Data Processing Addendum

1. Introduction

This Data Processing Addendum (“DPA”) is entered into by the entity identified in the signature box below (“Customer”) and the Regional CA Entity, a Broadcom Inc. company, (“CA”) and forms part of the agreement between CA and Customer for CA to provide Services (“Agreement”) to the Customer.

In the course of providing Services to Customer pursuant to the Agreement, CA may Process Customer Personal Data that is subject to the European Union’s General Data Protection Regulation, Regulation (EU) 2016/679 (“GDPR”) or other Data Protection Laws. This DPA reflects the parties’ agreement with regard to the Processing of such Customer Personal Data. For purposes of this DPA CA is the Processor and Customer is the Controller.

The parties agree to comply with the following provisions, each acting reasonably and in good faith.

2. Definitions

“Affiliates” means any entity which directly or indirectly owns, controls, is controlled by, or is under common control with a party, where control is defined as owning or directing more than fifty percent (50%) of the voting equity securities or a similar ownership interest in the controlled entity.

“Agreement” means all current and future agreements between CA and Customer in connection with which CA provides Services involving the Processing of Personal Data on behalf of Customer. This DPA is incorporated into such Agreements by this reference.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

“Data Protection Laws” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom including the GDPR, applicable to the Processing of Personal Data under the Agreement.

“Regional CA Entity” shall mean, depending on the CA entity that is a party to the Agreement, CA Inc., 1320 Ridder Park Drive, San Jose, CA 95131, CA, Inc.,1320 Ridder Park Drive, San Jose, CA 95131 (North America) or CA Europe Sarl Route de la Longeraie 9, 1110 Morges Switzerland (Europe, Middle East and Africa) or CA Programas de Computador, Avenida Dr. Chucri Zaidan, 1240 – 27º andar, Golden Tower, CEP 04711-130 - São Paulo-SP, Brazil - CNPJ/MF 08.469.511/0001-69 (Latin America) or CA (Singapore) Pte Ltd., Collyer Quay, Singapore 049318 SG (Asia, Pacific and Japan).

“Personal Data” means any information relating to an identified or identifiable natural person (**“Data Subject”**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;, “Personal Data Breach” breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

“Processing” (and its cognates), means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Services” means the provision of maintenance and support services and/or the provision of software as a service (“SaaS”) and/or any other services, hosted, managed or otherwise, which are provided under the Agreement and for the purposes of which CA Processes Personal Data on behalf of the Customer.

“Standard Contractual Clauses” means the agreement pursuant to the European Commission’s decision 2010/87/EU of 5 February 2010 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in third countries, which do not ensure an adequate level of data protection.

“Supervisory Authority” means an independent public authority which is established under applicable Data Protection Laws

“Sub-Processor” means any Processor engaged by CA or its Affiliates.

3. Processing Operations

a) The subject matter and duration of the Processing of Personal Data are set out in the Agreement, which describes the provision of the Services to Customer. The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set forth in Annex 1 to this DPA (titled “Annex 1: Details of Processing Customer Personal Data”).

b) In its Processor capacity, CA shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Services then constitutes further instructions. CA will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Laws and technically feasible.

c) As part of the configuration of the Services, certain security features and data Processing functionalities are made available to the Customer. Customer is responsible for properly configuring the Services to meet its specific Processing and security requirements, which may include use of pseudonymization and/or encryption technologies and of any other such information security and/or privacy enhancing measures as Customer deems appropriate to protect the Personal Data from unauthorized Processing.

d) Customer is responsible for the accuracy, quality, and legality of the Personal Data, and the means by which Customer acquired the Personal Data.

4. Processing Obligations

When providing the Services, CA shall:

a) Process such Personal Data in compliance with Customer’s instructions as set forth in the parties’ Agreement for Services, including with regard to transfers of Personal Data to a third country or international organization, unless other Processing is required by applicable Data Protection Laws, in which case CA shall inform Customer of that legal requirement before Processing unless the law prohibits such notice on important public-interest grounds;

b) Ensure that CA personnel authorized to Process such Personal Data have committed themselves to confidentiality at least as protective as those of this DPA or the Agreement governing the applicable engagement with CA for which Processing is performed or are under an appropriate statutory obligation of confidentiality;

c) Implement appropriate technical and organizational measures to protect such Personal Data in accordance with applicable Data Protections Laws, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons; as set forth in Annex 2 - Security of Processing

d) Taking into account the nature of the Processing and the information available to CA, assist Customer in ensuring compliance with Customer's obligations pursuant to Articles 32 to 36 of the GDPR and in accordance with applicable Data Protections Laws;

e) Upon termination of the parties' Agreement and/or after the end of provision of the Services to which this DPA applies, delete or return any Customer Personal Data in accordance with Data Protection Laws and/or consistent with the terms of the Agreement as soon as reasonably practicable, unless applicable law requires further storage;

f) Inform Customer if CA cannot comply with an instruction or in CA's opinion, a Customer instruction infringes applicable Data Protection Laws.

