Data Processing and Security Policy for eComply & Verify SaaS

This eComply & Verify Data Processing Policy ("**DPA Policy**") describes the responsibilities of the parties with respect to the processing and security of any Client Personal Information in connection with the SaaS Services provided under any Service Order under the Agreement as agreed between Accenture & Client. Terms not defined below shall have the meaning set forth in the Agreement. In the event of a conflict between the Agreement and this DPA Policy, this DPA Policy shall prevail.

1. **Definitions**.

(a) "Business Contact Information" means the names, mailing addresses, email addresses, and phone numbers regarding the other party's employees, directors, vendors, agents, and customers, maintained by a party for business purposes as further described in Section 9 below.

(b) "Client Personal Information" means client-owned or controlled personal data provided by or on behalf of Client to Accenture or an Accenture affiliate or subcontractor for processing under a Service Order. Unless prohibited by applicable Data Protection Laws, Client Personal Information shall not include information or data that is anonymized, aggregated, de-identified and/or compiled on a generic basis and which does not name or identify a specific person.

(c) "Consents" includes all necessary consents, permissions, as well as notices and authorizations necessary for the processing or onward transfer by Accenture of Client Personal Information which is required to perform the SaaS Services, including the transfer of Client Personal Information outside of the country of origin and any of the foregoing, as applicable, from employees or third parties; valid consents from or notices to applicable data subjects; and authorizations from regulatory authorities, employee representative bodies or other applicable third parties;

(d) "Data Protection Laws" means all applicable data protection and privacy Laws that apply to the processing of personal data under a particular Service Order, including, as applicable, General Data Protection Regulation 2016/679 (GDPR), Federal Data Protection Act of 19 June 1992 (Switzerland), UK Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR), and any US state or federal laws or regulations pertaining to the collection, use, disclosure, security or protection of personal data, or to security breach notification, e.g., California Consumer Privacy Act of 2018 ("CCPA") and California Privacy Rights Act of 2020 ("CPRA").

(e) "Information Security Incident" means a breach of Accenture's security leading to the accidental or unlawful destruction, loss, alteration or unauthorized acquisition, disclosure, misuse, or access to unencrypted Client Personal Information transmitted, stored, or otherwise processed by Accenture.

(f) "Sub processors" means Accenture Affiliates and third parties authorized under the terms of this DPA Policy to have access to and process Client Personal Information in order to provide a portion of the Services.

(g) The terms "controller," "data subject," "de-identification," "personal data," "process," "processing," "processor," "pseudonymize," "sale," "service provider" and "supervisory authority" as used in this DPA Policy have the meanings given to any equivalent terms in the applicable Data Protection Laws, as relevant.

2. **Roles of the Parties; Compliance with Data Protection Laws**.

(a) Each party will comply with the requirements of the Data Protection Laws as applicable to such party with respect to the processing of the Client Personal Information.

(b) Client warrants to Accenture that it has and will maintain all necessary rights (including lawful legal basis), licenses and Consents to provide the Client Personal Information to Accenture for the processing to be performed in relation to the Services and agrees that Client shall be responsible for obtaining all necessary Consents or identifying the appropriate legal basis for the processing, and providing all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the Client Personal Information.

(c) Unless otherwise required by law, Accenture shall process Client Personal Information on Client's behalf as follows:

a. **The subject matter of the processing** is limited to the Client Personal Information identified in this document.

b. **The nature and purpose of the processing** shall be to provide the SaaS Services as defined in the applicable SO.

c. **The duration of the processing** is the Term of the applicable SO.

d. **The types of Personal Information** are name, address, vat ids, phone numbers, e-mail addresses, system access / usage / authorization data, and other information contained in client invoices submitted to the SaaS Services as part of Client Content.

e. **The categories of data subjects** are clients, employees, vendors, contractors, business partners or other individuals whose Personal Information is stored in the Client Content submitted to the SaaS Services.

(d) Accenture will process the Client Personal Information only in accordance with Client's documented processing instructions as set forth in the Agreement, including this DPA Policy and the applicable Service Order, unless otherwise required by law.

(e) If Accenture is acting as a sub processor in relation to any Client Personal Information (i.e., the data owner/controller is an entity other than Client), Client warrants to Accenture that Client's instructions with respect to the Client Personal Information have been authorized by the applicable data owner/controller, including the appointment of Accenture as a sub processor.

