Balancers). Encryption keys via AWS Key Management Service (KMS) are IAM (Identity and Access Management) role protected. The default symmetric AWS KMS key spec is utilised for encrypting data at rest. This represents a symmetric algorithm based on Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) with 256-bit keys, an industry standard for secure encryption. For transmission of data through public networks, First AML utilise TLS 1.2+ via the "TLSv1.2_2021" security policy in AWS Cloudfront, and TLS 1.2+ using the “ELBSecurityPolicy-FS-1-2-Res-2020-10” AWS ALB security policy cipher suites. Up to date details of supported ciphers for these policies can be found on the AWS website:

	• https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/secure-connections-supported-viewer-protocols-ciphers.html • https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Confidentiality** • Quarterly application penetration testing undertaken by an independent third party. • Numerous measures as part of First AML's ISO27001 certified Information Security programme, such as quarterly user access reviews, BC/DR and incident response procedures, IT related controls including anti-virus, mobile device management for company laptops, disk encryption, reduced IT environment for general staff i.e. no administrative access, and permitting whitelisted software only. • Data is encrypted in transit and at rest at all times. • Access is secured utilising Auth0, which includes a number of controls to address common authentication attack vectors (such as brute force protection). Fine-grained roles and permissions are utilised to ensure users only have access to the data they are permitted to see. **Integrity** • Integrity of data transmitted to the platform is ensured through the use of end-to-end encryption (utilising TLS 1.2+). • All interactions with the platform are secured, with authentication handled by a dedicated third party identity as a service platform (Auth0). • Data is stored in a versioned manner, with updates captured as new versions, and accompanying audit history recorded of who made what changes and when. • Data stored at rest is held in RDS and S3 buckets with strict access controls applied in AWS to prevent unauthorised access or tampering. • All access to the platform passes through AWS Cloudfront (CDN) and AWS WAF (Web Application Firewall) with inbound traffic analysed to identify and filter out malicious. **Availability** • The platform is generally deployed across multiple AWS availability zones within each region, with various components configured in a high-availability design. • AWS RDS (database) use storage auto-scaling to ensure resilience in case of excessive database utilisation. • Dedicated Site Reliability Engineer function.

	• Utilisation of Identity-as-a-Service (IDaaS) provider for handling authentication which operates in a high-availability fashion. **Resilience** • All data is held across multiple availability zones within a primary AWS region (eu-west-1 Ireland), and replicated to a secondary DR AWS region (eu-central-1 Frankfurt). • The platform design utilises a message queuing technology (AWS SQS) and retry policies to be resilient to intermittent failures when community with third party services.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	First AML has a documented Business Continuity/Disaster Recovery plan with documented and tested procedures, including with respect to: • Loss of platform operation (Production Internet/DNS); • Loss of platform - complete loss of all Production systems (Storage or Host); • Loss of platform operation – database; and • Cyber-attacks. Information assets are backed up regularly for operational recovery purposes as well as to comply with Business Continuity/Disaster Recovery plan and that backups are retained in accordance with business unit retention requirements. Backups are periodically tested to ensure recoverability from these backups. The information restoration procedures are regularly tested for effectiveness and acceptable performance.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	**Internal** • Half-yearly log, vulnerability, alerts and code process reviews with engineering and security teams. • Quarterly user access reviews. • Annual access card reviews. • Annual asset review process, which focuses on security context, requirements, and opportunity for security hardening. • Business Continuity/Disaster Recovery validation exercises as part of the First AML BC/DR plan. • Various alerts which may indicate security events/incidents. **External** • Quarterly application penetration testing. • Annual ISO27001 surveillance audits. • Annual internal audit, currently undertaken by an independent third party.

Measures for user identification and authorisation	• First AML has a cloud-first IT environment, and utilises staff email addresses in GSuite as an identifier [username] when accessing various systems. • In terms of platform access by customers, First AML provisions initial login(s) to authorised users, which enables those users to actively manage access to their unique platform environment through administrative controls available within the platform (including inviting additional users). • First AML has defined and documented user access privileges which relate to the role of the user. • Staff access to systems is granted on a least-privilege basis, identifying the minimum levels of access needed for a staff member to perform their job. • A third party provider is used for authentication and authorising access to the platform (Auth0) which meets the highest security standards for an identity provider. See https://auth0.com/security for more details.