5. Data Subject's Rights

a) Taking into account the nature of the Processing, CA shall use appropriate technical and organizational measures insofar as possible to assist Customer in fulfilling Customer's obligation to respond to requests for the exercise of Data Subject rights in accordance with applicable Data Protections Laws.

b) CA shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, objection to further Processing, or its right not to be subject to automated individual decision making ("Data Subject Request"). Except to the extent required by applicable law, CA shall not respond to any such Data Subject Request without Customer's prior written authorization or explicit instruction, except to confirm that the request relates to Customer.

6. Data Protection Impact Assessment

a) CA shall provide Customer with reasonable assistance as needed to fulfil Customer's obligation to carry out a data protection impact assessment as related to Customer's use of the Services. CA will provide such assistance upon Customer's reasonable request and to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to CA.

b) CA shall provide Customer with reasonable assistance in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 6 and to the extent required under applicable Data Protection Laws.

7. Sub-Processing

a) CA is granted a general authorization to subcontract the Processing of Personal Data to Sub-Processors. CA shall enter into a written agreement with any such Sub-Processor that Processes Customer Personal Data which imposes obligations on the Sub-Processor no less protective than those imposed on CA under this DPA.

b) CA shall remain liable to Customer for the performance of Sub-Processors' obligations with respect to Customer Personal Data in accordance with the terms of this DPA. The list of Sub-Processors used by CA in connection with its provision of the Services is set forth in Annex 2, and such list includes all Sub-Processors' identities and country of location ("Sub-Processors List"). In the event CA makes any changes or additions to such list, CA shall provide notice through the current Sub-Processor List made available to Customer at: https://techdocs.broadcom.com/us/product-content/admin-content/subprocessor-list.html or https://www.symantec.com/enterprise-privacy for Symantec branded solutions or through email where Customer has subscribed under http://learn.broadcom.com/subprocessor-news-opt-in for notification. Customer may object to such changes as set forth in subsection c) below.

c) Customer may object to CA's use of a new Sub-Processor by notifying CA promptly in writing within thirty (30) calendar days after any updates are made by CA to the Sub-Processor list or Customer has been notified by email. In the event of such objection by Customer, CA will take commercially reasonable steps to address the objections raised by Customer and provide Customer with reasonable written explanation of the steps taken to address such objection.

8. Data Transfers

a) CA will abide by the requirements of European Economic Area, the United Kingdom and Swiss data protection laws regarding the collection, use, transfer, retention, and other Processing of Personal Data from the European Economic Area, the United Kingdom and Switzerland. Solely for the provision of Services to Customer under the Agreement, Personal Data may be transferred to and stored and (or) Processed in any country in which CA or its Sub-Processors operate. Customer instructs CA to perform any such transfer of Personal Data to any such country and to store and Process Personal Data to provide the Services. All transfers of Personal Data out of the European Union, European Economic Area, United Kingdom and Switzerland shall be governed by the Standard Contractual Clauses or be subject to appropriate safeguards in accordance with applicable Data Protections Laws.

b) CA and CA Affiliates acting as Sub-Processors have previously entered into The EU Standard Contractual Clauses for a Controller-Processor relationship and for the benefit of the Customer. In addition, CA has certified its compliance to the EU-US Privacy Shield Program. CA shall maintain its certification to the Privacy Shield for so long as it maintains any European Economic Area Personal Data.

c) In the event of a conflicting clause between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. For the avoidance of doubt, where this DPA further specifies Sub-Processor and audit rules in Sections 7 and 9, such specifications also apply in relation to the Standard Contractual Clauses and shall only supplement them.