(f) Except as otherwise set forth in the applicable Service Order, (i) Accenture is a service provider and/or processor with respect to the Client Personal Information; and (ii) Client is an owner / controller or service provider / processor, as applicable, of the Client Personal Information.

(g) Accenture will promptly notify Client if Accenture determines, in its reasonable business judgment, that a Client processing instruction violates any applicable Data Protection Law (if nothing herein shall require Accenture to provide legal or regulatory advice or monitor Data Protection Laws as they apply to Client). In such event, the parties will work together in good faith to resolve such issue in a timely manner. In no event will either party be required to perform any activity that violates any applicable Data Protection Law. If Client requires that Accenture follow a processing instruction despite Accenture's notice that such instruction may violate an applicable Data Protection Law, Client will be responsible for all liability for all claims and damages arising from any continued processing in accordance with such instruction.

3. **Disclosure and Use of Data**.

(a) When providing or making available Client Personal Information to Accenture, Client shall only disclose or transmit Client Personal Information that is necessary for Accenture to perform the applicable Services.

(b) Following expiration or termination of the provision of Services relating to the processing of Client Personal Information, or at Client's request, Accenture shall (and shall require that its sub-processors) promptly and securely delete (or return to Client) all Client Personal Information (including existing copies), unless otherwise required or permitted by applicable laws. Unless otherwise agreed, Accenture will comply with any Client deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.

(c) All Accenture personnel, including subcontractors, authorized to process the Client Personal Information shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.

(d) Client expressly acknowledges and agrees that, in the course of providing the Services, Accenture may anonymize, aggregate, and/or otherwise de-identify Client data ("**De-Identified Data**") and subsequently use and/or disclose such De-Identified Data for the purpose of research, benchmarking, improving Accenture's offerings generally, or for another business purpose authorized by applicable Data Protection Law provided that Accenture has implemented technical safeguards and business processes designed to prevent the re-identification or inadvertent release of the De-Identified Data.

(e) Without prejudice to what is provided for in subsection (d) above, if Client Personal Information includes California Personal Data, Accenture shall:

(i) not sell or share any such Client Personal Information.

(ii) not retain, use, or disclose any such Client Personal Information for any purpose other than business purposes specified in accordance with the Agreement; or

(iii) not retain, use, or disclose such Client Personal Information outside the direct business relationship between Accenture and Client, as set forth in the Agreement, including this DPA Policy and the applicable Service Order, unless otherwise required by law.

(iv) not process such Client Personal Information outside the specified business purpose.

(v) provide the same level of privacy protection required by the applicable obligations under CPRA for such Client Personal Information received by Accenture.

(vi) not combine personal information of opted out customers from the Client with different sources or with data collected from its own interaction with consumer.

(vii) notify the business if it can no longer meet its obligations under CPRA and will work with the business to take appropriate steps regarding such Client Personal Information.

Client agrees that execution of the Agreement by Accenture shall be deemed to constitute any certification that is required under applicable Data Protection Law to the restrictions on sale, retention, use, or disclosure of Client Personal Information herein.

4. **Security Obligations**.

(a) Each party shall implement appropriate technical and organizational security measures to safeguard Client Personal Information from unauthorized processing or accidental loss or damage, as further described in **Attachment A** ("**Data Safeguards**") and the applicable Service Order.

(b) Taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Information, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in **Attachment A** and the applicable Service Order is designed to provide a level of security appropriate to the risk in respect of the processing of the Client Personal Information.

5. If **Additional Accenture Responsibilities**.

(a) **Documentation, Audits, and Inspections**. Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in this Section and submit to inspections by Client (or Client directed third parties) in accordance with a process to be mutually agreed designed to avoid disruption of the SaaS Services and protect the confidential information of Accenture and its other clients. As required by applicable law, Accenture shall inform Client if, in Accenture's opinion, any Client inspection instruction infringes upon any applicable Data Protection Law. Client shall be solely responsible for determining whether the Services and Accenture's security measures as set forth in **Attachment A** and the applicable Service Order will meet Client's needs, including with respect to any Data Protection Laws. In the context of the SaaS Services, Client acknowledges that Accenture's Cloud Vendors use external, independent auditors to audit and verify the adequacy of their security measures, including the security of their physical data centres, and generate an audit report, available annually ("Report"). The Reports are the Cloud Vendors' Confidential Information and will be available to Client, at Client's request, subject to Client executing the Cloud Vendor's standard non-disclosure agreement. Client agrees to exercise any right to conduct an inspection of the Cloud Vendor, including under the EU Model Clauses if applicable, by instructing Accenture to obtain the relevant Cloud Vendor's Report, as described in this section. Client may change this instruction at any time upon written notice to Accenture, provided if the Cloud Vendor declines to submit to an inspection requested by Client, Accenture will not be in breach of this DPA Policy or the Agreement.