Measures for the protection of data during transmission	• For transmission of data through public networks First AML utilises TLS 1.2+ via the "TLSv1.2_2021" security policy in AWS Cloudfront, and TLS 1.2+ using the "ELBSecurityPolicy-FS-1-2-Res-2020-10" AWS ALB security policy cipher suites. Up to date details of supported ciphers for these policies can be found on the AWS website, including at:
	  ○ https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/secure-connections-supported-viewer-protocols-ciphers.html and
	  ○ https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html.
	• When responding to individual requests for information, First AML utilises secure file sharing tools, which have numerous security controls in place including encryption in transit.
	• First AML ensures that Sub-processors have robust Information Security systems to reduce the risk of breaches in transmission. First AML regularly performs a review of the security-level of Sub-processors used.

Measures for the protection of data during storage	• At rest encryption. • User access controls. • Robust platform security which is maintained through secure development practices, testing, and external assessment (PEN testing). • Utilising AWS IAM policies to restrict access and operations that can be performed on data held in AWS RDS and AWS S3, such as permanent deletions. • Utilising AWS versioned buckets for S3, to ensure all modifications to data are retained as unique versions.

Measures for ensuring physical security of locations at which personal data are processed	• First AML's physical offices have security controls which comply with ISO27001. • First AML ensures Sub-processors have strict physical security controls e.g. the data centres with around-the-clock security, automatic fire detection and suppression, redundant power supply systems, and strict controls for physical access. • Access to office areas is restricted. A continuously controlled reception area or gates secured by badge readers or other appropriate mitigating control to restrict access to the premises. Each staff member is responsible for swiping their individual badge at the badge reader associated with the secured access control point. • When arriving at the First AML secured area, visitors are required to sign either an electronic visitor's log indicating (i) the date of the visit, (ii) the time of the visit and (iii) the First AML person visited. Visitors are escorted by the First AML visit sponsor or delegate. • Perimeters are designed to address environmental protection (e.g. fire and flood) as well as physical access. • Environmental threats are considered and controls appropriate for risk mitigation are implemented to reduce the potential for an incident to occur from fire, theft, vandalism, explosion, smoke, water, vibration, chemical exposure, electrical failure, electrical interference or accidental damage. • Environmental controls such as heating, ventilation, air conditioning, emergency lighting, drainage, fire suppression, continuous power and humidity control are implemented in facilities in accordance with security risk assessments.
Measures for ensuring events logging	First AML business units and functional organisations maintain processes to monitor and capture information related to the interaction between users and information assets. Specific events are recorded in order to identify security incidents, establish individual accountability and reconstruct events. Measures in place include: • Dedicated SRE function with specific responsibilities. • Half-yearly log process review. • Alerts in place to detect absence of logging.
Measures for ensuring system configuration, including default configuration	• AWS production access is restricted to the on-call engineering team. • Utilising AWS Config to ensure AWS configuration standards are upheld (such as not allowing for public S3 buckets). • All AWS infrastructure changes are orchestrated via an infrastructure as code tool, tracked in source control and must undergo peer review before being applied. • A common set of based container images are utilised for all platform systems and regularly updated for vulnerabilities, with configuration tracked in source control.