9. Audit

a) CA shall make available to Customer, upon reasonable written request, information related to the Processing of Personal Data of Customer as necessary to demonstrate CA's compliance with the obligations under this DPA. CA shall allow for inspection requests by Customer or an independent auditor in relation to the Processing of Personal Data to verify that CA's is in compliances with this DPA, if (a) CA has not provided sufficient written evidence of its compliance with the technical and organizational measures, e.g. a certification of compliance with ISO 27001 or other standards; (b) a Personal Data Breach has occurred; (c) an inspection is officially requested by Customer's Supervisory Authority; or (d) Data Protection Law provides Customer with a mandatory on-site inspection right; and provided that Customer shall not exercise this right more than once per year unless mandatory Data Protection Law requires more frequent inspections. Any information provided by CA and/or audits performed pursuant to this section are subject to the confidentiality obligations set forth in the Agreement. Such inspections shall be conducted in a manner that does not impact the ongoing safety, security, confidentiality, integrity, availability, continuity and resilience of the inspected facilities, networks and systems, nor otherwise expose or compromise any confidential data Processed therein.

b) Customer is responsible for all costs associated with any such audit or inspection, including reimbursement of CA for all reasonable costs of complying with Customer or regulator instructions, unless such audit reveals a material breach by CA of this DPA, then CA shall bear its own cost of an such audit. If an audit determines that CA has breached its obligations under the this DPA, CA will promptly remedy the breach at its own cost.

10. Security and Breach

a) CA shall implement appropriate technical and organizational measures to protect such Personal Data in accordance with applicable Data Protections Laws taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and as set forth in Annex 2 - "Security of Processing".

b) CA shall notify Customer without undue delay after becoming aware of any Personal Data Breach involving such Customer Personal Data Processed by CA; CA will use reasonable efforts to identify the cause of such Personal Data Breach and shall without undue delay: (a) investigate the Personal Data Breach and provide Customer with information about the Personal Data Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Article 33(3) of the GDPR to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach to the extent the remediation is within CA's reasonable control. Notification will be delivered to Customer in accordance with subsection d) below.

c) CA's obligation to report or respond to a Personal Data Breach under this Section is not and will not be construed as an acknowledgement by CA of any fault or liability with respect to the Personal Data Breach.

d) Notification(s) of Personal Data Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means CA selects, including via email. It is Customer's sole responsibility to ensure it provides and maintains accurate contact information at all times.

11. Limitation of Liability

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement governing the applicable Services, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Annexes, Schedules and/or Appendices.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement(s) between Customer and the Regional CA Entity, which is party to the Agreement, as of Customer's Signature Date below. If this document has been electronically signed by either party such signature will have the same legal affect as a hand-written signature.

Agreed for and on behalf of CA	**Agreed for and on behalf of Customer**
CA, Inc., 1320 Ridder Park Drive, San Jose, CA 95131 DocuSigned by: By: Mark Brazeal 4AF36F177230453... Mark Brazeal	Customer: Signature: ______________________ Name/Title: Signature Date:
CA Europe Sarl, Route de la Longeraie 9, 1110 Morges, Switzerland DocuSigned by: By: ______________________ 4D217E50FB3240A... Deborah Streeter	
CA Programas de Computador, Participações e Serviços Ltda., Avenida Dr. Chucri Zaidan, 1240 – 27º andar, Golden Tower, CEP 04711-130 - São Paulo-SP, Brazil - CNPJ/MF 08.469.511/0001-69 DocuSigned by: By: ______________________ 532DEB4BF5DC428... Denise Bicho	
CA (Singapore) Pte Ltd., Collyer Quay, Singapore 049318 SG DocuSigned by: By: ______________________ 4D217E50FB3240A... Deborah Streeter	

Annex 1 – Details of Processing of Customer Personal Data

This Annex 1 includes certain details of the Processing of Customer's Personal Data as required by Article 28 (3) GDPR (or as applicable, equivalent provisions of any other Data Protection Law).

1. Customer Data Protection Officer:

2. Subject matter and duration of the Processing of Customer Personal Data:

Customer Personal Data is used to provide the Services as set out in the Agreement. The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this Addendum.

3. The nature and purpose of the Processing of Customer Personal Data:

- Collection
- Recording
- Disclosure
- Deletion
- Alteration
- Restriction
- Use

4. The Categories of Customer Personal Data (*) to be Processed may include:

(a) Contact details including but not limited to name, job title and level, business email addresses, phone numbers and office addresses;

(b) Email addresses, IP addresses and other network and devices or software identification information;

(c) Online data (e.g. website usage, browsing activities and preferences and other web traffic data);

(d) Log data which may include certain source and destination IP addresses, host name, user-ids, URLs, policy names, email addresses, date and time stamps, data volumes, email activity and content;

(e) Any Personal Data which may be contained within (i) email and web communications (including their attachments) which are sent to or from employee or users of the Customer' network, (ii) any Personal Data that may be shared by Customer's employees or users with cloud applications used in the data exporter's network and ;(iii)technical and support requests raised by or on behalf of Customer; and

(f) Any other email and web activity related Personal Data as required for the provision of the Services.