(b) **Data Subject and Supervisory Authority Requests**. As required by law and considering the nature of the Services provided, Accenture shall:

(i) provide assistance to Client as reasonably requested with respect to Client's obligations to respond to requests from Client's data subjects as required under applicable Data Protection Laws. Accenture will not independently respond to such requests from Client's data subjects, but will refer them to Client, except where required by applicable Data Protection Law; and

(ii) provide assistance to Client as reasonably requested if Client needs to provide information (including details of the Services provided by Accenture) to a competent supervisory authority, to the extent that such information is solely in the possession of Accenture or its Sub processors.

(c) **Privacy / Data Protection Impact Assessments**. As required by law and considering the nature of the Services provided and the information available to Accenture, Accenture shall provide assistance to Client as reasonably requested with respect to Client's obligations to conduct privacy / data protection impact assessments with respect to the processing of Client Personal Information as required under applicable Data Protection Laws.

6. **Sub processors**. Client generally authorizes the engagement of Accenture's Affiliates as Sub processors as may be further identified in the list attached to the Agreement or any applicable Service Order, and specifically authorizes the engagement of third parties (including the Cloud Vendor) as Sub processors as identified in the applicable Service Order. Accenture shall contractually require (including via EU SCCs or via intra-company agreements with respect to Affiliates as applicable) any such Sub processors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder. Accenture shall remain fully liable for the performance of the Sub processors. Accenture shall provide Client with written notice of any intended changes to the list of authorized Sub processors, or any intended appointment of a new third-party Sub processor and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes / appointment. If Client's objection is based on anything other than the proposed Sub processor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the parties shall be resolved via the contract dispute resolution procedure.

7. **Cross-Border Transfers of Client Personal Information**.

(a) **Transfers of EEA/Swiss Data**.

Subject to subsection (d) below, the parties shall rely on the EU Standard Contractual Clauses for the transfers of personal data to third countries pursuant to Regulation (EU) 679/2016, adopted by the EU Commission by its Implementing Decision (EU) 2021/914 of 4 June 2021 (the "**EU SCCs**") to protect Client Personal Information being transferred from a country within the European Economic Area ("**EEA**") and/or Switzerland to a country outside the EEA/Switzerland that is not recognized as providing an adequate level of protection for personal data. The parties will cooperate in good faith to agree on and execute the appropriate module of the EU SCCs to be used based on the data transfer occurring under the applicable Service Order.

(b) **Transfers of UK Data**. Subject to subsection (d) below, the parties shall rely on the EU Standard Contractual Clauses for the transfers of personal data to processors established in third countries, dated 5 February 2010 (2010/87/EU) as amended from time to time by the Information's Commissioner Office (the "**UK SCCs**") to protect Client Personal Information being transferred from the United Kingdom (UK) to a country outside the UK not recognized as providing an adequate level of protection for personal data. Where the transfer relies on the UK SCCs, the Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such UK SCCs with the relevant Accenture entity or a third-party entity, acting as a data importer.

(c) **Transfers of non-EEA/Swiss/UK Data** In the event that Client Personal Information is to be transferred outside the country of origin in connection with the provision of Services under the Agreement and this country is not located within the EEA, Switzerland or the United Kingdom, the parties will work together expeditiously and in good faith to establish the appropriate transfer mechanism to be implemented, as required by applicable Data Protection Law.

(d) **Accenture BCR-P**. If and when Accenture's Binding Corporate Rules for Processors are approved, the parties shall rely on such Binding Corporate Rules for Processors to cover any cross-border transfer of Client Personal Information to Accenture, provided that Accenture (i) maintains the applicable approval of its Binding Corporate Rules for Processors for the duration of the applicable Service Order; (ii) promptly notifies Client of any subsequent material changes in the Binding Corporate Rules for Processors or such approval; and (iii) downstream all of its applicable data protection obligations under its Binding Corporate Rules for Processors to Sub processors by entering into appropriate onward transfer agreements with any such Sub processors.