	• All system configuration changes and related infrastructure changes are linked to tickets in First AML's issue tracking system. • Access to perform tasks (such as manual database maintenance) are logged, and activity is reported/alerted into First AML's collaboration tool for review.
Measures for internal IT and IT security governance and management	• **Security governance** - numerous efforts including an ISMS committee which meets quarterly, annual internal/external audits, annual management reviews, ISMS operational tasks and monthly ISMS reviews. • **IT governance** - First AML has implemented various IT controls such as antivirus, MDM, and disk encryption on company laptops and DesktopCentral which provides for a reduced general user IT environment and numerous security related controls e.g. screen autolock, enforcing password requirements, non-admin access for general staff etc.
Measures for certification/assurance of processes and products	• Successful AWS Well Architected Assessment. • ISO27001:2013 certification. • Quarterly application penetration testing. • Monthly QA on analyst manual processing. • AWS has obtained certifications for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 9001:2015, and CSA STAR CCM v3.0.1. For more information, see for example the pages www.aws.amazon.com/compliance/soc-faqs and https://aws.amazon.com/compliance/iso-certified/.
Measures for ensuring data minimisation	• During the provision of the Service, First AML only obtains data which is necessary for the provision of the Service.
Measures for ensuring data quality	• The platform collects and stores data in a consistent and structured manner (held in a relational data store), implementing a variety of business logic checks and validation to ensure data is stored in a standardised manner, and is internally consistent and accurate. • Data is stored in a versioned manner, allowing reconstruction of data held in the platform at a point in time, to meet a customer need to provide an accurate point-in-time view of verifications undertaken in relation to customer onboarding based on available information at the time. • Mechanisms exist for data subjects to request changes to their data held by customers, and for customers to action those requests as required.

	• Platform features allow for the review of all data collected and resultant verifications by customers, ensuring customers have the ability to monitor and rectify any identified data quality issues.
Measures for ensuring limited data retention	• First AML provides tools and processes which enable customers to meet their data retention obligations. • Data controlled by First AML is retained in accordance with an internal Data Retention Policy.
Measures for ensuring accountability	As per ISO27001:2013 related controls, First AML employs various measures for ensuring accountability, including: • Roles and responsibilities e.g. asset, supplier, and risk ownership, IT management, DPO role in internal privacy policy, documented ownership of specific ISMS areas by various staff, ISMS committee including specific roles & responsibilities for each member. • From an engineering perspective - appropriate team structure and responsibilities, including dedicated Site Reliability, Testing, and on-call engineer functions which ensure high impact activities are performed to the right level, by the right people, with the right processes and tools. • Systems and monitoring in place to ensure accurate audit trails are maintained for production environment access, infrastructure changes, configuration and code changes, which allows attributing changes to a specific staff member. • Software development lifecycle and processes ensure all activities are attributable and peer reviewed, and have bi-directional traceability from requirement, ticket/issue and code/configuration change ensuring high levels of appropriate accountability for system changes are maintained.
Measures for allowing data portability and ensuring erasure	• **Data portability:** Customers may export data from the Platform using in-built functionality and/or with assistance from First AML as and when requested. • **Data erasure:** Where a Customer has established that it is no longer required to retain data in order to meet its obligations under applicable laws, First AML will work with that customer to ensure data is permanently deleted.

Annex C – Standard Contractual Clauses

(a) In relation to transfers of Customer Personal Data subject to the EU GDPR, the EU SCCs shall apply, completed as follows:

i. Module Two (Controller to Processor) 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 Sub-processor changes shall be as set out in Section 5.3 of this DPA;

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

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

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

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

viii. Subject to Section 6.2 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA;

(b) In relation to transfers of First AML Data protected by the EU GDPR, the EU SCCs shall apply, completed as follows:

i. Module One (Controller to Controller) 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 EU SCCs will be governed by Irish law;

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

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

vii. Subject to section 6.2 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA;

(c) In relation to transfers of Personal Data subject to the UK GDPR, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, but shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK Addendum, and the parties confirm that the information required for the purposes of Part 1 (Tables) of the UK Addendum is set out in Annexes A and B to this DPA, except that for the purposes of Table 4 of Part 1 the parties select both the “Exporter” and “Importer” options.

(d) In relation to transfers of Personal Data subject to the Swiss DPA, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, with the following modifications:

i. references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

iii. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law" (as applicable);

iv. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

v. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

vii. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

viii. with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland,

(e) If the EU SCCs, implemented as described above, cannot be used to lawfully transfer such personal data in compliance with the Swiss DPA, the parties agree that the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Annex A and B this DPA (as applicable);

(f) If neither paragraph (c), (d) or (e) applies, then the parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by applicable Data Protection Laws without undue delay.