5. The Categories of Data Subjects (*) to whom the Customer Personal Data relates:

Customer's employees, representatives, customers, vendors, and/or any other business contacts including senders and recipients of emails, as applicable.

(*) Complementary description of the categories of Personal Data and Data Subjects for Symantec branded solutions can be found at https://www.symantec.com/enterprise-privacy

6. Other Personal Data:

7. Special Categories of Personal Data (Art. 9 GDPR):

8. Sub-processors:

A current list of Sub-processors is maintained at https://techdocs.broadcom.com/us/product-content//admin-content/subprocessor-list.html for CA Technologies Infrastructure Products and Solutions and at https://www.symantec.com/enterprise-privacy for Symantec branded solutions

Annex 2 - Security of Processing

CA adopts a standards neutral approach in its commitment towards security of processing. The applicability and scope of various standards (and corresponding controls) may differ with respect to the requirements of a specific business unit, service, product or specific engagement. Controls and standards referenced herein this document reflect a "minimum" standard of policies and procedures and are intended to provide a general confirmation of implementation of such standards across applicable products and solutions.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, CA shall implement the measures outlined below to ensure an appropriate level of security for the provision of maintenance and support services ("On Premise") and/or the provision of software as a service ("SaaS").

1. Measures on pseudonymization /anonymization of personal data

Data stored in this product is not generally of a nature that requires pseudonymization or anonymization. If required, Customer should escalate to CA.

On Premise:
Not applicable

2. Measures on the encryption of personal data:

ENCRYPTION
All data is encrypted in-transit using TLS 1.2 or higher. In addition, Customer Data is encrypted on any server or device that is removed from CA's premises for backup or off-site storage (where applicable). Key management procedures are employed that assure the confidentiality, integrity and availability of cryptographic key material. Use of encryption products comply with local restrictions and regulations on the use of encryption in a relevant jurisdiction.

Encryption Policy
Data security policy that dictates encryption use is documented. The encryption strength of Customer Data in transmission is defined.

Encryption Key Management
Cryptographic key management procedures are documented and automated. Products or solutions are deployed to keep the data encryption keys encrypted (e.g., software based solution, Hardware Security Module (HSM)).

Encryption Uses
Customer Data transmission over the public internet always utilizes encrypted channel. Encryption details are documented if transmission is automated. Approved and dedicated staff is responsible for encrypting/ decrypting the data, if manual. Customer Data must also be encrypted while in transit over any network. VPN transmissions are performed over an encrypted channel.

On Premise:
Controller provides support case data in an encrypted manner to processor. Case resolution is done in a secured environment. 30 days after case is closed, support case data is deleted

3. Measures of ensuring the ongoing confidentiality of personal data:

All access to the data centers where Customer data is stored, is restricted to CA's Operations Team according to CA Information Access Control Policies and CA Segregation of Duties Policy (CA follows the principle of least privilege and only grants access based on role and business use case). Access rights are reviewed regularly or upon change of role/termination of an employee. Access to the environment where Customer data is stored is strictly controlled and monitored. Customer is responsible for managing access to their subscription data and are responsible for the lifecycle of those accounts. Customer Subscription Administrators are responsible for user administration and related password policies within the application.
The Customer is responsible for the lifecycle of this account.

On Premise:
Work is done in secure environment; data transfer is secured. Deletion of data after closing of support case.

4. Measures to ensure ongoing integrity of personal data:

DATA INTEGRITY
CA Technologies Policies and Procedures are designed to ensure that any data stored, received, controlled or otherwise accessed is not compromised and remains intact. Inspection procedures are in place to validate data integrity.
Data Transmission Controls
Data transmission control processes and procedures to ensure data integrity are documented. Check sums and counts are employed to validate that the data transmitted is the same as data received.
Data Transaction Control
Controls to prevent or identify duplicate transactions in financial messages are documented. Digital certificates (e.g., digital signature, server to server) utilized for ensuring data integrity during transmission follow a documented process and procedure.