Transfer Mechanism. If the transfer mechanisms agreed by the parties herein are amended, replaced, or cease to be authorized to provide "adequate protection" with respect to transfers of Client Personal Information,

the parties will work together expeditiously and in good faith to establish another valid transfer mechanism and/or implement supplementary measures as needed to establish appropriate safeguards for such data. Any impacts on the terms of the Agreement and the provision of the Services caused by such new requirements will be addressed by the parties in accordance with Section 10 below.

8. **Information Security Incidents**. Accenture shall maintain procedures to detect and respond to Information Security Incidents. If an Information Security Incident occurs which may reasonably compromise the security or privacy of Client Personal Information, Accenture will promptly notify Client without undue delay. Accenture will cooperate with Client in investigating the Information Security Incident and, considering the nature of the Services provided and the information available to Accenture, aid Client as reasonably requested with respect to Client's breach notification obligations under any applicable Data Protection Laws.

9. **Use of Business Contact Information**. Each party consents to the other party using its Business Contact Information for contract management, payment processing, service offering, and business development purposes, including business development with partners, and such other purposes as set out in the using party's global data privacy policy (copies of which shall be made available upon request). For such purposes, and notwithstanding anything else set forth in the Agreement or this DPA Policy with respect to Client Personal Information in general, each party shall be considered a controller with respect to the other party's Business Contact Information and shall be entitled to transfer such information to any country where such party's global organization operates.

10. **Changes in Laws**. In the event of (i) any newly enacted Data Protection Law, (ii) any change to an existing Data Protection Law (including generally-accepted interpretations thereof), (iii) any interpretation of a new or existing Data Protection Law by Client, or (iv) any material new or emerging cybersecurity threat, which individually or collectively requires a change in the manner by which Accenture is delivering the Services to Client, the parties shall agree upon how Accenture's delivery of the Services will be impacted and shall make equitable adjustments to the terms of the Agreement and the Services in accordance with the Change Control Procedures.

11. **Relationship with Other Agreements.** For avoidance of doubt and without prejudice to the rights of any data subjects thereunder, this DPA Policy and any EU SCCs (or other data transfer agreements) that the parties or their affiliates may enter into in connection with the Services provided pursuant to the Agreement will be considered part of the Agreement and the liability terms set forth in the Agreement will apply to all claims arising thereunder.

12 **Security Standards & Management**. Data Safeguards for Client Data

These data safeguards ("Data Safeguards") set forth the security framework that Client and Accenture will follow with respect to protecting Client Content in connection with the Agreement. In the event of a conflict between these Data Safeguards and any terms and conditions set forth in the Agreement, the terms and conditions of these Data Safeguards shall prevail.

I. Security Standards.

1. General Obligations. Each Party will maintain and comply with globally applicable standards, policies and procedures intended to protect data within their own respective environments (e.g., systems, networks, user workstations, facilities) and such standards will govern and control in their respective environments.

2. Accenture Standards. Accenture's applicable security standards are as set out in Attachment A.

II. Remote Work. In addition to providing the SaaS Services support (if applicable) from Accenture locations, Accenture personnel may perform such services (or any portion) remotely, provided that performing remotely does not (i) adversely impact Accenture's ability to perform its obligations under the Agreement; or (ii) require any increase to the Fees.

For Services provided on a remote basis, any contractual requirements to provide physical and environmental security controls (e.g., secure bays; security guards; CCTV) at the Accenture service locations will not apply to remote work locations.

ATTACHMENT A

Data Safeguards for Client Content

These data safeguards ("Data Safeguards") set forth the technical and organizational measures that Accenture will follow with respect to maintaining the privacy and security of Client Content.

I. Controlling Standards

1. Accenture Standards. Accenture will, and will contractually require its vendors and contractors to, maintain globally applicable Accenture policies, standards, and procedures intended to protect data within Accenture's environments, and, except as otherwise set forth herein, will comply with such policies in connection with the provision of the Services. Such policies will govern and control within Accenture's environments and be reviewed at least annually.