On Premise:
Not applicable; Data is deleted after closing of support case, see section 2 a) to e)

5. Measures to ensure ongoing availability of processing systems and services:

AVAILABILITY CONTROL
Protection against fire and measures in case of power outages in the data processing centers including backup
Physical Controls
CA Technologies has effective controls in place to protect against physical penetration by malicious or unauthorized people. Physical controls covering the entire facility are documented. Additional access restrictions are enforced for servers/ computer/ telecommunications room compared to the general area.
Backup and Offsite Storage
CA Technologies has a defined backup policy and associated procedures for performing backup of data in a scheduled and timely manner. Effective controls are established to safeguard backed up data (onsite and off-site). CA Technologies also ensures that Customer Data is securely transferred or transported to and from backup locations. Furthermore, CA Technologies conducts periodic tests to ensure that data can be safely recovered from backup devices.
Backup Process
Backup and offsite storage procedures are documented. Procedures encompass ability to fully restore applications and operating systems. Periodic testing of successful restoration from back-

up media is demonstrated. The on-site staging area has documented and demonstrated environmental controls (e.g., humidity, temperature).

Backup Media Destruction

Procedures are defined for instructing personnel on the proper methods of backup media destruction. Back up media destruction by a third party is accompanied by documented procedures (e.g., certificate of destruction) for destruction confirmation.

Offsite Storage

Physical security plan for the offsite facility is documented. Access controls is enforced at entry points and in storage rooms. Access to the off-site facility is restricted and there is an approval process to obtain access. Electronic transmission of data to off-site location is performed over encrypted channel.

On Premise:

Closed-Shop-Environment; not applicable. Data remains with controller in existence

6. Measures to ensure ongoing resilience of processing systems and services:

VULNERABILITY MONITORING

CA Technologies continuously gather and analyze information regarding new and existing threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. Monitoring controls include related policy and procedure, virus and malicious code, intrusion detection, and event and state monitoring. Related logging process provides an effective control to highlight and investigate security events.

Vulnerability Policy and Procedure

Penetration/ vulnerability testing of the internal/ external networks and/ or specific hosts is performed. The tests are usually performed externally by a reputed external organization. Customer environments are covered as part of the scope of the tests. All issues rated as high risk are remediated with appropriate timelines.

Anti-virus and Malicious Code

Servers, workstations and internet gateway devices are updated periodically with latest antivirus definitions. Defined procedure highlights all anti-virus updates. Anti-virus tools are configured to run weekly scans, virus detection, real time file write activity and signature files updates. Laptops and remote users are covered under virus protection. Procedures to detect and remove any unauthorized or unsupported (e.g., freeware) applications are documented.

Alert events include the following attributes:

Unique identifier
Date
Time
Priority level identifier
Source IP address
Destination IP address
Event description
Notification sent to security team
Event status

Security Event Monitoring

Security events are logged (log files), monitored (appropriate individuals) and addressed (timely action documented and performed). Network components, workstations, applications and any monitoring tools are enabled to monitor user activity. Organizational responsibilities for responding to events are defined. Configuration checking tools are utilized (or other logs are utilized), that record critical system configuration changes. The log permission restricts alteration by administrators. Retention schedule for various logs are defined and adhered.

7. Measures to restore availability and access to personal data in the event of a technical of physical incident:

See above AVAILABILITY CONTROL
INCIDENT RESPONSE
CA Technologies documents a plan and associated procedures in case of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant notification parties. Incident response personnel are trained. Execution of the incident response plan is tested periodically.
Incident Response Process
Information security incident management policy and procedures are documented. The incident management policy and/ or procedures include the following attributes:

- Organizational structure is defined
- Response team is identified
- Response team availability is documented
- Timelines for incident detection and disclosure are documented
- Incident process lifecycle is defined including the following discrete steps:
  - Identification
  - Assignment of severity to each incident
  - Communication
  - Resolution
  - Training
  - Testing (check frequency)
  - Reporting
- incidents must be classified and prioritized
- incident response procedures must include Customer notification to the relationship (delivery) manager or another contact listed in the contract

Escalation/Notification
Incident response process is executed as soon as CA Technologies is aware of the incident (irrespective of time of day).

On Premise:
Only partially applicable; Data is deleted after support case is closed.

8. Measures for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures:

ORGANIZATIONAL CONTROL
OPERATIONS
CA Technologies has documented IT operational procedures to ensure correct and secure operation of its IT assets.

Operational Procedures and Responsibilities.
Operational procedures are documented in an operations manual and successfully executed.
The operations manual includes the following components:
Scheduling requirements
Handling errors (e.g., transport of data, printing, copies)
Generating and handling special output
Maintenance and troubleshooting of systems
Documented procedures to manage the SLAs/ KPIs and the reporting structure for escalations

Internal security audits are done on a regular basis at the processor including the data protection officer