Examples of such policies and Standards include:

- System Security
- Security of Information and Acceptable Use of Systems
- Confidentiality
- Data Privacy
- Data Management
- Application Security Standard
- Encryption Standard
- Identification and Authentication Standard
- AWS and Azure Cloud Security Configuration Standard

II. Technical and Organizational Measures. Without limiting the generality of the foregoing, Accenture has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Client Content against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction, as follows:

1. Organization of Information Security

a) Security Ownership. Accenture will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.

b) Security Roles and Responsibilities. Accenture personnel with access to Client Content will be subject to confidentiality obligations.

c) Risk Management Program. Accenture will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Client Content in connection with the applicable Agreement in place between the Parties.

d) Client Program. Client will manage, as applicable, its own information security program, including reasonable policies and procedures to be applied on its users and the components that interact with the Accenture ec&V Platform Services, including those addressing:

a. Client end-user training,

b. end-user authentication or API based authentication to the Platform Services

c. security on workstations from Client users, and

d. security on backend systems, integration points or network devices into Client network that is connecting with the eC&V Service.

2. Asset Management

a) Asset Inventory. Accenture will maintain an inventory of all media, servers, and other systems (including third-party and cloud systems) on which Client Content is stored. Access to the inventories of such media will be restricted to the Parties' personnel authorized to have such access.

b) Data Handling.

i. Each Party will classify Client Content to help identify such data and to allow for access to it to be appropriately restricted (e.g., through encryption). Without limiting the generality of the foregoing, Accenture shall encrypt Client Content at rest within the Accenture eC&V platform using ciphers at least as strong as 256-bit AES. Accenture shall ensure that Client Content in transit to and from the eC&V Platform Services is transferred to/from the eC&V Platform Services across encrypted network connections and/or protocols (i.e., HTTPS and/or VPN).

ii. Accenture will limit printing of Client Content to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Client Content.

iii. Accenture will require its personnel to obtain appropriate authorization prior to storing Client Content on portable devices or processing Client Content outside the Parties' facilities.

3. Human Resources Security

a) Security Training.

i. Each Party will inform its personnel about relevant security procedures and their respective roles. Each Party also will inform its personnel of possible consequences of breaching the security rules and procedures.

ii. Accenture will only use anonymous data in training.

iii. Accenture Resources working to provide support to the eC&V platform will be rolled on in the eC&V CDP plan.

4. Physical and Environmental Security

a) Physical Access to Facilities. Accenture shall maintain appropriate physical safeguards at and will only allow authorized individuals to access facilities where information systems that process Client Content are located.

b) Protection from Disruptions. Accenture will use a variety of industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) systems to protect against loss of data due to power supply failure or line interference.

c) Component Disposal. Accenture will use industry standard (i.e., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) processes to delete Client Content when it is no longer needed.

5. Communications and Operations Management

a) Operational Policy. Accenture will maintain security documents describing their security measures and the relevant procedures and responsibilities of their personnel who have access to Client Content.

b) Network Security. Accenture shall utilize an enterprise-class security information and event management (SIEM) system and maintain firewalls and other control measures (e.g., security appliances, network segmentation) to provide reasonable assurance that access from and to its networks is appropriately controlled.

c) All AWS and Azure subscriptions used in the provision of the eC&V service will be provisioned via myNav CMO and will be integrated into Accenture Information Security SOC / ISD.

d) Data Recovery Procedures

i. Accenture will have specific data recovery procedures in place designed to enable the recovery of Client Content being maintained in its systems.

ii. Accenture will review and test its data recovery procedures at least annually.

iii. Accenture will log data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

iv. Accenture will meet its Recovery Point Objectives and Recovery Time Objectives set forth in the disaster recovery plan as per the defined operating level agreement.

e) Data Beyond Boundaries.

i. Accenture will encrypt Client Content that is transmitted over public networks.

ii. Accenture will implement Multi-Factor Authentication for remote access over virtual private network (VPN).

f) Event Logging.

i. Accenture will log the use of their respective data-processing systems.

ii. Accenture will log access and use of information systems containing Client Content, including at a minimum registering the access ID, time, and authorization granted or denied.

iii. Accenture will implement a log retention policy for the Platform logs according to current Accenture logging and auditing standards, including, at a minimum, a 6-month retention.

iv. As part of the eC&V Platform service, Accenture will enable SOC tools including the Security Information & Event Management system that will analyze log and event data in real time to provide threat monitoring, event correlation and incident response.

6. Access Control

a) Access Policy. Accenture will maintain, periodically review, and manage a record of security privileges of individuals having access to Client Content. Client will maintain, periodically review, and manage a record of security privileges of individuals in connection with accessing the eC&V Platform Services or keys.

b) Access Authorization.

i. Accenture will maintain and update a record of personnel authorized to access Client Content s.

ii. When responsible for access provisioning, each Party will promptly provision authentication credentials.

iii. Accenture will deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed six months).

iv. Client will provide notice to Accenture so that it may deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days. Accenture shall promptly deactivate access credentials to all systems where access by the applicable person is no longer needed (e.g., employee termination, project reassignment, etc.).

v. Accenture will identify those personnel who may grant, alter, or cancel authorized access to data and resources.

vi. Each Party will ensure that where more than one individual has access to systems containing Client Content, the individuals have unique identifiers/log-ins. As applied to Client, this obligation only applies to the eC&V Platform Service.

c) Least Privilege.

i. Technical support personnel will only be permitted to have access to Client Content when needed.

ii. Each Party will restrict access to Client Content to only those individuals who require such access to perform their job function.

iii. Each Party will limit access to Client Content to only that data minimally necessary to perform the services.

d) Integrity and Confidentiality. Each Party will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.

e) Authentication.

i. As applicable, Accenture Enterprise Sign-on (ESO) will be enabled for Client end user access.

ii. Authentication for backend API keys or other integrations will follow Accenture Information Security standards.

iii. Accenture individuals supporting any layer or component of the Platform and accessing with administrative privileges will be required to use multi-factor authentication for access to the Platform console and administrative utilities. Specifically, all access from Accenture individuals to AWS or Microsoft Azure Console or to the SSL VPN solution will require Multi Factor Authentication. All Kubernetes management, Operating System, Middleware and Database management access will also require connectivity to the SSL VPN with Multi Factor Authentication.

f) Testing. Accenture shall perform security testing of the EC&V platform, including:

i. Dynamic Scans (web App/API) every 6 months or with every new major release of the eC&V product.

ii. Static/Source Code Scans every 6 months or with every new major release of the eC&V product.

iii. SOC Tools infra scans (internal, external, NCS, Container, etc.) following the standard ISD scanning periodicity.

iv. Open Source (OSS) Scans every 6 months or with every new major release of the eC&V product.

v. Accenture may agree to share with Client summary level information related to such tests as conducted by Accenture to the extent applicable to the Services.

vi. For clarity, as it relates to such penetration and vulnerability testing, Client will not be entitled to (i) data or information of other customers or clients of Accenture; (ii) test third party IT environments except to the extent Accenture has the right to allow such testing; (iii) any access to or testing of shared service infrastructure or environments, or (iv) any other Confidential Information of Accenture that is not directly relevant to such tests and the Services.

vii. For any Accenture IT systems that are physically dedicated to Client, the Parties may agree to separate, written testing plans and such testing will not to exceed two tests per year.

7. Patch Management

a) Accenture will have a patch management procedure, aligned to Accenture Information Security patch management and security remediation standards, that deploys security patches for systems used to process Client Content that includes:

i. Defined time allowed to implement patches (not to exceed 90 days for all patches); and

ii. Established process to handle emergency patches in a shorter time frame.

b) Accenture agrees that no software or hardware that is past its End of Life (EOL) will be used in the scope of services without a mutually agreed risk management process for such items.

8. Workstations

a) Accenture will implement controls to ensure only Accenture workstations can be used in the provision and operation of the Service.

9. Information Security Breach Management

a) Security Breach Response Process. Accenture will maintain a record of Security Incidents (defined below) with a description of the breach, the period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.

b) Security Incident Notification. Client will promptly notify Accenture about any confirmed misuse of Client accounts or authentication credentials, or other known security incidents originating with Client that, in each case, relates to unauthorized use of the Platform Services. Accenture will promptly notify

Client if it becomes aware of any actual misuse or unauthorized access or disclosure of PII in breach of any obligation in this Services Order.

c) Security Incidents will not include any of the following that results in no unauthorized access to Client Personal Information or to any systems storing Client Personal Information (without limitation): pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents. Accenture will provide regular updates on any Security Incident and the investigative action and corrective action taken.

d) In case there is a Security Incident impacting Client Data, in addition to the upfront Accenture notification and incident response process (including forensics, root cause analysis and communications), for components under the Accenture control, Accenture will provide full cooperation with Client to facilitate access to client-specific logs, Client-specific information related with the Security event (e.g. client specific IP or network diagrams).

10. Business Continuity Management

a) Accenture will maintain and test, at least once per year, emergency, and contingency plans for the facilities in which Accenture's information systems that process Client Content are located.

b) Accenture's redundant storage and procedures for recovering data will be designed to reconstruct Client Content stored by a Party in its original state from before the time it was lost, damaged, or destroyed.

c) Accenture shall provide 24/7 managed backup services of any persistent data (if any) include Client Content stored in the primary site backed up on at least a daily basis to a secondary site.

d) EC&V service will be implemented on multiple cloud Availability Zones, as a multi-AZ service, thus, effectively enabling a metropolitan DR approach. System will be resilient to a failure into a specific AWS AZ or AWS Datacenter.

e) While offsite regional backups will be available, Accenture will not initially implement a formal multi-regional DR approach so in the unlikely event of an outstanding AWS regional failure, the recovery of the service in a secondary region will be enabled on a "best effort" basis.

11. Client data protection: Aspects described in the section below are related the data exchange inbound and outbound via the eComply & Verify API Endpoints in production.

11.1 Client Data Encryption

The eComply & Verify Service applies client data encryption in transit and at rest, which prevents unauthorized data access.

11.2 Client Data Persistence

The eComply & Verify Service persists the data as provided until the processing end state is reached. Once the end state is reached, data and log protocol will be entirely and permanently removed from the eComply & Verify Service.

The processing starts when eComply & verify receives data through dedicated API Endpoints.

The processing ends when all applicable processing steps are completed, and the internal service retention period has elapsed.

An internal service retention period is defined as part of the eComply & Verify service which defers the full end state of client data processing as following:

For successful processing up to 72h = 3 x 24h (3 days)

For processing with error up to 240h =10 x 24h (10 days)

Deferring the purge of data is solely to enable detailed analysis and support as part of the eComply & Verify service in case of immediate request.

The eComply & Verify Service provides API to return the processing status, protocol, log information as well as the processed data back to the caller / client. The client is responsible for any required data retention to persist this information outside of the eComply & Verify Service.

The eComply & Verify Service generated information (Logs, Processing Statistics, Identifier, etc.) is stored without any client data (or anonymized/masked) and is therefore not in scope.

11.3 Client Data Isolation

The eComply & Verify Service is designed with a multitenant architecture which supports client data isolation by default.

Accenture can offer the additional option to host the eComply & Verify Service on a dedicated instance for exclusive operation.

11.4 Client Data Transfer

By using the eComply & Verify Service the client permits the transfer and exchange of the data with the respective parties and platforms eComply & verify interacts with to perform the service.

All transmissions between eComply & Verify Service and the external systems use TLS and require HTTPS secure connections. The eComply & Verify API access is secured via OAuth2 protocol.

11.5 Client Data Transformation

The eComply & Verify Service is designed to transform the structured information from Unified Business Language (UBL) standard into the format required by the receiving entity. The eComply & Verify Service will transform only format. The data content itself will remain unchanged. In cases where the data does not pass the content requirement checks, the eComply & Verify Service will respond with the related check error (there will be no auto correction mechanism which represents a data content change).

11.6 Malicious Data Input Handling:

By implementing the process of validating incoming data, the eComply and Verify service effectively minimises the potential risk of receiving and processing malicious or harmful data. This validation mechanism acts as a robust defence mechanism, ensuring that only legitimate and trustworthy data is accepted and processed by the service.

11.7 Authorization

The eComply and Verify service adheres to the principle of minimal privilege (PoMP), which enhances its security measures. By implementing PoMP, the service ensures that each user or process has precisely the permissions required to fulfil their specific responsibilities.

11.8 Error Handling

The eComply & Verify Service provides robust error handling and captures processing activities within secure log files.

11.9 Security

eComply and verify is built on the technology offered by major cloud providers covering compute, network, and storage layers. Cloud provider maintains third party security certifications, global examples include: ISO 9001, ISO 27001, ISO 27017, ISO 27018, CSA, SOC 1, SOC 2, SOC 3, PCI-DSS. On top of the underlying Cloud Provider security, all services and activities associated with the development, maintenance, configuration, and operation of the eComply, and Verify Platform are in scope of ISO 27001 certification.